



CYBERSECURITY ANALYSIS

An Overview: The Elements of Cybersecurity Analysis (Modules 1-9)

Cybersecurity Analysis (CCA)

An Overview:
The Elements of Cybersecurity Analysis
(Modules 1-9)



International Institute of Business Analysis, Toronto, Ontario, Canada.

IEEE-Computer Society, Los Alamitos, California, United States of America.

© 2020 International Institute of Business Analysis and IEEE-Computer Society.. All rights reserved.

Print Edition ISBN: 978-1-927584-18-7

PDF Edition ISBN: 978-1-927584-19-4

This document is provided to the business analysis community for educational purposes. IIBA® does not warrant that it is suitable for any other purpose and makes no expressed or implied warranty of any kind and assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information contained herein.

IIBA®, the IIBA® logo, BABOK® and Business Analysis Body of Knowledge® are registered trademarks owned by International Institute of Business Analysis. CBAP® is a registered certification mark owned by International Institute of Business Analysis. Certificate in Cybersecurity Analysis (CCA), Certified Business Analysis Professional, ECBA, EEP, and the EEP logo are trademarks owned International Institute of Business Analysis

No challenge to the status or ownership of these or any other trademarked terms contained herein is intended by the International Institute of Business Analysis.

Any inquiries regarding this publication, requests for usage rights for the material included herein, or corrections should be sent by email to info@iiba.org.

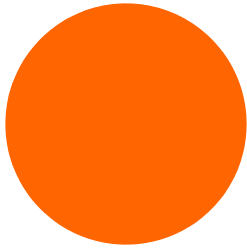


Table of Contents

Module 1: Introduction to Cybersecurity Analysis

- 1.1 IIBA and IEEE Perspective: Overview of Concepts and Approach to Improving Cybersecurity 1
- 1.2 Importance of Security 5
- 1.3 IT Functions & Roles 9
- 1.4 IT 101 - 1: The Pieces 14
- 1.5 IT 101 - 2: Using & Managing the Pieces 18
- 1.6 IT 101 - 3: Advancement 24
- 1.7 The Role of Business Analysis in Cybersecurity 28
- 1.8 Governance Perspectives of Cybersecurity 32

Module 2: Enterprise Security Concepts

- 2.1 Security Accountability 39
- 2.2 Cost of Securing an Organization 42
- 2.3 Outsourcing for Cybersecurity Expertise and Services 45
- 2.4 Risk Tolerance 48
- 2.5 Compliance 50
- 2.6 Best Practices and Benchmarking 54
- 2.7 Data Privacy 56
- 2.8 Data Privacy Nuances 59
- 2.9 Digital Rights Management (DRM) 62
- 2.10 Audit – Internal and External 65



Module 3: Enterprise Risk

- 3.1 Risk Management & Control Assurance Framework 71
- 3.2 Organizational Risk Assessment 74
- 3.3 Risk Analysis: Threat Risk Assessments 77
- 3.4 Risk Analysis: Vulnerability Assessments 80
- 3.5 Business Case Development 83
- 3.6 Disaster Recovery and Business Continuity 86

Module 4: Cybersecurity Risks and Controls

- 4.1 Understanding Security Controls and IT Risk: Part 1 91
- 4.2 Understanding Security Controls and IT Risks: Part 2 94
- 4.3 CIA Triad 98
- 4.4 Applying Controls 102
- 4.5 Cybersecurity Threats: Part 1 106
- 4.6 Cybersecurity Threats: Part 2 112
- 4.7 Cybersecurity Vulnerabilities: Part1 115
- 4.8 Cybersecurity Vulnerabilities: Part 2 118
- 4.9 Adverse Impacts 123
- 4.10 Risks and Controls – Putting It All Together 127

Module 5: Securing the Layers

- 5.1 Physical Security 137
- 5.2 Endpoint Security 140
- 5.3 Network Security: Security Architecture 142
- 5.4 Network Security: Firewalls 145
- 5.5 Network Security: Anti-Virus/Anti-Malware 148
- 5.6 Network Security: Segregation 150
- 5.7 System Security: Servers 152
- 5.8 Platform Security 155
- 5.9 Product Security: Threat Models 158
- 5.10 Product Security: Embedded Systems 161
- 5.11 Product Security: Internet of Things 163

Module 6: Data Security

- 6.1 Data Security At Rest: Information Classification & Categorization 167
- 6.2 Data Security In Transit: Encryption and Keys 170
- 6.3 Data Security In Transit: SSL/TLS 173
- 6.4 Data Security In Transit: Digital Signature and Identification 175

Module 7: User Access Control

- 7.1 Directory Management 181
- 7.2 Authorization 185
- 7.3 Authentication and Access Control 188
- 7.4 Privileged Account Management 192
- 7.5 Users and Security Awareness 195

Module 8: Solution Delivery

- 8.1 SDLC and Solution Security Planning 199
- 8.2 Requirements and Security Engineering 202
- 8.3 Requirements and Solution Development 205
- 8.4 Solution Security: Applications 208
- 8.5 Solution Security: Databases 211
- 8.6 Solution Security: Web 214
- 8.7 Change Impact Analysis 217

Module 9: Operations

- 9.1 Incident Response, Recovery, and Remediation 223
- 9.2 Metrics and Reporting 228
- 9.3 Risk Logging and Mitigation Tracking 231
- 9.4 Operational Risk Ownership 234
- 9.5 Computer Forensics: SOC, SIEM 236
- 9.6 Future Proofing your Security Posture 239



Module 1: Introduction to Cybersecurity Analysis

1. IIBA and IEEE Perspective: Overview of Concepts and Approach to Improving Cybersecurity
2. Importance of Security
3. IT Functions & Roles
4. IT 101 - 1: The Pieces
5. IT 101 - 2: Using & Managing the Pieces
6. IT 101 - 3: Advancement
7. The Role of Business Analysis in Cybersecurity
8. Governance Perspectives of Cybersecurity

1.1

IIBA and IEEE Perspective: Overview of Concepts and Approach to Improving Cybersecurity

1. Overview
2. BA Work Practices
3. Enterprise Level Perspective
4. Infrastructure & Technical Considerations
5. Solution Perspectives
6. Operations Security Considerations
7. General Approach
8. Summary

1.1.1 Overview

- Cybersecurity Imperative
 - The expansion of technology in our business and in our lives has made cybersecurity a top of mind concern for enterprises, government, and individuals.
- IIBA Perspective
 - Governance and Risk
 - Infrastructure and Networking
 - Applications and Information integrity
- Business Analysis (BA) Focal Points
 - Analysis is the basis of planning and preparation for a secure cyber environment.
 - Business Analysis is about understanding the requirements, the value, and in cybersecurity context it is about building in not bolting on security into everything we work on.

1.1.2 BA Work Practices

IIBA Perspective

- Governance and Risk
 - Understanding the enterprise environment is critical
 - BAs work with the business, the architects, the security specialists in establishing the security framework and governance processes; this requires very senior BA task involvement
- Infrastructure and Networking
 - Key in every enterprise – BA's work in generally traditional way to go between the business and the technical team to assure business needs are effectively part of the requirements and plan and collaborate on key initiatives. BA's also are support to operations
- Applications and Information integrity
 - BAs play a critical role in assuring that the security requirements, the data integrity issues, the interface and integration components, and the functional and non-functional requirements are met. This applies across Agile, DevOps, and SDLC methods. It applies to applications/ solution maintenance and iterations. It applies to making sure the application or solution requirements are met while maintaining overall security controls in this layer. Most BA's will work at this level.

1.1.3 Enterprise Level Perspective

- Understanding the context of the environment and the risk tolerance is a strategic imperative for the analysis approach.
- Key topics
 - Governance of Security
 - Risk Tolerance
 - Compliance

- Privacy
- Digital Rights
- Organization Risk Assessment
- Risk Analysis
- Disaster Recovery and Business Continuity
- Business case Development
- Understanding Security Controls
- CIA Triad – Confidentiality – Integrity – Availability
- Threats and Vulnerabilities
- Impacts

1.1.4 Infrastructure & Technical Considerations

- Securing the Layers
- Physical Security
- Network Security – Architecture, Firewalls , Segregation
- Platforms and Server-Side Security
- Product Security – Embedded Systems, Internet of Things
- Cloud Products
- Overall Threat Models

1.1.5 Solution Perspectives

- Access Controls & Data Level
- Solution Delivery

.1 Access Controls & Data Level

- Data at Rest – Information Classification and Categorization
- Data in Transit – Encryption and Keys
- Directory Management
- Authentication and Access Controls
- Privileged Account Management
- Users & Security Awareness

.2 Solution Delivery

- SDLC and Security Planning
- Requirements Definition and Analysis
- Solution Security – Applications
- Solution Security – Databases
- Solution Security – Web
- Change Impact Analysis

1.1.6 Operations Security Considerations

- Incident alerts, escalation process, roles for response teams
- Incident response, recovery, and remediation
- Risk log and mitigation tracking
- Operational risk management and ownership
- Security operations center concepts and Security information and event management (SIEM)
- Forensics and continuous improvement
- Future proofing your security investment

1.1.7 General Approach

- Topics covered with discrete learning modules – offering training and learning online LMS
- Topics in each module typically include:
 - Key Terms
 - BA Focal Points
 - Use Cases – where this topic applies
 - Related Risks
 - Technology Controls
 - Process Controls
 - Explanations of Key Learnings and important concepts to understand

1.1.8 Summary

- Cybersecurity remains a critical concern for all enterprises and is an essential knowledge area for the business and for all BAs and many other professionals. No longer just a technical skill.
- BAs have an obligation to develop basic knowledge and competency in the effective use of cybersecurity tools and approaches to information and process management.
- IIBA and IEEE have partnered to provide a robust perspective on what the business and the business analyst need to know to be prepared for today's challenges. The training and the certification give everyone the opportunity to learn key concepts needed to perform, and the credibility of a joint certification to demonstrate core competency.
- The information provided is a broad-based set of the basics of cybersecurity designed around the kind of analysis needed to assist in the overall cybersecurity solution, but leverages the collaboration of the business, the analyst, the architects and the technology experts to create a safe and secure cyber environment.

1.2 Importance of Security

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Technology Expertise
7. Process Controls
8. Process Expertise

1.2.1 Business Analysis Practitioner (BA) Focal Points

- Understand the importance of security; importance of protecting networks, systems, data and information.
- Understand the risks associated with cyber-attacks, identity and data theft, loss or disruption of services, communication, systems and infrastructure.
- Recognize industry-wide standards and practices to assess and minimize risk.
- Identify government and non-governmental organizations engaged in establishing security standards, as well as sources of guidelines and frameworks for securing our systems.
- Become familiar with the effects of well-known cyber-attacks; with historical, precedent-setting incidents and events.

1.2.2 Key Terms and Definitions

- **Breach:** Any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters a private, confidential or unauthorized logical IT perimeter.¹
- **Hacking/Hacker:** An unauthorized user who attempts to or gains access to an information system.²
- **Threat:** Refers to anything that has the potential to cause serious harm to a computer system.³

1.Techopedia.com. Definition - What does Security Breach mean?. <https://www.techopedia.com/definition/29060/security-breach>.

2.National Initiative for Cybersecurity Careers and Studies (NICCS). *NICCS Glossary*. <https://niccs.us-cert.gov/about-niccs/glossary>.

3. Goswami, Rajendra, Samarth Sharma, Charanjeet Singh Chawla, and Jeetendra Pande. *Cyber Attacks and Counter Measures: User Perspective*. Uttarakhand Open University, Haldwani. 2016.

- **Phishing:** The fraudulent act of acquiring private and sensitive information, such as credit card numbers, personal identification and account usernames and passwords. (Pronounced like “fishing”).¹
- **Identity Theft:** The unauthorized collection of personal information and its subsequent use for criminal reasons such as to open credit cards and bank accounts, redirect mail, set up cellphone service, rent vehicles and even get a job.²
- **Exploit:** A general term for any method used by hackers to gain unauthorized access to computers, the act itself of a hacking attack, or a hole in a system's security that opens a system to an attack.³
- **Ransomware:** Using malware to lock up a set of computer files and asking for payment to the offender to undo the malware control of the computer files. (analogy to kidnapping and ransom).

1.2.3 Use Cases

- Businesses can incur huge fines for failing to protect and handle data effectively.
- The European Union’s General Data Protection Regulation (GDPR) has introduced new fines that will be a minimum of €20 million, or 4% of the business’ annual turnover, whichever is the greatest.⁴
- In a connected world, we each have a responsibility to protect ourselves and the people we interact with.
- As the rate of cyber-attacks continues to increase, the damage they cause to individuals, governments and private companies is also increasing.
- In a 2018 Cybersecurity Ventures report on cybercrimes, the firm projects that:
 - the cost of cyber threats will rise to \$6 trillion annually by 2021⁵
 - by 2020, a business will fall victim to a ransomware attack every 14 seconds⁶
 - the FBI estimates that the total amount of ransom payments approaches \$1 billion annually⁷

1. Billingsley, Luanne. *Cybersmart: Protect the Patient, Protect the Data*. Journal of Radiology Nursing Volume 38, Issue 4. Elsevier Inc. December 2019. <https://www.sciencedirect.com/science/article/abs/pii/S1546084319301737?via%3Dihub>.

2. Techopedia.com. Definition - What does Identity Theft mean?. <https://www.techopedia.com/definition/13637/identity-theft>.

3. Techpanther. *All about Ethical Hacking*. Techpanther. October 2017. <https://www.techpanther.in/2017/10/all-about-ethical-hacking.html>.

4. The European Centre of Technology. *The Importance of Cyber Security*. <https://theect.org/importance-cyber-security/>

5. Seetharaman, R. *Risk integration is key to better cybersecurity management*. Gulf Times. February 23 2019. <https://amp.gulf-times.com/story/623073/Risk-integration-is-key-to-better-cybersecurity-ma>.

6. Cybersecurity Ventures. Annual Cybercrime Report. Cybercrime Magazine. 2019. <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016>.

7. Ibid.

- Increasing threats, severity of attacks and future outlook suggest we are no longer asking why cybersecurity is important, rather what do we need to do to protect our assets, information, infrastructure, customers and ourselves.
- Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.¹
- The cybercrime epidemic has escalated rapidly in recent years, while companies and governments have struggled to hire enough qualified professionals to safeguard against the growing threat. This trend is expected to continue into 2019 and beyond, with some estimates indicating that there are some one million unfilled positions worldwide (potentially rising to 3.5 million by 2021).²

1.2.4 Related Risks

- Every aspect of our lives is jeopardized by hackers who are targeting the following:
 - Personal information and identities
 - Customer data
 - Intellectual property
- Bad agents are continually attempting to perform the following illegal and harmful activities:
 - Damaging infrastructure
 - Interrupting communications
 - Holding data hostage for ransom
 - Engaging in political and social disruption

1.2.5 Technology Controls

- Advanced Fraud Detection
- Cloud Security
- Data and Application Security
- Endpoint Security
- Identity and Access Management
- Mobile Security
- Network Security
- Security Analytics
- Threat Intelligence

1. Seetharaman, Dr. R. *Risk integration is key to better cybersecurity management*. Gulf Times. February 2019. <https://desktop.gulf-times.com/story/623073/Risk-integration-is-key-to-better-cybersecurity-ma>.

2. Morgan, Steve. *Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021*. Cybersecurity Business Report. CSO. June 2017. <https://www.csoonline.com/article/3200024/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html>.

1.2.6 Technology Expertise

- Foundational knowledge of most common forms of security threats and attacks.
- Awareness of potential risks associated with various types of security threats.
- Knowledge of the most effective security controls: inventory management, patch management, continuous vulnerability assessment, secure baseline configuration management, controlled use of administrative and least privileged access.
- An understanding of the benefits and importance of perimeter security fundamentals, strategies and systems: firewalls, radius servers, intrusion detection, intrusion prevention, antivirus, anti-malware, virtual private networks, content filtering and white listing.

1.2.7 Process Controls

- Security and cybersecurity framework
- Governance and risk management system
- Enterprise IT and Technology Security Standards
- Enterprise risk assessment
- Network logging and monitoring
- Asset logging and monitoring
- Enterprise business continuity and recovery plan
- Security Incidence response capability
- Employee education and information program

1.2.8 Process Expertise

- BA should acquire working knowledge of the key areas of the below list of process areas:
 - Understand current industry standard practices in cybersecurity, as well as local government policies and global or national standards in the practice of cybersecurity.
 - Understand the national level efforts which are intended to reduce threats and issues related to cybersecurity such as those provided by NIST (in the USA), and other similar government agencies.
 - Understand the key elements of understanding the organization's strategy and risk tolerance, and able to develop risk and threat assessment support for the governance process.
- BA should have working knowledge of the data and application environment, as it fits within the infrastructure, network, and ecosystem of data relationships for the organization. This should be specific to the assigned project initiative area and its overall context of the organizations environment.

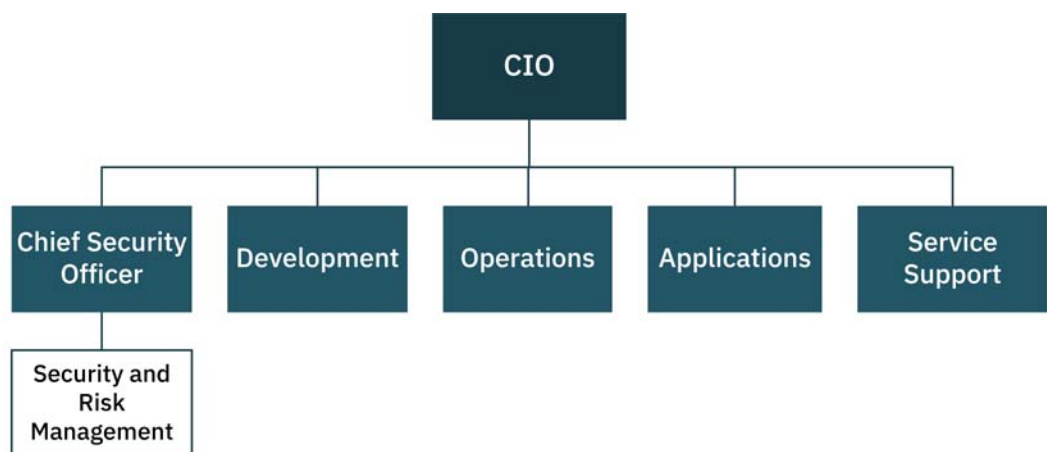
1.3 IT Functions & Roles

1. Introduction
2. Business Analysis Practitioner (BA) Focal Points
3. IT Leadership
4. Architecture and Design
5. Project Management Office (PMO)
6. Quality Assurance and Testing
7. IT Operations
8. Service Management and Support
9. IT Application Support
10. IT Security and Risk Management

1.3.1 Introduction

- BAs who have not worked in an IT field, or whose experience is not with a large, mature IT business, will need to understand the functions and responsibilities of the IT teams in order to perform effectively in the cybersecurity space.
- Of course, not all IT departments are alike, and range in size and capabilities. This module intends to cover common IT roles with which the BA would typically interact.

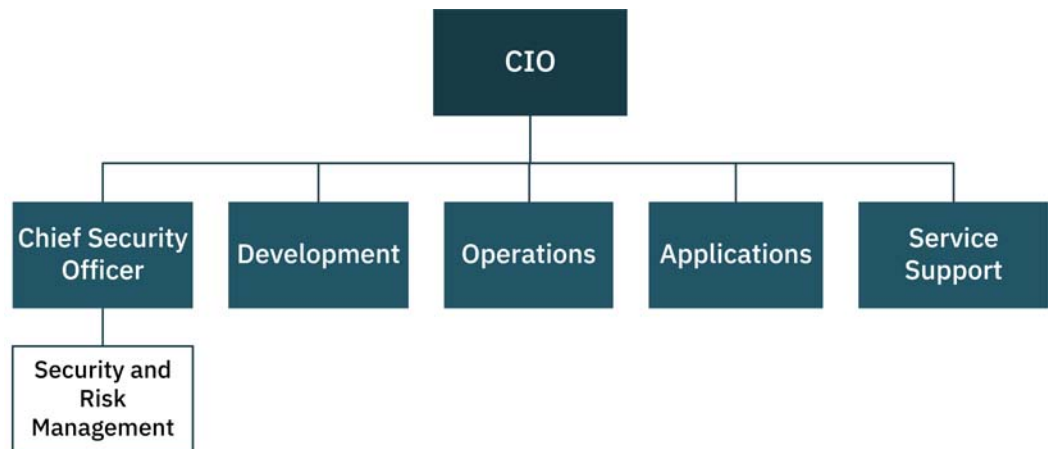
1.3.2 Business Analysis Practitioner (BA) Focal Points



- BAs are the link between the business and technology. In a cybersecurity setting from an infrastructure perspective, the business in the most direct sense, is IT, which means the IT departments are your clients.
- BAs are also the first line of defense when protecting data assets and are involved with eliciting the rules to manage data assets.

- The BA's domain can range from being highly technical to being business focused depending on the nature of their assignment. There can be a steep learning curve depending on your background, experience and the related industry.
- Although cybersecurity may be considered by many as an “IT Security’s job”, it is in fact everyone’s responsibility, particularly those in IT.
- The BA working in cybersecurity must understand how cybersecurity plays a role in each of these departments’ services.

1.3.3 IT Leadership



- An IT department may be known as a variety of names, including Information Systems (IS), Information & Communications Technology (ICT), to name a few. All organizations’ IT departments will be unique to that business, and they come in all shapes and sizes.
- At the top level of an IT service may be a Chief Information Officer (CIO), or a Vice President, or a Director, if the organization is very small; larger organizations will have these and possibly more levels of accountability in their IT organization structure.
- The highest level would typically report to the CEO, President, or the highest leader in the company; or, sometimes IT is grouped with Finance and so would fall into that reporting structure.
- Services delivered by IT departments, and the teams within them, may be outsourced in part or in whole depending on the business case of the organization’s IT model. For this learning module we will describe just one simple example of an IT department, organized as shown in the chart above.

1.3.4 Architecture and Design

- How architecture and design are actually used varies by enterprise. The notion of architecture generally refers to the set of capabilities that the enterprise needs to achieve its business/organization objectives. Within the cyber security space, this covers the areas of traditional Information Technology as well as the entire spectrum of the component level of the systems for use in an enterprise.

- Overall architecture operations at the strategic level, rather than at a specific application or component level, and deals with how the enterprise uses those components.
- There are many forms of enterprise architecture and one of the most common is TOGAF. TOGAF defines high level architecture as:
 - The Business Architecture defines the business strategy, governance, organization, and key business processes.
 - The Data Architecture describes the structure of an organization's logical and physical data assets and data management resources.
 - The Application Architecture provides a blueprint for the individual application systems to be deployed, their interactions, and their relationships to the core business processes of the organization.
 - The Technology Architecture describes the logical software and hardware capabilities that are required to support the deployment of business, data, and application services. This includes IT infrastructure, middleware, networks, communications, processing, standards, etc.¹
- Security Architecture is across all of these elements of Architecture as discussed in the balance of this set of materials. Design covers the structure in which the architecture crosses all elements with specific considerations of the components, systems and networks of a particular organization and its initiatives.

1.3.5 Project Management Office (PMO)

- In some organizations, the resources of project management may be managed in a central group for the organization. It would typically include any organizational standards of practice, and would likely manage the repository of tools, templates, and examples of project management artifacts. It may also house the human resources for some of all of the project managers, and project administrators.
- Some organizations are moving to Agile and may keep a PMO structure, or it may move to a broader concept consistent with Agile. In many organizations the Project Managers will work across all elements, but often the PMO is working with the business applications layer, and may include Business Analysts. The organizational structure may be of value in an organization, but is only one of many organizational approaches which will impact cybersecurity.
- BA's need to engage with cybersecurity considerations regardless of organization structure to assure that the technical experts, Scrum Masters, Project Managers, Architects and Process Designers and Data Analysts are united in their approach to solving problems with deep consideration for the 'non-functional' requirements of the need for cyber security controls.

1.The Open Group. *Open Group Architecture Framework (TOGAF)*. Van Haren Publishing. April 2018.

1.3.6 Quality Assurance and Testing

- Any product or change being introduced into production through IT must be tested to ensure functionality, satisfaction of requirements and that it fulfills its business purpose. This role is owned by Quality Assurance, or Testing. Large teams are led by test leads and executed by testers. These roles work very closely with the BA to understand traceability to requirements. Security testing must be included where appropriate to ensure the product not only meets functional needs but is secure.
- For a delivery, a Test Strategy would typically be created, followed by a Test Plan, as more information is available by the project team. Lastly, test cases or test scenarios are created which are executed by testers before the product can be approved for handover to operations.
- Types of testing may include:
 - Default Scenario (Happy Path) Testing and Alternate or Exception Path Testing
 - Regression Testing
 - Integration Testing, Performance Testing, High Availability (fail-over) Testing
 - System/End-to-end Testing
 - User Acceptance Testing

1.3.7 IT Operations

- Operations is responsible for “keeping the lights on”; ensuring that the technology used by the business to operate, is available.
- Some key functions performed by IT Operations include:
 - Provisioning of personal computers and mobile devices
 - Maintaining infrastructure
 - Change management
 - Service support/incident management
 - Network and firewall security management
 - Directory management and access control
 - Asset management
 - Maintaining databases

1.3.8 Service Management and Support

- Service Management for IT (ITSM) includes the discipline of the consistent reporting, tracking and resolving of service requests and problem tickets. In terms of cybersecurity, security breaches are often first reported to the Service Desk, so that a defined problem resolution process can be executed by the appropriate staff and systems.
- In practice, a common method for delivering ITSM is with a standard operation framework known as ITIL. ITIL describes a process for managing service management in the IT area. ITIL and service management in general attempts to meet the business needs with a value based approach with matching service delivery.

1.3.9 IT Application Support

- Business applications used by employees across the organization require support. They may fail due to software bugs, known defects, integration issues, or any number of causes.
- This team is tasked with ensuring that application-specific problems that negatively affect users from performing their work within their application are dealt with in a timely manner.
- Resources in this group require training and/or experience with the application(s) for which they provide support. Some key functions performed by this team include:
 - Fixing defects in the way the application is intended to work
 - Making code changes or modifying the look and feel of the application user interface
 - Implementing upgrades and patches as they are issued by the application developer/vendor
 - Creating custom reports required by users or management
 - Performing data analysis for the business application owner
 - Assisting end-users with day-to-day tasks within the application
 - Application level security management

1.3.10 IT Security and Risk Management

- The Security and Risk Management Team takes a leadership role in IT in the protection of information assets across the organization. Although every employee has a responsibility to practice secure behaviours when it comes to their interactions with data and systems, this team is responsible for protecting the networks, infrastructure and systems, identifying and quantifying potential security and cyber risks and threats, informing the business of their choices in terms of managing identified risks, and providing expertise to their IT counterparts in all technology initiatives and operations.
- Key functions and services managed, often with outsourced assistance, include:
 - Threat Risk Assessments, Vulnerability Scans and Assessments, Penetration Testing
 - Information Risk Planning and Management
 - Compliance and Audit Management, Internally and Externally
 - Incident and Event Monitoring and Forensics
 - Inspection and Maintenance of Security Technology and Systems
 - Developing and Managing Security and Risk Policies, Procedures, and Processes
 - Building Security Awareness across the organization
- The IT Security and Risk Management team interacts with both business and technical leadership.

Introduction to IT 101

Recognizing that not all BAs come from an IT background, we created these three IT 101 modules to provide learners with a high level, basic introduction to some of the key IT concepts that are important to be familiar with when performing business analysis in cybersecurity.

The modules are roughly divided into three sections, and each section ends with a few words on how the concepts introduced are relevant to the BA in cybersecurity. The sections are:

- IT 101 - 1: The Pieces (p. 14)
- IT 101 - 2: Using & Managing the Pieces (p. 18)
- IT 101 - 3: Advancement (p. 24)

1.4 IT 101 - 1: The Pieces

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Data Centers and Networks
4. Servers and Clients
5. Types of Servers
6. Platforms
7. Layers: The OSI Model

1.4.1 Business Analysis Practitioner (BA) Focal Points

- Key terms and concepts that a BA working in cybersecurity will encounter regularly.
- Understand the terms related to IT infrastructure and hardware, and how it all fits together to enable organizations to conduct business.
- Understand external and internal networking to form a foundation for learning how to secure both against cyber threats.
- Understand how information is stored and shared and how that creates vulnerabilities.
- Understand some of the physical technology constraints and considerations a BA must navigate within, in a cybersecurity context.

1.4.2 Key Terms and Definitions

- **Information System:** Describes the collection, validation, storage, calculating, sorting and transmission of data across an organization.
- **Application:** Describes how a computer program is used to accomplish a specific business function in an organization. A group of applications can define an information system.
- **Database:** Information which is stored in a defined computerized structure to facilitate storage and retrieval of data. Most modern databases use a 'relational model' such as SQL to store data in two dimensional tables, and link these tables. This is where the data is structured and can fit into defined cell structures within the tables.
- **Database Application:** The database application is the linking of the technology of a database with the programming of an application to handle logic and rules for how the data is to be processed and may include reporting, or passing along to other applications for additional uses.
- **IT Infrastructure:** This describes the computer hardware, such as servers, storage devices, network interfaces, network routers, necessary peripheral devices and appliances to do the necessary processing, storage and transmission of information.

1.4.3 Data Centers and Networks

- **Data Center:** where the primary computing power for a local organization is placed and protected with physical security to control entry, to protect equipment from heat and fire and other local hazards.
- **Central Data Center:** Some organizations may employ multiple data centers and will most often align to the natural organization structure. Many organizations may choose only one single data center, and others may have several in divisional areas, and consolidate data as needed to the central data center. Generally all data centers have a network of devices attached for user interface devices, such as PC's and laptops. They may also have devices, such as lab equipment or manufacturing devices attached for monitoring and control.
- **Network:** computer network or data network refers to the wiring or wireless capability to connect devices to the local network, the wide area network, or the internet backbone. Networks may connect data centers, and may allow integration to third party computing services such as the cloud based systems. Networks allow for secure access and compress data and potentially encrypt data for transmission to the destination location.

1.4.4 Servers and Clients

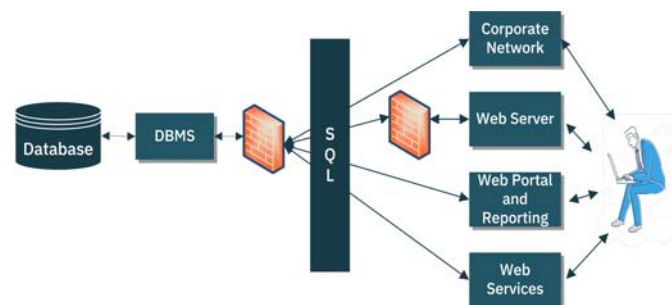
- A client computer is typically a device such as a PC or laptop which is operated by a user. Certain computing functions are best handled at the client level such as graphical presentation and basic information edit rules on an application presentation form.
- Servers are larger computers typically found in a data center, which take in transactions from clients and process the requests to the right

computing element for the application form, and will handle the processing logic and the database storage and retrieval functions.

- A Client-Server computing model allows client computers to request services from the shared resources of a server. This allows for processing and storage optimization of an application, with centralized control of the data storage and its security.

1.4.5 Types of Servers

- The most common form of servers (which can be physical, or logical) in the application area are:
 - Web Server: the web server handles application requests from a client with an HTTP interface to move information and send and receive information for intake to the service to push out information to the client. HTTP describes to the server and the client how to deal with the information exchange.
 - Application Server: The application server handles the processing logic on the data received from the client and from the database and applies the programming logic rules to the data. The application server holds the primary logic for processing data fields and tables.
 - File Server (database server): The file server stores and retrives information and optimizes the input and output logic for storage in a defined file structure. The file server handles the data handling needs of one or several applications or application servers.
 - Directory Servers: The servers are intended to manage the user accounts and which resources are available to any given user, such as which application they are allowed to use, the specific privileges they have within an application (which transactions they can perform), and what files they can access. This server is a core component of the cybersecurity control process.

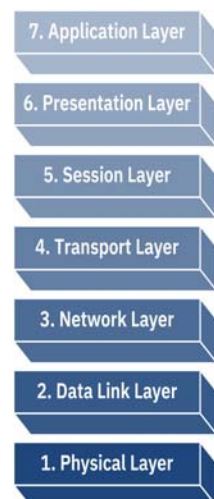


1.4.6 Platforms

- A computer is made up of several parts including the processor, memory, disc/data storage, network interface, power supply, and other components.
- The computer platform is controlled by software which is referred to as the operating system. The operating system on a typical personal computer is Microsoft Windows or Apple IOS while on a server that may be Unix or Windows Server. Virtualization software such as VMware is also able to share computing resources and create virtual machines within a single computer device.
- Platform as a Service: PaaS is a way that the entire environment can be shared in the cloud. This means that the computing platform lives outside a customer premise and often it provides specialized software services. A cloud based shopping cart experience may be considered a PaaS when combined with a cloud based buyer-connecting seller platform. Some computing platforms are more comprehensive and cover all the infrastructure components, and are referred to as Infrastructure as a Service (IaaS) or if just a single application with defined functionality in software is referred to as Software as a Service - SaaS.

1.4.7 Layers: The OSI Model

- The International Standards Organization (ISO) developed the Open Systems Interconnection (OSI) model. It divides network communication into seven layers.
- Layers 1-4, the “lower layers” mostly concern themselves with moving data around.
- Layers 5-7, the “upper layers”, contain application-level data.
- Networks operate on one basic principle: "pass it on." Each layer takes care of a very specific job, and then passes the data onto the next layer.



1

1. International Organization for Standardization (ISO). *ISO 35.1: Open Systems Interconnection (OSI)*. International Organization for Standardization (ISO). <https://www.iso.org/ics/35.100/x/>.

Re-introduction to IT 101

Recognizing that not all BAs come from an IT background, we created these three IT 101 modules to provide learners with a high level, basic introduction to some of the key IT concepts that are important to be familiar with when performing business analysis in cybersecurity.

The modules are roughly divided into three sections, and each section ends with a few words on how the concepts introduced are relevant to the BA in cybersecurity. The sections are:

- IT 101 - 1: The Pieces (p. 14)
- IT 101 - 2: Using & Managing the Pieces (p. 18)
- IT 101 - 3: Advancement (p. 24)

1.5 IT 101 - 2: Using & Managing the Pieces

1. Business Analysis Practitioner (BA) Focal Points
2. Communication and IP
3. Systems Development
4. Waterfall and Agile Software Development
5. Deployment Environments
6. ITIL: Information Technology Infrastructure Library
7. Patch and Release Management
8. Web Applications

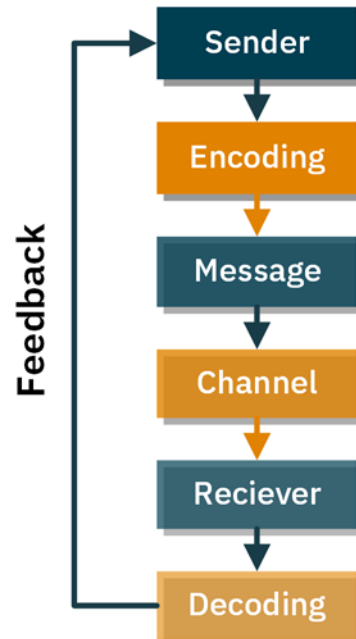
1.5.1 Business Analysis Practitioner (BA) Focal Points

- Understand the moving parts of IT, and how they integrate and relate.
- Understand how electronic communication occurs.
- Understand the ongoing operation and maintenance of technology solutions.
- Begin to see how information systems and applications present specific cyber threats and concerns that a BA will need to consider.

1.5.2 Communication and IP

- The client-server computing model allows client computers to request services from the shared resources of a server. These messages form the communication mechanism, whereby the server returns a response to the client's request, or command.

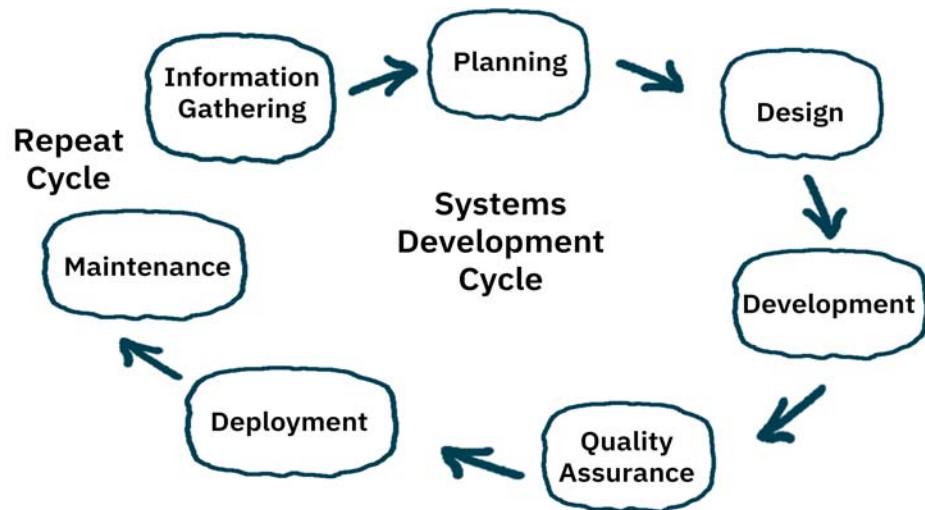
- To communicate, the interacting computers must use a common language and follow the same rules; these are defined in what is called the communication protocol.
- When it comes to transmitting packets of information (requests and responses) across network boundaries, the Internet Protocol (IP) is principally used. The internet is the product of the working of all these routings.
- Each sending and receiving computer entity within the network has a unique IP address, used to identify the source and destination of the communication packet.



1.5.3 Systems Development

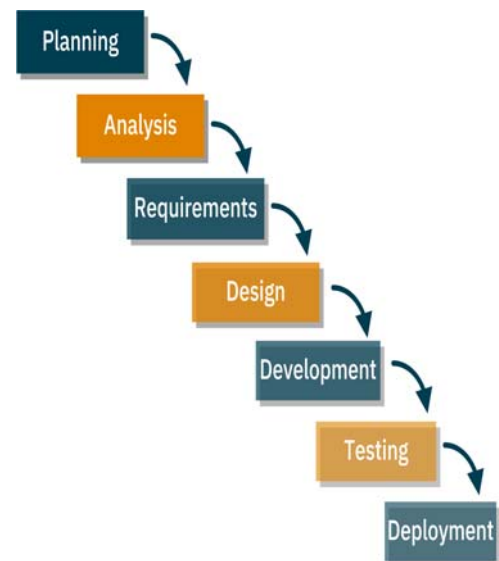
- Systems development is the process for identifying business problems, defining business requirements, defining system requirements and solution options. By following systems selection methodology we can decide whether we want to buy commercial-off-the-shelf (COTS), build (App/Dev) or rent (SaaS).

- The BA includes non-functional requirements such as cybersecurity throughout the development process phases of elicitation, planning and design.

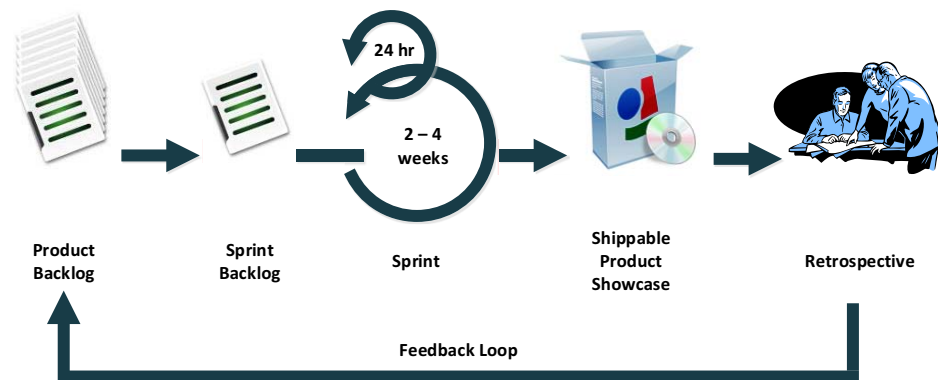


1.5.4 Waterfall and Agile Software Development

- Waterfall software development assumes the majority of the planning is done and complete before the construction period is initiated and that change is then handled by change orders. In a system development life cycle it appears to be predominately linear in the stages of the work process flow. In the sense of cybersecurity there is some reasonable belief that some amount of security planning is needed up-front as part of a description of the non-functional requirements of the initiative.



- Agile is a mindset which is iterative rather than linear. The work effort starts with a general description of solution outcomes and a clear value statement rather than with detailed requirements and design. The requirement details and design are progressive with each iteration. The outcome of each iterative cycle emphasizes workable product as a priority over written artifacts. This mindset has shown to increase the time to market for many (not all) initiatives. Common specifics in this area include SCRUM, KANBAN, and Lean.¹



1.5.5 Deployment Environments

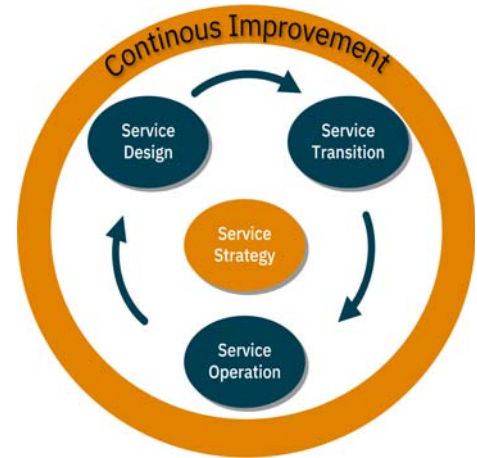
In software deployment, a staged approach is used to ensure proper quality assurance can be performed depending on the type of solution. A common four-tier architecture is development, testing, staging, production (DEV, TEST, STAGING, PROD), with software being deployed to each higher environment, in order. Other potential environments include Training, Sandbox, Integration, etc.

- DEV: the environment used by developers to unit test functionality. Often scrubbed or obfuscated data for security purposes.
- TEST: an integrated environment used to ensure modules interact with each other and used for more comprehensive testing such as integration or performance testing. Often scrubbed or obfuscated data for security purposes.
- STAGING: an environment also known as pre-prod used to ensure merging with production systems can be performed successfully. May have full volume or production data to ensure functionality.
- PROD – the production or live environment where all live data and systems inter-operate. Requires implementation of all security controls.

1. International Institute of Business Analysis. *Agile Extension to BABOK Guide® version 2*. IIBA. 2017.

1.5.6 ITIL: Information Technology Infrastructure Library

- ITIL is a standard of best practices for IT Service Management.
- ITIL generally breaks down the engagements as:
 - Service Strategy
 - Service Design
 - Service Transition
 - Service Operation
 - Continuous Improvement



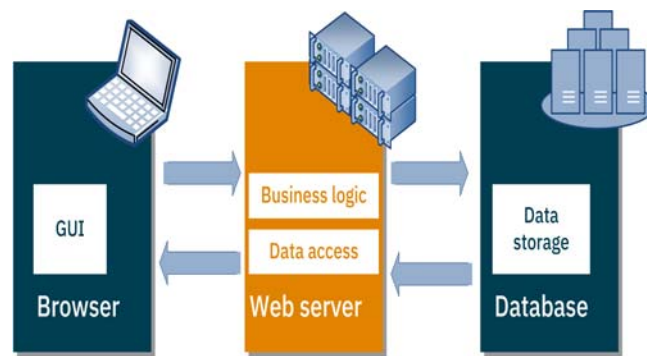
1.5.7 Patch and Release Management

- Patch Management: The term 'patch' generally refers to a set of software intended to update the software (code), and may fix known problems, or improve security vulnerabilities that have been identified. A patch can be applied to the operating system of the computer, to an application program, or even to devices using custom software. Patches may come from the commercial software vendor or they may be developed by the internal development team.
- Release management: this term takes software patches and other software improvements, such as user maintenance service tickets, and takes them through a validation process prior to releasing them to the production environment. As part of release management, the validation process would include defined testing approach, user acceptance in some cases, and the necessary planning to manage changes to impacted users.

1.5.8 Web Applications

- Web application refers generally to any application which is invoked through the client via a web browser. Typical web browsers include Microsoft Edge (or Explorer), Google Chrome, FireFox, and others. The browser handles the presentation layer and forms which in turn communicate to a central service, such as an application server, and a database server.
- Web applications have some well known security vulnerabilities, and often require that the client have anti-virus software installed locally to protect the browser from the several known types of cyber attacks at the local level. The server side also needs cyber protection software installed to monitor for code level threats. All devices require regular patch

updates to defend ever evolving anti-virus and malicious software threats.



Re-introduction to IT 101

Recognizing that not all BAs come from an IT background, we created these three IT 101 modules to provide learners with a high level, basic introduction to some of the key IT concepts that are important to be familiar with when performing business analysis in cybersecurity.

The modules are roughly divided into three sections, and each section ends with a few words on how the concepts introduced are relevant to the BA in cybersecurity. The sections are:

- IT 101 - 1: The Pieces (p. 14)
- IT 101 - 2: Using & Managing the Pieces (p. 18)
- IT 101 - 3: Advancement (p. 24)

1.6 IT 101 - 3: Advancement

1. Business Analysis Practitioner (BA) Focal Points
2. Information Management
3. Cloud Computing
4. Hosting: Cloud vs On-Prem
5. Managed Services vs SaaS
6. Digitization and Digitalization
7. Business Intelligence and Analytics
8. Internet of Things

1.6.1 Business Analysis Practitioner (BA) Focal Points

- Understand how technology not only supports business but enables growth and improvement.
- Understand some of the key trends and advancements in IT, and terms that will be used as the BA engages in cybersecurity initiatives.

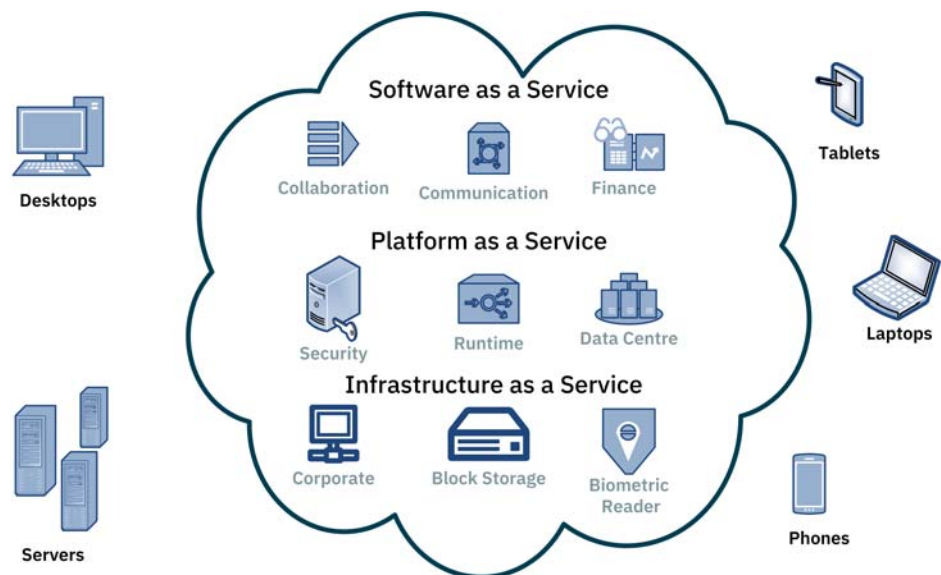
1.6.2 Information Management

- Information management (IM):
 - the acquisition of information from one or more sources,
 - the custodianship and the distribution of that information to those who need it, and,
 - its ultimate disposition through archiving or deletion.¹
- is closely related to, and overlaps with, the management of data, systems, technology, processes and strategy
- involves a variety of stakeholders, who might have rights to originate, change, distribute or delete information according to policies
- Information gains value when presented to those with organizational roles or functions that depend on it and can put that information to use.



1.6.3 Cloud Computing

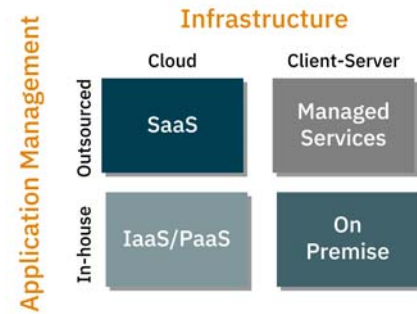
- Cloud computing:
 - enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the internet
 - relies on sharing of resources to achieve coherence and economies of scale



1.Crawlist. *Top 10 best Information Management solution*. April 2019. <http://www.crawlist.net/2019/04/top-10-best-information-management.html>.

1.6.4 Hosting: Cloud vs On-Prem

- On-premises software ("on-premise" or "on-prem") is installed and runs on computers on the premises (in the building) of the organization using the software, rather than at a remote facility such as a server farm or cloud.
- Off-premises software is commonly called "software as a service" ("SaaS") or "cloud computing".



1.6.5 Managed Services vs SaaS

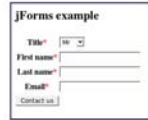
- Managed or Outsourced services provider:
 - an IT services provider that manages and assumes responsibility for providing a defined set of services to its clients either proactively or as the provider determines that services are needed.
 - the client and the provider are bound by a contractual, service-level agreement that states the performance and quality metrics of their relationship.
- Software as a service (SaaS):
 - A software licensing and delivery model in which software is licensed on a subscription basis.
 - is centrally hosted and delivered to an end user from a cloud environment.
- Because SaaS applications aren't sold as software packages for download or purchase, users don't buy licenses or upgrades. Instead, they pay a flat, usually monthly, subscription fee. The software resides on the host server from which all users, no matter their organization, access it.

1.6.6 Digitization and Digitalization

- Digitization is the process of making all analog (manual) business information available and accessible in a digital format.

- Digitalization is the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business.

Digitization



- Making analog or print into a digital format such as with scanning, or moving paper forms to online.

Digitalization



- Using digital technologies to change the business model. Examples include Amazon, Uber, apps for insurance claims process, etc.

1.6.7

Business Intelligence and Analytics

- Business Intelligence (BI)
 - strategies and technologies used by enterprises for data analysis of business information
 - provides historical, current and predictive views of business operations
 - combines market (external data) with internal company data, creating an "intelligence" that cannot be derived from any singular set of data
 - handles and allows for easy interpretation of large amounts of structured or unstructured data, to:
 - empower organizations to gain insights and help identify and create new markets and strategic business opportunities
 - assess demand and suitability of products and services for different market segments
 - gauge the impact of marketing efforts
- Common functions include: reporting, online analytical processing, analytics, data mining, process mining, complex event processing, business performance management, benchmarking, text mining, predictive analytics and prescriptive analytics, operational and strategic business decision support.

1.6.8

Internet of Things

- The network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data.
- Each thing is uniquely identifiable through its embedded computing system but can inter-operate within the existing Internet infrastructure.
- Allows objects to be sensed or controlled remotely across existing network infrastructure.
- Creates opportunities for more direct integration of the physical world into computer-based systems.
- Results in improved efficiency, accuracy and economic benefit in addition to reduced human intervention.

1.7 The Role of Business Analysis in Cybersecurity

1. Overview
2. Business Analysis Practitioner (BA) Focal Points
3. Defining Cybersecurity
4. Use Cases
5. Strategic and Tactical Roles
6. Operational Roles
7. Technology Expertise
8. Process Expertise

1.7.1 Overview

A Guide to the Business Analysis Body of Knowledge® (*BABOK® Guide*) defines Business Analysis as the practice of enabling change in an enterprise by defining needs and recommending solutions that deliver value to stakeholders.

BAs in the IT industry are the interface between business and technology; we are interpreters and translators. A BA can work in cybersecurity in a number of possible capacities:

- introducing new security services/processes/technology via projects;
- supporting security operations;
- as a BA outside security (even outside IT) who must engage with the IT Security team and operate within security frameworks/requirements.

In this environment, the 'Business' or the most immediate client is IT, so it is more technical than other business stakeholder groups. The BA needs to be able to create Requirements around the application they are working on, and to work with the appropriate security expert to ensure the requirements and voice of the business are well understood and built into solutions.

1.7.2 Business Analysis Practitioner (BA) Focal Points

- The business analysis tools, techniques, tasks, practices and competencies discussed in the *BABOK® Guide* and throughout the six Knowledge Areas, are relevant and applicable in cybersecurity. Unlike specialty areas such as Agile, gaining the cybersecurity knowledge to work in this area does not require an add-on to the *BABOK® Guide* of more tools, techniques, tasks, etc.; they are all needed.
- The difference with cybersecurity is that it is very specific, technical subject matter and context, with which the skills and techniques would be executed.

- What sets the subject of cybersecurity apart from other business areas in which BAs practice is that a working, technical understanding of the business itself is critical.

1.7.3 Defining Cybersecurity

- Cybersecurity: The protection of computer networks and data from various of electronic and digital threats.
- Network protection:
 - prevents attacks that deny users access to the business's computer resources such as servers
 - extends to shielding the business from intrusions and use of the network for unauthorized purposes
- Data protection: Safeguarding the privacy of an organization's data, which often contains customer information that would be harmful in the wrong hands.
- Business organizations apply cybersecurity by adopting and using policies, tools, and practices directed towards the prevention of cyber-attacks.¹
- The role of the business analyst in cybersecurity is primarily to ensure that the business properly adopts and employs those policies, tools, and practices.

1.7.4 Use Cases

- Requirements gathering and analysis:
 - business, solution, security, trust requirements
- Event root cause analysis and process/system redesign
- Project delivery:
 - Business concepts, business cases, information security, operational support, business continuity
- Developing, maintaining, and ensuring compliance to security governance, standards and policies
- Managing audit events and findings; tracking risks and mitigations
- Reporting on operational security issues and metrics
- Leading security awareness activities
- Facilitating and interpreting risk assessments and analysis
- Identification of new technologies, cyber threats, vulnerabilities

1.Barrios, Joe. *Five Key Roles For The Business Analyst in Cybersecurity*. <https://www.joebarrios.com/roles-business-analyst-in-cybersecurity/>.

1.7.5 Strategic and Tactical Roles

- Compliance to policies
 - The organization needs to establish a governance process to manage the risks of cybersecurity, and the BA should provide guidance to represent the requirements of the organization and its relationships with key stakeholders and their interests.
 - The governance process should establish clear policies for use throughout the organization and the BA role should assist in making sure those policies are known and understood by all involved in business/organization initiatives.
- Business Cases and Budgeting
 - The BA is involved in reviewing any business case to assure that adequate solution approaches include cybersecurity and that the funding for meeting policy requirements is part of the business case.
 - For shared cost components, most organizations will allocate those costs either to each project, and charge only direct costs to the project budget. Other organizations will want to totally centralize certain costs such as cybersecurity.
- Security Tools Implementation
 - The BA role here is to define the various stakeholders and determine the needs for the tool assessment. Once selected and installed, the BA would assist in the deployment in working to train the organization in the appropriate use of the tool.

1.7.6 Operational Roles

- Risk Management
 - learn about cyber risks from IT or business process owners
 - keep a risk log to track identified risks along with how the business is mitigating those risks
 - report on risks to executive management on a regular basis
 - determine how to best mitigate those risks, possibly through new requirements or process changes
 - conduct or be part of an impact assessment
 - work with business and technical stakeholders to establish the precise nature of a problem and the amount of resources needed to maintain security
- Incident Recovery: Problem Solving, New Requirements and Processes
 - help devise solutions to fix a breach and make sure the disaster never happens again
 - participate in or lead analysis to see what happened and how to fix the problem
 - create new requirements, and define new processes, policies, procedures, or tools

1

1.Stevenson, Christopher, Andrew Douglas, Mark Nicholson, and Adnan Amjad. *From security monitoring to cyber risk monitoring: Enabling business-aligned cybersecurity*. Deloitte Review issue 19. Deloitte Insights. July 2016. <https://www2.deloitte.com/us/en/insights/deloitte-review/issue-19/future-of-cybersecurity-operations-management.html>.

1.7.7 Technology Expertise

There are some key information technology concepts that are important for a Cybersecurity BA to be effective, and these are covered in more detail in later modules:

- Directory Management
- Networking
- Platforms, Systems, Applications and Databases
- Servers and Communication
- Data Classification, Storage and Retrieval
- Encryption
- Internet, Web and Cloud
- Authentication and Authorization
- Environments
- Digital and Endpoint security

1.7.8 Process Expertise

Similarly, there are some key business practices and processes that the Cybersecurity BA will use, which are also discussed in more detail in later modules:

- Solution and System Development Lifecycle
- Risk Analysis and Management
- Compliance and Auditing
- Roles and Responsibilities of IT
- Governance and Incident Management
- Stakeholder Management including RACI modeling

1.8 Governance Perspectives of Cybersecurity

1. Introduction
2. Governance Levels
3. Use Cases
4. Stakeholder Groups
5. RACI: Responsible-Accountable-Consulted-Informed
6. Considerations
7. Examples

1.8.1 Introduction

- A fundamental task that Business Analysis Practitioners (BAs) perform is Stakeholder Analysis.
- In the cybersecurity domain, depending on the work being undertaken, and where within the organization the work is being performed, those who affect/will be affected by the initiative will vary:
 - Initiatives of an enterprise level will naturally require decision makers and influencers sitting at an executive or senior leadership level.
 - Security strategizing and planning at the infrastructure level may require a higher level of leadership engagement as well, but those in the director and management levels will likely hold much of the accountability and responsibility for these initiatives.
 - In terms of solution delivery and operations, those from the business side as well as more tactical level IT management will be playing more significant roles in application-related projects and day-to-day operational activities.
- Input from security professionals within the organization will be essential at all levels of responsibility.
- The purpose of this module is to provide you with considerations and questions to ask when defining which group or individual(s) must be assigned roles of Responsible for, Accountable for, Consulted on, and Informed of, decisions related to your assignment.

1.8.2 Governance Levels

1. Enterprise-Level Security Governance
 - i. Organizational Risk Assessments and Roadmap
 - ii. Risk Tolerance and Appetite
 - iii. Compliance to Regulations, Laws, Standards
 - iv. Audit
 - v. Internal Policy

2. Infrastructure-Level Security Governance

- i. Physical Infrastructure, Business Continuity and Disaster Recovery
- ii. Network and Perimeter Security: Firewalls, Segmentation
- iii. Remote Access, VPN, Secure Gateways
- iv. IaaS, PaaS

3. Application-Level Security Governance

- i. Hardware and software hosting: cloud solutions vs on-prem
- ii. Application delivery: SaaS, managed service
- iii. Solution development with built-in security
- iv. Business Risk Ownership

1.8.3

Use Cases

- The BA is part of the IT Security team and is responsible for Security Operations analysis activities.
- The BA is part of the Risk Management or Compliance teams and is responsible for risk management, compliance, audit and enterprise-level analysis activities.
- The BA is part of the Project/Program Management group and is responsible for BA activities related to solution design, development, and/or deployment.
- The BA works within a support function of IT, such as Operations or Application Support.
- The BA is positioned in the business environment and is the business' connection point into IT or other Security and Risk functions.

1.8.4 Stakeholder Groups

Stakeholder Group	Examples: actors will vary based on the initiative	Engagement Points: when to engage the stakeholders	BA Focal Points/ Related Deliverables
Leadership	<ul style="list-style-type: none"> Project Sponsor, Owner (enterprise security initiative) Steering Committee 	<ul style="list-style-type: none"> Security Road Mapping Org Risk Assessments Project Initiation 	<ul style="list-style-type: none"> Charter Business Requirements Approvals
Business/ Client	<ul style="list-style-type: none"> Project Sponsor, Owner (business application initiative) Users Customers 	<ul style="list-style-type: none"> Project Initiation Solution Selection Change Management Operational Risk Management 	<ul style="list-style-type: none"> Business Process Maps Solution Requirements Gap Analysis Training
Enablers	<ul style="list-style-type: none"> IT Security, Architecture, DevOps Vendors, Procurement Project Management Regulatory/Legal/ Compliance 	<ul style="list-style-type: none"> Solution, Integration Design Options Identification and Analysis Solution Delivery Audits 	<ul style="list-style-type: none"> Security Requirements Threat Risk Assessments Integration Requirements Demos, RFP, Contract Business Requirements
IT Operations	<ul style="list-style-type: none"> Service Support Application Support Change Management Change Approval Board (CAB) 	<ul style="list-style-type: none"> Operational/Service Design Maintenance Planning Change Requests 	<ul style="list-style-type: none"> Transition, Support Requirements Gap Analysis Training

1.8.5 RACI: Responsible-Accountable-Consulted-Informed

A RACI Matrix is typically used to define stakeholders' roles; depending on the initiative, the engagement or participation role of each stakeholder will vary:

- **Responsible:** The stakeholder(s) who ultimately executes the task or deliverable; must be at least one individual assigned to this role but can be more; may leverage other resources as contributors.
- **Accountable:** The stakeholder who signs off the work of and enables the responsible actor(s) to deliver, either through provision of resources, removing barriers, or through escalation; can only be one individual; ultimately held to account for the deliverable or decision, and any consequences.

- "A" in RACI can also be used to represent Approve – the one who makes and owns decisions.
- Consulted: Provides subject matter expertise, feedback, professional advice; engages in two-way communication with the responsible or accountable actors.
- Informed: Does not actively participate in the decision, task or deliverable execution, but must be made aware of the outcome/output in order to perform

It is possible to have the same individual identified in both the Accountable and Responsible roles for a given task or deliverable.

Although it is possible and feasible to have a person or role assigned to more than one participation type for a given task, it is best practice to assign only one whenever possible.

1.8.6 Considerations

- BAs working on cybersecurity initiatives should be very clear on their role and level of participation in terms of responsibility for each task and deliverable.
- The BA may be directly involved in the development of the RACI, and if so, there are some questions to consider when assigning stakeholders to roles:
 - R: Which department is typically responsible and therefore likely best equipped? Who has capacity and influence to get the job done?
 - A: Which organization will be provisioning the resources for this activity and must live with the outcome? Who in that organization has the right level of authority for this decision?
 - C: Who knows about specific aspects of this work; whose input is essential? Are there groups in the organization that have an oversight or professional obligation to consult on the item?
 - I: Who will be affected by this work or decision? Who will need to inform others of the outcome, perhaps external to the organization?
- Cybersecurity should be a consideration for all initiatives; if a cybersecurity professional is not on your team or part of your RACI, you must get them there!

1.8.7 Examples

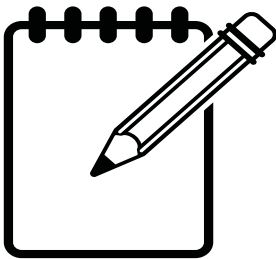
Example 1: Firewall Solution Implementation Project

Task/ Deliverable	BA	Project Sponsor	Architect	Vendor	Business Users	IT Operations	Test Lead	OCM
Business Requirements	R	A	C	I	C	C	I	I
Gap Analysis	R	C	C	C	C	A	-	I
Business Case	R	A	C	C	C	C	-	-
Test Strategy	C	A	C	C	C	C	R	I
Training Plan	C	A	-	C	C	C	-	R

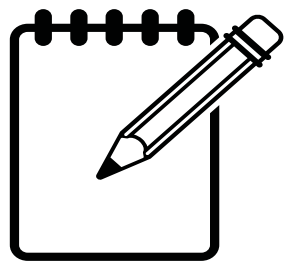
Example 2: Information Security Management System (ISMS) Implementation

Task/ Deliverable	BA	CISO	Risk/ Compliance Office	Vendors	Business Users	IT Groups	Executive	OCM
Project Plan	C	A	R	I	I	I	I	C
Org Risk Assessment	C	R	R	C	C	C	A	I
Risk Treatment Plan	C	R	R	I	I	I	A	I
Certification Audit	I	R	C	C	I	I	A	I
ISMS Management	C	A	R	C	I	C	C	C

NOTES



A series of horizontal dashed lines for writing notes.



NOTES



Module 2: Enterprise Security Concepts

1. Security Accountability
2. Cost of Securing an Organization
3. Outsourcing for Cybersecurity Expertise and Services
4. Risk Tolerance
5. Compliance
6. Best Practices and Benchmarking
7. Data Privacy
8. Data Privacy Nuances
9. Digital Rights Management (DRM)
10. Audit – Internal and External

2.1

Security Accountability

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

2.1.1

Business Analysis Practitioner (BA) Focal Points

- Recognize the information assets of the organization.
- Ensure governance (policies, processes) is aligned to the overall organization's goals.
- Facilitate stakeholders' identification of security requirements and implementation controls.
- Incorporate security aspect as part of analysis, both systems and processes.

- Support the Executive Management team which is accountable for enterprise security.
- Liaise across domains of application design, development and maintenance; operations; infrastructure and value chains of the organization.

2.1.2 Key Terms and Definitions

- **Governance:** Security governance is a framework containing security policies, approach, tools and awareness programs for achieving the organization's security objectives. Risk and data privacy are enforced by security policies.
- **Security Policy:** A policy that “includes security objectives or provides the framework for setting information security objectives”.¹
- **Information Security Management System (ISMS):** Consists of the policy, procedures, guidelines, and associated resources and activities, collectively managed by an organization in the pursuit of protecting its information assets.²
- **Confidentiality, Integrity, and Availability:** (CIA, also known as the CIA triad): A model designed to guide policies for information security within an organization.³
- **Chief Information Security Officer (CISO):** Accountable for security governance and interacts with Chief Data Officers and Chief Digital Officers, when they exist.

2.1.3 Use Cases

- Collaborate with the business to identify and protect their information assets.
- Consistently apply Confidentiality, Integrity and Availability (CIA) metrics on the information assets of the organization based on their criticality and their impact on the business.
- Perform risk assessments of the identified key assets.
- Recognize both internal and external (legal, regulatory and contractual) security considerations.
- Consider all digital assets, beyond information assets, such as Internet of Things (IoT) devices, machine learning, artificial intelligence (AI) and robotics.

1. Technical Committee. *ISO/IEC JTC 1, Information technology, SC 27, IT Security techniques. ISO/IEC 27000:2018*. International Standards Organization (ISO). 2018.

2. Ibid.

3. ICS. *Official (ISC)² Guide to the CISSP CBK*, Fourth Edition. Auerbach Publications. March 2015.

2.1.4 Related Risks

- Absence of security governance may lead to compromising the CIA of information assets and threaten the existence of the organization.
- Without an integrated approach to security, key resources will be in jeopardy.
- Cultural stigma could hinder raising concerns about security, whereas a culture of "see something, say something" will increase the quality of security for the organization.
- New business models often have complex and extended supply chains which can increase exposure to security risks.

2.1.5 Technology Controls

- Government IT Security Policy and Guidelines
- ISO 27001 (ISO/IEC 27001:2013) is considered the international standard for an ISMS
- Guidelines on Conducting Online Businesses and Activities
- Legal and Regulatory Requirements
- Performance Measurement Tools to track unusual traffic or events, Incident Detection, Security Operations Centre (SOC)
- Governance Frameworks such as: COBIT – Control Objectives for Information and related Technology, Trust Services Principles (used by SysTrust), and Criteria for Systems Reliability
- Data and privacy standards such as CASL, GDPR, PIPEDA, HIPPA, PCI impact security governance and policies

2.1.6 Process Controls

- Policies and Procedures, and activities that enforce or influence them:
 - Risk Assessments
 - Audits, both internal and external
 - Definition of authority and accountability for security decisions
 - Availability of information to make security decisions
 - Education, awareness and training to all personnel as part of an ongoing process

2.2 Cost of Securing an Organization

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Incidents and Breaches
6. Process Controls
7. Process Expertise

2.2.1 Business Analysis Practitioner (BA) Focal Points

- Knowledge of commonly deployed security controls and pricing schemes.
- Familiarization with security assessment, estimation and Return On Investment (ROI) processes.
- An understanding of risk-based implementation of security controls.
- An awareness of the cost to mitigate and monitor for threats.
- A foundational understanding of balancing cost, risk and resources in a budget-constrained environment.
- Historical awareness of the financial impacts of recent attacks and theft on businesses, governmental agencies and utilities.
- Understanding the differences among SaaS, PaaS, and IaaS cloud services, and how each of these has its own benefits, and to know how to best choose one based on the risk tolerance and systems deployment strategies in your organization.
- Understanding the budget and risk tolerance of the organization when considering cybersecurity impacts and objectively stating the costs and benefits.

2.2.2 Key Terms and Definitions

- **Return on Investment (ROI):** a performance measure used to evaluate the efficiency of an investment or compare the efficiency of several different investments. ROI tries to directly measure the amount of return on a particular investment, relative to the investment's cost.¹
- **Managed Security Service Provider (MSSP):** provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services.²
- **Software as a Service (SaaS):** SaaS providers host, manage and offer their entire infrastructure as well as application for users. With a SaaS

1.Chen, James. *Return on Investment (ROI)*. Investopedia Definition. January 2020. <https://www.investopedia.com/terms/r/returnoninvestment.asp>.

2.Gartner. *Gartner Information Technology Glossary: Managed Security Service Provider*. <https://www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider>.

platform, the user does not install anything but rather simply logs in and uses the providers application for a subscription fee. SaaS security is the responsibility of the SaaS provider.

- **Risk-based assessment:** are used to identify those items or areas that present the highest risk, vulnerability, exposure and potential effects on the enterprise, for inclusion in the IS annual audit plan.¹

2.2.3 Use Cases

- The cost of establishing standards, governance and risk assessments is prohibitive to many government and smaller non-governmental organizations without expert guidance and consultation.
- Identifying the right areas to invest in security, as the price of protecting the wrong things or applying outdated, ineffective tools to prevent attacks, has no appreciable value.
- Focusing cybersecurity spending on capabilities to detect and respond to cyber events earlier can minimize the impact.
- Moving from “protect-the-perimeter” model of cybersecurity to an approach that focuses on security in layers can be a huge advantage for an organization.
- Investing in managed security service providers and vendor-agnostic independent security professionals can increase cybersecurity capabilities more quickly and efficiently.

2.2.4 Related Risks

- Failure to implement defense in depth security controls to protect critical data and infrastructure greatly increases the threat of attacks and compromise.
- Failure to recognize the growing sophistication of cybersecurity threats and capabilities can diminish the value of an organization’s existing security capabilities.
- Agencies and firms that fail to implement appropriate security standards based on industry-recognized risk-based standards are likely to face increased threats from attacks.
- Regulatory, licensing and insurance costs are steadily increasing, while the cost associated with failing to meet regulatory and licensing requirements are significantly more.
- Often, with security-related initiatives, there are little to no tangible cost savings, so justification for the stated solution doesn’t offset the cost of the required resources.

1.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

2.2.5 Incidents and Breaches

- Organizations spend more than ever to deal with the costs and consequences of more sophisticated attack; the average cost of cybercrime for an organization increased US\$1.4 million to US\$13.0 million.¹
- As the average costs of breaches increases, spending on cybersecurity will need to increase, and focus on establishing business resilience.
- The average cost of a malware attack on a company is \$2.4 million.²
- The most expensive component of a cyber-attack is information loss, which represents 43% of costs.³
- Companies with an incident response team that regularly and extensively test their incident response plans experience significantly less in data breach costs than organizations that didn't have incident response in place.
- Breaches originating from a third party (such as a partner or supplier) cost \$370,000 more than average, emphasizing the need for companies to closely vet the security of the companies they do business with.

2.2.6 Process Controls

- Defining body to govern and oversee cybersecurity
- Approved technology security standards
- Enterprise risk management (ERM) and business impact assessment (BIA) capabilities
- Adoption of industry standard security and risk framework(s) such as NIST, ISO, and/or COBIT
- An incident and response plan that includes a comprehensive communications plan

2.2.7 Process Expertise

- National Institute of Standards and Technology (NIST) voluntary risk-based cybersecurity framework (CSF), implementation steps, and the five core functions: identify, protect, detect, respond and recover.⁴
- Possess a conceptual understanding of Defense in Depth strategy vs. layered security approach, and the costs to implement and support.
- Possess an understanding of resource allocation modeling to support various security controls and approaches.

1.Accenture. *Ninth Annual Cost of Cybercrime Study*. MARCH 6, 2019. <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study?src=SOMS>

2.Accenture. *Cybersecurity threats are growing*. Attack them. 2018. <https://www.accenture.com/us-en/about/security-index?src=SOMS#block-insights-and-innovation>.

3.Ibid.

4.National Institute of Standards and Technology (NIST). NIST SP 800 30: *Information Security: Guide for Conduction Risk Assessments*. U.S. Department of Commerce. September 2012.

2.3 Outsourcing for Cybersecurity Expertise and Services

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technical Controls
6. Process Controls

2.3.1 Business Analysis Practitioner (BA) Focal Points

- Understand the business model for the organization and if there are any unique security issues that are better addressed externally.
- Understand how external cybersecurity services will be onboarded and what is required for the organization to maximize the benefit of the subscribed services.
- Understand how Managed Security Service Providers will gain access to the environment and what data will be transmitted from your network to theirs.
- Understand the process for bringing outsourced security services back on-premise if the business needs change.
- Subject Matter Experts on the more technical aspects of cybersecurity may be engaged for their professional services, particularly for organizations lacking in this area; the BA is crucial as the interpreter between the consultant and the business, to ensure mutual understanding and to maximize the value of the expertise.

2.3.2 Key Terms and Definitions

- **Managed Service Provider (MSP):** An information technology provider of Software-as-a-Service (SaaS), or any other subscription-based technology delivery.
- **Managed Security Service Provider (MSSP):** Provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services.¹
- **Intrusion Detection Service (IDS):** Analyze and monitor network traffic for signs that indicate attackers are using a known cyber threat to infiltrate or steal data from your network. IDS systems compare the current network activity to a known threat database to detect several kinds of behaviours like security policy violations, malware, and port scanners.²

1. Gartner. *Gartner Information Technology Glossary: Managed Security Service Provider*. <https://www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider>.

2. Hello Clouders. *Cloud Basics*. <https://helloclouders.com/>.

- **Intrusion Prevention Service (IPS):** Live in the same area of the network as a firewall, between the outside world and the internal network. IPS proactively deny network traffic based on a security profile if that packet represents a known security threat. ¹
- **Demilitarized Zone (DMZ):** A screened (firewalled) network segment that acts as a buffer zone between a trusted and untrusted network; typically used to house systems such as web servers that must be accessible from both internal networks and the internet. ²

2.3.3 Use Cases

- Few mid-sized companies (and hardly any small businesses) have the internal IT security staff necessary to implement and manage a comprehensive cybersecurity program.
- Due to the demand for cybersecurity professionals, an organization may not be able to hire or retain skilled cybersecurity resources.
- By outsourcing security services to an external provider, an organization can have a lower cost for comparable services due to the economies of scale provided by MSSPs.
- Depending on the size of an organization, they may not require a team of full-time security specialists. They can outsource to scale at the right level.
- By outsourcing cybersecurity to a third party, an organization can determine which specific services are required to be outsourced, such as networking operations centre (NOC) and penetration (pen) testing but keeping payment card information (PCI) compliance in-house.

3

2.3.4 Related Risks

- Due to the potentially large volume of sensitive data from multiple organizations, Managed Service Providers (MSP) are an obvious target for malicious cyber-attacks.
- When cybersecurity services are outsourced, the organization is also handing over a level of control to the third party.
 - This arrangement will require the organization to comply with a set of terms and conditions which may include the use of specific software. These packages – and the lack of control associated with them – may expose the organization to new threats that were previously not an issue.
- Although outsourcing of cybersecurity services can lower upfront costs of enhancing security posture, there is a risk of increased costs down the road should the vendor drastically increase fees, or it becomes necessary to migrate the services in-house.

1.Ibid.

2.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

3..Maria, by Gitanjali. *What is MSSP and how it helps small business IT security*. GetApp.com. March 2019. <https://lab.getapp.com/what-is-mssp/>.

2.3.5 Technical Controls

- Virtual Private Networking (VPN): A secure private network that uses the public telecommunications infrastructure to transmit data; uses encryption and authentication, maintaining privacy and security on all data that pass between two internet points.¹
- Security Information and Event Management (SIEM): A solution that involves harvesting logs and event information from a variety of different sources on individual servers or assets and analyzing it as a consolidated view with sophisticated reporting.²
- Data Loss/Leak Prevention (DLP): a suite of technologies designed to prevent breaches by locating, classifying and cataloging sensitive information, and monitoring and controlling the data in all three states: at rest, in transit, and in use.
- Network Segmentation: A common technique to implement network security is to segment an organization's network into separate zones that can be separately controlled, monitored and protected.³

2.3.6 Process Controls

- Principle of Least Privilege: Providing the minimum amount of access to perform the work.
- Vendor onboarding and offboarding processes.
- Internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets. In a cybersecurity context, it is used so that no single person is in a position to introduce fraudulent or malicious code without detection.⁴

1.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

2.ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

3.Ibid.

4.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

2.4 Risk Tolerance

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technical Controls
6. Process Controls

2.4.1 Business Analysis Practitioner (BA) Focal Points

- Facilitate identification of the organization's key risks.
- Define risk appetite and tolerance in relation to enterprise risk and leverage a consistent approach to risk management.
- Establish risk governance, policies and processes for monitoring and shifting the risk appetite and tolerance, accordingly, based on the changing internal and external factors.
- Define infrastructure risk tolerance, using a consistent approach.
- Define risk tolerance for data and applications, as part of the solution design and delivery.
- Implement controls for ensuring management of risk through the life of the solution.
- Extend evaluation of risk to include value chain partners, and the likelihood and impact to the organization's goals.

2.4.2 Key Terms and Definitions

- **Risk:** A risk can be defined as the effect of uncertainty on objectives.
- **Risk Appetite:** The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission.¹
- **Risk Tolerance:** Risk tolerance is about what an organization can cope with, the maximum limit beyond which the organization does not want to perform.
- **Risk Probability:** The estimated likelihood that an event will be realized, typically expressed as a percentage.
- **Risk Impact:** The estimated impact to the business, which could be positive or negative, and typically expressed as a dollar amount.
- **Risk Register:** A risk register is a living document that is created to list and track identified risks, and should include the following information for every risk: unique identifier, description, likelihood of occurrence, impact to business, any associated threats or vulnerabilities that have been identified, the planned treatment, risk owner, status, and all significant dates.

1.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

2.4.3 Use Cases

- Defining risk appetite and tolerance within the enterprise risk management approach.
- Setting business objectives while considering risk appetite and tolerance.
- Defining appetite and tolerance for cybersecurity related risks, including:
 - Defining infrastructure risks based on CIA parameters.
 - Defining data asset risks based on CIA parameters.
 - Defining digital asset risks based on CIA parameters.

2.4.4 Related Risks

- Assets can be both tangible and intangible, and the value of each of these will need to be determined accordingly to gauge tolerance.
- Determining accurate risk appetite and tolerance depends on the nature of the business, size of the organization, and culture, among many other internal and external factors, but the most important will be the perception of the risk by the organization.
- Organizations must be flexible in their operation including their ability to assess and evaluate risk tolerance.
- It may be difficult to define and assess all factors when determining risks, such as damage to reputation.
- External risks may be difficult to predict, such as natural disasters or socio-economic factors.

2.4.5 Technical Controls

- Leverage data analytics to recognize changes to risk appetite and risk tolerance. This should trigger a re-evaluation of the appropriate risk tolerance thresholds.
- Enforce defined risk tolerance thresholds.
- Analyze existing controls to check if they remain fit for purpose and make enhancements, as applicable.
- Implement appropriate controls to ensure defined risk appetite and tolerances are enforced.
- Implement appropriate access controls to identify exceptions to risk appetite and tolerances.
- Apply controls to verify and validate the data for any exceptions.

2.4.6 Process Controls

- Define Policies and Procedures for regular risk assessments.
- Implement processes for monitoring and governance of risk appetite and risk tolerance based on changing internal and external factors.
- On-going analysis of the organization's vulnerabilities which includes physical, procedural, personnel and logical risks.
- Ensure consensus when determining an estimation approach, as there are many ways to estimate risk. The agreed upon approach should be used consistently within the organization.
- Ensure ongoing awareness training to achieve consistent risk tolerance within the organization.

2.5 Compliance

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Frameworks
6. Standards

2.5.1 Business Analysis Practitioner (BA) Focal Points

- Analyze requirements for the protection of information assets and ensure appropriate controls are applied for their protection, across all considerations of people, process and technology.¹
- Participate in the implementation of standards and restrictions that local legislation may place on how information can/must be handled, by collaborating with subject matter experts.
- Provide any regulatory or compliance bodies with the necessary access to information in a format acceptable to the regulators, to demonstrate compliance.
- Maintain a risk register, an up-to-date set of security policies with a review process, a record of any dispensations from security policies, results from assurance reviews and security testing and compliance reviews, assurance breaches or incidents.
- Facilitate reviews of processes, procedures and controls for information assurance against changed requirements.
- Monitor the constant and rapid changes and upgrades required for the assurance systems to cope with the ever-changing climate of the business.
- Incorporate the information assurance policy with all the necessary, comprehensive, easy-to-understand documentation covering the standards expected, guidelines on how to do things correctly and procedures for what must be done to preserve the assurance of the information.²

1. International Organization for Standardization (ISO). *The ISO/IEC 27000 family of standards*. ISO.org. <https://www.iso.org/isoiec-27001-information-security.html>.

2. Taylor, Andy, David Alexander, Amanda Finch, and David Sutton. *Information Security Management Principles*. BCS, The Chartered Institute for IT. June 2013.

2.5.2 Key Terms and Definitions

- **Compliance:** Working in accordance with the defined actions, processes, policies and procedures; ensuring that a system or process complies with the defined or expected operating procedures.¹
- **Information assurance:** The confidence that information systems will protect the information they carry and ensure that “the right people, have access to the right information, at the right time”.
- **Policy:** High-level statement of an organization’s values, goals and objectives specific to an area or at the organizational level. Compliance with policies is obligatory.
- **Standard:** More prescriptive than a policy. It quantifies what needs to be done and provides consistency in controls that can be measured. Standards should support policy and state “what must be done and how it should be achieved”. Compliance with standards is obligatory.²
- **Procedure:** A set of detailed working instructions that will describe what, when, how and by whom something should be done and should be supported by enterprise policies and standards. Compliance with procedure is obligatory.
- **Guideline:** Provides advice, direction and best practice in instances where it is often difficult to regulate how something should be done. Compliance with guidelines is not obligatory.

2.5.3 Use Cases

- Define the scope of compliance, based on national and international standards (e.g., ISO/IEC 27000 series) relevant to the level of “information assurance” and scope of governance based on organizational structure.
- Identify and categorize sensitive data based on the industry sector and deploy suitable strategies to meet information assurance and compliance obligations.
- Put policies and practices in place for regular compliance checks to gauge the level of user understanding and awareness of assurance responsibilities.
- Extend full support to the compliance checker to formally address major nonconformities, recommend corrective action and amend measures to prevent instances of non-compliance.
- Use models (comprising of methodology, structure and processes) to maintain a formal and efficient control process for reporting compliance issues.
- Establish regular, formal review of compliance documentation in an organized and timely manner involving all required internal and external parties and maintain records of results.

1.Ibid

2.Ibid.

2.5.4 Related Risks

- Not understanding and adhering to global legal compliance requirements can lead to serious security breaches.
- Not assessing the security risks and the importance of compliance requirements may pose a threat to the existence of the organization.
- Absence of “information assurance” can lead to uncertain business operations and cannot guarantee accurate and accountable information affecting critical decision-making.
- Absence of regular compliance checks can weaken information assurance and will increase tendencies of users to show less regard as they are not challenged.

2.5.5 Frameworks

- Information Security Management Systems (ISMS):
 - a set of policies, procedures, technical and physical controls to protect the confidentiality, availability and integrity of information, which can be applied to the entire organization or a specific area
 - a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to meet business objectives by effectively treating and managing risks
 - supports IT and business management process with controls for technical and business risks related to people, resources, assets and processes, based on a risk assessment and the organization's risk tolerance

1

- Control Objectives for Information and Related Technology (COBIT):
 - a good-practice framework created by the ISACA (Information Systems Audit and Control Association) for IT governance and management, aimed at the whole enterprise
 - provides an implementable set of controls over information technology and organizes them around a logical framework of IT-related processes and enablers, facilitating easier, tailored implementation
 - defines the components and design factors to build and sustain a best-fit governance system

2

1. International Organization for Standardization (ISO). *The ISO/IEC 27000 family of standards*. ISO.org. <https://www.iso.org/isoiec-27001-information-security.html>.

2. ISACA. *COBIT 5 for Information Security*. ISACA, COBIT 5, Information Security. June 2012.

2.5.6 Standards

- ISO/IEC 27000 series: Information security management standard by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC); helps organizations protect their information through effective technology, auditing and testing practices, organizational processes and staff awareness programs.
- Data Protection Act 2018 (DPA 2018): Sets out the framework for data protection law in the UK; updates and replaces the Data Protection Act 1998 and came into effect on May 25, 2018.
- General Data Protection Regulation of May 2018 (GDPR): A regulation in EU law on data protection and privacy for all individual citizens; sets out the key principles, rights and obligations for most processing of personal data.
- Personal Information Protection and Electronic Documents Act (PIPEDA): A Canadian law relating to data privacy; governs how private sector organizations collect, use and disclose personal information in the course of commercial business.
- Although the U.S. does not have a single overarching piece of legislation for privacy protection, acts such as the Health Insurance Portability and Accountability Act (HIPAA) may be applicable to standards compliance.

2.6 Best Practices and Benchmarking

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technical Controls
6. Process Controls

2.6.1 Business Analysis Practitioner (BA) Focal Points

- Understand how benchmarking data will be used to prioritize security service maturity.
- Understand the implications of applying best practices to the organization's security posture and if the best practices being applied are relevant.

2.6.2 Key Terms and Definitions

- **Security Benchmarking:** How an organization's security architecture compares with those of its peers, how it compares to industry standards and best practices, and where gaps and shortcomings exist that lower the overall security maturity of the organization.
- **Defense in Depth:** An approach where the protected assets have multiple independent layers of security. This includes network layers (net and sub-nets) as well as general controls such as password protection, encryption, and access control on assets including data.
- **Policy:** A high level statement from management saying what is and is not allowed in the organization. Should be broad enough to encompass the entire organization and should have the endorsement of those in charge. ¹
- **Standard:** Dictates what will be used to carry out the policy. e.g. Outlook as the corporate email standard.
- **Procedure:** A description of how exactly to go about performing a certain task.
- **Internet of Things (IoT):** A concept in which devices (such as sensors and appliances) are connected to a network and are smart. It implies that these devices do not have direct human controls and operate via software within the network. The connection point and the software create vulnerabilities.

1. Raggad, Bel G. *Information Security Management Concepts and Practice*. CRC Press Book. 2010.

2.6.3 Use Cases

- Performing a gap analysis can help an organization understand the specific areas of security that require focus. This is often done in the form of a current state and target state assessment of the organization's complete security posture.
- As the Internet of Things expands, so does the attack surface of any organization. Benchmarking and best practices provide a method to understand the security posture in comparison to others and aid in prioritization.
- Rather than trying to protect against all kinds of threats, most IT departments focus on insulating the most vital systems first and then finding acceptable ways to protect the rest without making them useless. Some of the lower-priority systems may be candidates for automated analysis, so that the most important systems remain the focus.¹

2.6.4 Related Risks

- Benchmarking is a point in time picture. Peers, competitors and attackers are constantly changing which can result in major differences in security posture.
- Benchmarking analysis can be very subjective and may focus on how an organization feels about their security posture versus what the data tells them.
- Without benchmarking, objectives can devolve into vague promises about "increasing" security or building "better" security architecture. With no concrete performance goals, it becomes difficult to take action or to justify sufficient resource allocation.²
- Depending on the exact type of organization, failure to meet standards of good practice (in other words, being negligent) can result in fines, loss of accreditation, loss of ability to obtain government re-imbursements, lawsuits due to negligence, and loss of insurance coverage.³

2.6.5 Technical Controls

- Security Information and Event Management (SIEM)
- Defense in Depth

2.6.6 Process Controls

- Internal and External Audit
- Privacy and Data Protection Policies
- Legal and Regulatory Requirements
- Secure Development Policies

1.Techopedia .*The 7 Basic Principles of IT Security*. May 2017. <https://www.techopedia.com/2/27825/security/the-basic-principles-of-it-security>.

2.Dacri, Bryana. *Make Security Benchmarking a Reality*. BitSight. May 2018. <https://www.bitsight.com/blog/make-security-benchmarking-a-reality>.

3.Heimerl, Jon-Louis. *Best Practice: Can You Really Define 'Best' Security?*. Security Weeel. July 2012. <https://www.securityweek.com/best-practice-can-you-really-define-best-security>.

2.7 Data Privacy

1. Overview
2. Business Analysis Practitioner (BA) Focal Points
3. Key Terms and Definitions
4. Use Cases
5. Related Risks
6. Technical Controls
7. Process Controls

2.7.1 Overview

- Data Privacy refers broadly to the need to protect sensitive information; the largest area of concern currently is the personal information of individuals.
- Data Privacy encompasses appropriate use of data as well as its protection from loss or theft.
- Data Privacy is an emerging global concern and regulations vary by jurisdiction.

2.7.2 Business Analysis Practitioner (BA) Focal Points

- Data minimization: what is really needed?
- Capturing rationale
- Determining retention periods
- Designing processes and systems to respond to data subject rights requests
- Designing processes and systems with correct defaults, notification, and consent requirements
- Non-functional requirements for archiving, encryption, anonymization, and data security
- Including and managing Legal, Information Security and/or your Privacy Office as a stakeholder on application and analytics projects

2.7.3 Key Terms and Definitions

- **Privacy By Design:** The practice of incorporating data privacy requirements into a technical solution and its associated processes during the project design phase, rather than as an afterthought.
- **Data Subject:** The person whose information is being protected. Data privacy is primarily about protecting the privacy of an individual.

- **Personal Information:** Information that is associated to a human being, such as name, age, or reputation. We will cover important categories of personal information in later modules. Note that personal information can even be on paper.
- **Data Subject Rights:** Data privacy regulations are often phrased in terms of human rights. The most famous data subject right is the “right to be forgotten” – that is, to have personal information removed from a company’s possession. We will cover additional data subject rights in later modules.
- **Privacy Policy:** A company’s statement disclosing to its customers how their information is gathered, managed, used and disclosed to others.
- **Notice:** The act of informing a data subject how his or her information will be gathered, managed, used, and disclosed to others.
- **Consent:** The act of acquiring permission to gather, manage, use or disclose personal data.
- **Data Minimization:** The act of limiting data elements to be used in a technical solution by investigating the rationale behind collecting them and confirming that the data gathered is the minimum required for the given purpose or use case.
- **Pseudonymization:** The act of assigning an artificial identifier to replace personal information, in order to minimize the amount of personal information processed by an application.
- **Anonymization:** The act of disassociating data about a person from information that could cause that person to be identified in a larger context. Note that pseudonymization does not necessarily constitute anonymization.
- **Data Retention:** The act of defining how long a company needs to keep a given piece of information and removing it when the retention period has expired.

2.7.4 Use Cases

- Use cases for data privacy will range widely across your organization – essentially, you need to consider data privacy anywhere an application or a business process manages information about a human being. Here are a few examples, but this is by no means an exhaustive list:
 - A Customer Service agent discusses personal health or financial information with a customer
 - An Application Development team considers purging or removing old records from a system
 - Human Resources revises the way annual performance reviews are performed and stored
 - A Data Scientist begins a discovery effort
 - Digital Marketing identifies Web leads
 - A customer calls your company to exercise his data subject rights
 - Human Resources analyzes candidate resumes with an algorithm that detects keywords
 - A salesperson leverages birthday information to personalize a message to a client

2.7.5 Related Risks

- Lawsuits
- Large Fines
- Reputational Risk
- Customer Dissatisfaction
- Identity Theft

2.7.6 Technical Controls

- Privacy by design: Build in privacy from the start.
- Privacy by default: Default settings should be the most private, not the most public.
- Data loss prevention: Leverage state-of-the-art security tools to ensure that personal data is not transmitted outside your network.
- Data encryption and obfuscation: Ensure that personal data is protected if leaked from its source systems.
- Data pseudonymization and anonymization: Isolate identity data from other relevant information as much as possible
- Data localization: Keep data in its country of origin.
- Access controls: Ensure that personal data is only visible to those who need to see it.
- Data retention, archiving and deletion: Keep personal data only as long as law requires, and then delete it.

2.7.7 Process Controls

- Contractual agreement: When personal data must be shared with another company, ensure that responsibility for data privacy issues is allocated as part of contractual agreements
- Data Subject Rights Processes: Ensure that you are prepared to respond to a request to invoke a data subject right.
- Incident Response Planning and Breach Notification Processes: Ensure that you are prepared to report data breaches to appropriate authorities, as a part of a more general security incident response plan.
- Physical isolation of personal information processing: Ensure that workers who need to discuss personal information on a regular basis (for example, the administrative staff at a hospital) are physically isolated from others so that information is not overheard.
- Training and Policy: Train everyone in your organization to protect personal data.
- Register of Processing Activities: Maintain an overall registry of how personal data is processed in your organization. Note that this is mandated by some regulatory frameworks.

2.8 Data Privacy Nuances

1. Privacy, Emotion, and Culture
2. Data Privacy Regulations
3. Data Subject Rights
4. Data Categorization
5. Best Practices for Data Minimization

2.8.1 Privacy, Emotion, and Culture

- Because data privacy is essentially an emotional topic, culture plays a role.
- If you are working on an application that will need to be used in multiple geographies, privacy culture may influence your requirements as well as privacy regulations.
- Cultures that stress individual choice may be more open to the idea that individuals are likely to want to trade privacy for services.
- A well thought out approach to data privacy is likely a positive feature for your customers – and it may even become a competitive advantage.
- Engage regional experts in areas like sales or marketing to gather privacy requirements based on culture.

2.8.2 Data Privacy Regulations

- The most famous data privacy regulation is the European Union's General Data Protection Regulation (GDPR)
- Multiple jurisdictions regulate data privacy as well. Here are a few examples:
 - The United States' Health Insurance Portability and Accountability Act, or HIPAA, contains laws about protecting the data privacy of patients
 - The United States also regulates the storage of credit and other financial information
 - Canada has a longstanding data privacy law, the Personal Information Protection and Electronic Documents Act, or PIPEDA
- Local regulations exist in U.S. states and EU member states
 - California recently passed the California Consumer Privacy Act
- Regulations may conflict with each other in intent or meaning
- U.S. law tends to encourage retaining information, whereas EU law tends to encourage deleting it
- You need a lawyer to sort all this out – don't try to do this yourself!
- Engage your legal team to discover which regulations apply to your business situation – and then work with them to derive specific requirements from those regulations.

2.8.3 Data Subject Rights

- Some data privacy requirements can be phrased in terms of the rights of the data subject.
- GDPR famously grants rights to each EU citizen with respect to his or her personal data, including
 - The right to access data about himself or herself
 - The right to correct data about himself or herself
 - The right to have data about himself or herself erased
 - The right to object to or opt out of automated decision making
- Other frameworks may include other declarations of rights.
- Work with your Legal team to confirm which rights apply to your business.
- Work with your Customer Service department to confirm that you have business processes to support a customer's request to exercise a data privacy right.

2.8.4 Data Categorization

- Data privacy analysis can frequently be performed at the data category level.
- For example, in the U.S., health care organizations frequently want to analyze whether a given system contains protected health information (PHI), which is information about a patient's health status, health care, or payment for health care.
- Payment Card Information, also called PCI, is another category of data that is governed by rules and regulations.
- The GDPR defines several special categories of data that can be handled by applications only under special circumstances.
- Fields in an information system will likely belong to one or more of these categories. You can often write requirements at the category level; for example, "PHI shall be encrypted in transit".
- Work with your Legal department to understand data categories that are relevant to your organization.

2.8.5 Best Practices for Data Minimization

- Eliminate Unused / Unneeded Data
 - When designing systems, don't create, use, or share data fields that you don't need.
 - This is somewhat obvious when you build systems from the ground up but can be especially important when configuring COTS software – hide and/or lock down fields that are not essential to perform a job function.
 - Think especially hard about "optional" fields – if a business process can be performed without specific information, why are you collecting it?

- Minimal data collection can make the user experience pleasant and efficient.
- Know Why You Need It
 - Document rationale for each field to confirm that you are using only what you need.
 - For information in sensitive or protected data categories, confirm with your Legal team that you can use that data for that purpose.
- Leverage Access Control to Regulate Use
 - Field-based access control allows you to hide sensitive information from job roles that do not need it; for example, a bank's customer service department might have access to your account number, but a security guard in the same bank should not.
 - Row-based access control can be especially effective. For example, many HR systems allow access only to the records of employees who are in a manager's direct reporting line. Row-based access control can also help focus users only on data relevant to themselves and their tasks. For international applications, consider row-based access control that limits a user to transactions only in his or her geography.
- Remove Obsolete Data
 - Strong retention policies that delete or archive data when it becomes obsolete are another way of minimizing data.
 - Note that removal of obsolete data also has positive application benefits, such as improved performance.
 - Many sensitive data are also subject to data retention regulations which may require data to be kept for a certain length of time – check with Legal.
- Disassociate or Remove Identifying Information
 - Data can be made more private by removing it from the context of other data. When managing personal data, a good practice is to disassociate the identifying information (such as names and birth dates) from the sensitive information (such as health status or bank routing numbers) as much as can be permitted by the application.
 - There are several techniques to accomplish this:
 - Pseudonymization: The practice of assigning an artificial identifier to replace personal (often identifying) information. The key distinction between pseudonymization and anonymization is that pseudonymization is reversible, usually by lookup in another database.
 - Anonymization: The practice of permanently disassociating personal information from a record. Anonymization is irreversible; once the data has been anonymized, the association to a real person should be impossible to construct.
 - Data Masking: The practice of replacing “real” personal information with dummy data. If you are constructing test systems with a copy of production data, masking personal information as the data is imported is a best practice.
 - Data Scrambling or Shuffling: The act of permuting identifying information so that it no longer is associated with itself – for example, swapping first name, last name, and birth date between records in a dataset until the data no longer represent real people.

2.9 Digital Rights Management (DRM)

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technical Controls
6. Process Controls

2.9.1 Business Analysis Practitioner (BA) Focal Points

- Identify the copyright content or part of the content (sensitive data) that requires protection.
- Establish processes and procedures for controlling the trading, protection, monitoring, and tracking of digital media.
- Establish appropriate role-based access controls of the copyright content.
- Verify effective controls are implemented based on high probability and high impact risks.
- Support the management of data classification policies, process flows, and procedures for copyright content as applicable.
- Ensure collaboration between the technical teams in building and maintaining the DRM architecture.
- Assess customer requirements relating to rendering of the copyright content.

2.9.2 Key Terms and Definitions

- Digital Rights Management (DRM): A collection of systems or approaches to protect the copyright of digital media.
 - It refers to a broad range of technologies and standards, and the purpose of DRM is to prevent unauthorized redistribution of digital media and restrict the ways consumers can copy content they have purchased.
 - DRM encrypts data and allows decryption by authorized users in accordance with rules determined by the author.
 - DRM is not an implementation of copyright law; it is a system for the protection of digital works.
 - DRM will implement licenses through software controls.

- Rights Expression Language (REL): Defines what rights you have in relation to the copyright content.
 - REL in the digital rights management sense is a formal language like mathematics or like programming code that can be executed as an algorithm.
 - A rights expression language is not open to interpretation but must be rendered precisely through software

1

2.9.3 Use Cases

- Determine the copyright content or part of the content (sensitive data) that requires protection.
- Define the DRM requirements for the copyright content based on strategic objectives and other internal and external factors.
- Implement appropriate DRM solutions based on all relevant requirements.
- Assess and understand the customers' requirements relating to rendering of the copyright content which is in addition to the needs of the copyright owner organization.
- Define REL requirements relating to time, units, value exchange, etc., for example:
 - e-commerce, where a price could be associated with a half hour of music listening, or
 - a non-monetary form, like granting a right to read a chapter to a user who first views a particular number of advertisements

2.9.4 Related Risks

- Information assets are the most important asset in this digital age and the risk of losing the whole or part of copyright content is high.
- New DRM solutions must be assessed and tested against the stated requirements to rule out any unknown vulnerabilities.
- Designing DRM solutions must be flexible to incorporate expansions and changes to the requirements.
- Balance between read-only access and “editable/comment-able” access to copyright content must be carefully considered.
- Technological change will create risks to stay current to the broader protection risks.

1. International Standards Organization. *ISO/IEC 27000: IT Security techniques*. ISO. 2016.

2.9.5 Technical Controls

- Defining the technology specification requirements, dependents and scope of future expansions; DRM solution based on computer/technology identification.
- Define user rights in a service which issues certificates to the users which define specific access and usage rights under a licensed usage rules.
- As DRM services are often cloud-based and are available from many vendors including Microsoft, Adobe, Google, SAP and others, it is important to match the right need to the right solutions, as the offerings vary significantly.

2.9.6 Process Controls

- The copyright content journey must be clearly understood and articulated to provide the right DRM solutions for the stated requirements.
- Management of complex relationships of distribution, sales and lending must be clearly defined based on term-limited licensing basis and permanent acquisition of the copyright content.
- Clearly define “Rights Expression Language” in a human-readable form to understand the algorithm.
- Clearly articulate any legal requirements/differences between the DRM solution provided and copyright law:
 - DRM approach is "everything that is not permitted is forbidden“
 - copyright law is an expression of "everything that is not forbidden is permitted"
- Audit of the management of Digital Rights would examine compliance to defined requirements and assure there is a process for "breach" of licensing or content uses.

2.10 Audit – Internal and External

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technical Controls
6. Process Controls

2.10.1 Business Analysis Practitioner (BA) Focal Points

- Understand the intended frequency and scope of internal and external audits.
- Understand how audit findings will be actioned.
- Understand how audit findings relate to relative regulatory and legal compliance requirements.
- All audits include findings and recommendations based on identified weaknesses. It is important to understand and document an organization's planned response.

2.10.2 Key Terms and Definitions

- **Internal Audit:** Performed by an organization's internal audit staff and is typically intended for internal audiences.¹
- **External Audit:** Performed by an outside auditing firm. These audits have a high degree of external validity because the auditors performing the assessment theoretically have no conflict of interest with the organization itself. Intended audience for an external audit may include the Board of Directors and investors.²
- **Evidence:** Records, statements of fact, or other information which are relevant to the audit criteria and verifiable.
- **Findings:** Results of the evaluation of the collected audit evidence against defined audit criteria.

2.10.3 Use Cases

- A comprehensive audit should scrutinize and evaluate many aspects of an organization's security posture. The technical scope of assessments would look at the environment, software, and physical hardware configurations. The business or process perspective would assess user practices and how information is handled.

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

2. Ibid.

- Organizations should implement a program for continuous monitoring and auditing of security controls and their implementation.
- External audits typically validate the security of the network by using techniques like penetration testing to assure that no unauthorized user can access the organizations assets.
 - Additional audit procedures will examine the processes used for such activity as access control, user privileges, network points of data exchange with external data and software services and other organization defined needs to assess policy compliance.
 - Internal audits are similar reviews of controls and data access areas, as well a software change, patch management and ongoing operational level controls. These are typically done on an ongoing basis and are not as periodic as external audits.
 - External audits are generally more depended on to assure to a board, or organization directors that the policies and governance practices are adequate and enforced. The independence of external audits gives credence to the findings and results of the audits.
- Although spending on business systems and data security is increasing, there's a question of whether these investments are going far enough. Most companies choose to concentrate on traditional and converged IT infrastructure security, such as firewalls. Audits can provide insight into what risks should be addressed first.¹

2.10.4 Related Risks

- Cyber risks are constantly evolving at a high pace and in an unexpected manner. The broad and connected nature of cyber risks make them particularly hard to manage. Cyber risks also remain largely abstract and high level rather than real and operational.
- The effects of non-compliance or not following a standard can cost an organization in loss of reputation, data or monetarily. In a worst-case scenario a breach can cause an organization to shut down temporarily or permanently.
- New regulations such as the General Data Protection Regulation (GDPR) call for stiff penalties in case of a breach or hack resulting in lost personal data. One way to mitigate the consequences of a breach is to show that your organization has followed government initiatives and taken the necessary steps to protect personal data to the highest extent possible.²

1.Kurchina, Paul. *The Five Most Common Cybersecurity Risks - and How to Fight Back*. Digitalist Magazine. April 2018. <https://www.digitalistmag.com/cio-knowledge/2018/04/02/5-most-common-cybersecurity-risks-how-to-fight-back-06037803>.

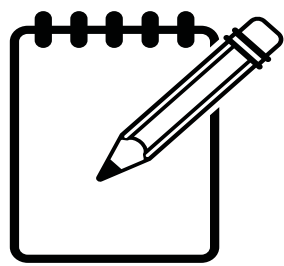
2.Official Journal of the European Union *Regulation (EU) 2016/679 (General Data Protection Regulation)*. May 2018. <https://gdpr-info.eu/>.

2.10.5 Technical Controls

- Central log processing and archiving
- Defense in Depth
- Governance, Risk Management, and Compliance (GRC) Software

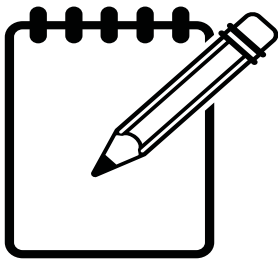
2.10.6 Process Controls

- Risk Management Process
- Project and Portfolio prioritization
- Detailed Policies and Procedures
- Certification Standards such as ISO 27001



NOTES

NOTES



A series of horizontal dashed lines for taking notes.

3

Module 3: Enterprise Risk

1. Risk Management & Control Assurance Framework
2. Organizational Risk Assessment
3. Risk Analysis: Threat Risk Assessments
4. Risk Analysis: Vulnerability Assessments
5. Business Case Development
6. Disaster Recovery and Business Continuity

3.1

Risk Management & Control Assurance Framework

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Frameworks
5. Related Risks
6. Process Controls

3.1.1

Business Analysis Practitioner (BA) Focal Points

- Have a thorough understanding of the organization's selected framework(s) and how they have been, or will be, implemented in the context of the business.
- Understand how an organization's control assurance framework establishes controls, monitoring, and periodic reviews to ensure business objectives can be met within an acceptable level of risk.
- Understand the roles of risk and control owners, independent auditors, and control sign-off approvers within the context of the assurance framework.
- Understand how control designs ensure that controls are appropriate for the risk, cover the full extent and scope, and integrate efficiently within the context of the business needs.

- Reviews and audits generally reveal findings that must be tracked and managed to ensure that timely changes are made, and risk management documentation is updated to reflect the adjustments.

3.1.2 Key Terms and Definitions

- **Risk owner:** A person or entity with the accountability and authority to manage a risk, including determining controls.
- **Control owner:** Accountable for implementing and maintaining the effectiveness of specific controls and may also be responsible for designing or modifying controls to improve their effectiveness.
- **Control:** An "enabler", something that helps an organization achieve its business objectives. A control often arises from implementing a risk treatment action.
- **Assurance:** A process that provides confidence that business objectives will be achieved with a tolerable level of residual risk.
- **Control design:** A central part of the risk treatment stage of the risk management process.
- **Potential exposure:** The total plausible maximum impact on the organization arising from a risk without regard to controls.

1

3.1.3 Use Cases

- Frameworks can be implemented in a progression that aligns with the organization's risk priorities. For example, controls related to perimeter security may be implemented first where this has been identified as among the highest risks to information security.
- It's important to monitor controls, providing confidence that goals and objectives are being met within an acceptable level of risk.
- Organizations should implement periodic and regular management reviews, including checks on processes and systems, using control self-assessment, and driven by the risk profile of the business area and the manager's span of control.
- Organizations that conduct independent reviews of controls provide another level of assurance that risk management and internal control frameworks are working as intended. However, independent audits tend to have a very specific focus, and they are rarely able to cover the full scope of business activities.

2

1. International Organization for Standardization (ISO). *ISO 3100: Risk Management-Guidelines*. ISO. 2018.

2. Finger, Pamela, Andrew MacLeod, Michael Parkinson, and Grant Purdy. *HB 158-2010 Delivering assurance based on ISO 31000:2009 Risk management – Principles and guidelines*. Standards Australia, The IIA Research Foundation and The Institute of Internal Auditors Australia. 2010.

3.1.4 Frameworks

- National Institute of Standards & Technology (NIST) Cyber Security Framework: Consists of standards, guidelines, and best practices to manage cybersecurity-related risk and help to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.
- ISO 27001: Although published and intended as a certification standard, the implementation guidance also represents a cybersecurity framework for organizations to follow when establishing an Information Security Management System (ISMS), practice, and program.
- COBIT (Control Objectives for Information and related Technology): A business framework for the Governance and Management of Enterprise IT. Although this is a governance-level framework, it aligns and maps to other major operational-level guidelines, standards, frameworks and compliance rules.

3.1.5 Related Risks

- Business processes change as do organizations' strategies and goals. Adapting to changes requires ongoing monitoring and evaluation of the controls in place to ensure goals and objectives are achievable at an acceptable level of risk. If the controls don't keep pace with those changes, the business may take on additional risk or an unacceptable level of risk.
- Monitoring, evaluating and modifying controls should be ongoing with periodic reviews and audits performed by an objective outside agent to provide assurance that in-place controls meet business needs and are aligned with current risk profiles. The impact of relying on internal reviews could provide a false sense of assurance, and the controls may not adequately meet their objectives.
- Compliance requirements generally compel a thorough review of the control designs, and as business and IT changes occur in the environment, reviews of the control designs will reveal weaknesses and opportunities for improvement. In the absence of control design reviews, the controls may be inefficient or inadequate, and the organization could be exposed to unacceptable levels of risk.

3.1.6 Process Controls

- Controls should fit the purpose, apply within the context, and address the root cause of the risk.
- Controls should be appropriate, covering the full extent and scope of the risk and its consequences.
- Controls should be cost-effective and efficient.
- When a new control is introduced, or if a control is modified, risk management documentation should be updated to reflect the changes.
- Control processes, risk owners and control owners should be reviewed periodically to ensure they are aligned with current business objectives and goals, and that changes to organizations have been incorporated into the control assurance framework.

3.2 Organizational Risk Assessment

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

3.2.1 Business Analysis Practitioner (BA) Focal Points

- Understand how risk assessments are tied to an overall security implementation, with systems and data prioritized based on a standardized classification.
- Understand the organization's risk appetite and risk culture; how the organization applies a contextual framework to estimate an acceptable level of risk that aligns with its values, missions, and goals.
- Understand the frequency of risk assessments and security controls, and how the organization adjusts its recovery plans based on the results.
- Recognize how the organization's decision makers seek cost-effective approaches to correcting security weakness.
- Understand how risk assessments provide insights into the effectiveness of security controls and their quality and potential impact on the environment in which they are deployed.

3.2.2 Key Terms and Definitions

- **Risk:** A function of the likelihood of a given threat-source exercising a potential vulnerability, and the resulting impact of that adverse event on the organization.¹
- **Risk Management:** The identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events; or to maximize the realization of opportunities.²
- **Risk appetite:** The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission.³

1.National Institute of Standards and Technology (NIST). *NIST 800-30: Information Security - Guide for Conduction Risk Assessments*. U.S. Department of Commerce. September 2012.

2.International Organization for Standardization (ISO). *ISO 3100: Risk Management-Guidelines*. International Organization for Standardization (ISO). 2018.

3.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

- **Risk capacity:** The amount of risk an organization requires to meet their goals. This can be described as the total risk exposure that is consistent with strategy and objectives.
- **Risk Management Framework (RMF):** A process that integrates security and risk management activities into the system development lifecycle.¹

3.2.3 Use Cases

- Organizations should prepare for events that compromise the integrity of their systems, networks and data by establishing a systematic, structured way to identify, classify, and assess risk to their systems and operations.
- Organizations that perform a risk assessment are in a better position for selecting the appropriate security controls for each system – the security controls necessary to protect individuals, business operations, and assets of the organization.²
- An organization that prescribes a risk management framework will follow a process to classify information and systems into categories based on an impact assessment, and then select and implement baseline security controls appropriate to the types and kinds of risk.
- Organizations will have different risk appetites depending on their sector, culture and objectives. A range of appetites exist for different risks and these may change over time.
- Organizations that routinely assess the validity of the security controls contained in their security and privacy plans are prepared to manage events and recover more quickly.

3.2.4 Related Risks

- Cyber threats are increasing at a fast pace with more cybercriminals joining the threat landscape and evolving as cybercrime tools and technologies steadily advance in design and availability.
- Failure to perform risk assessments periodically endangers systems if the security controls are no longer effective which can result in compromise, failure or complicity in a cyber-attack.
- A successful cyber-attack on a system protected by ineffective security controls can result in substantial financial loss, as well as loss to data, downtime to recover, and loss of brand integrity and customer trust.
- Organizations generally must accept some risks and avoid others as a matter of doing business to achieve an advantage and to compete in various markets. Organizations who don't quantify their risk appetite will likely miss opportunities toward achieving strategic goals and objectives.

1.National Institute of Standards and Technology (NIST). *NIST 800-30: Information Security - Guide for Conduction Risk Assessments*. U.S. Department of Commerce. September 2012.

2.National Institute of Standards and Technology (NIST). *NIST SP 800 53A: Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. U.S. Department of Commerce. December 2014.

- Organizations that haven't prepared to manage risk nor identified their risk appetite are more likely to take unacceptable risks while putting their systems in jeopardy against threats and unplanned events.

3.2.5 Technology Controls

- Risk registers or logs
- Software: Risk management, Risk mitigation and tracking
- Secure storage to ensure documents related to risk assessments, plans, and controls can be accessed by authorized individuals
- Logging and monitoring on the secured documents repositories
- Audit logs to ensure compliance and effective controls

3.2.6 Process Controls

- Enterprise security standards
- Enterprise Governance, Regulatory and Compliance publications and training
- Risk Management Framework
- Risk assessment lifecycle process
- Risk appetite statement
- Risk Assessment: Risk Identification + Risk Estimation + Risk Evaluation

3.3 Risk Analysis: Threat Risk Assessments

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Methodology
6. Technology Controls
7. Process Controls

3.3.1 Business Analysis Practitioner (BA) Focal Points

- The business analysis practitioner (BA) may conduct Threat Risk Assessments or support the Security Analyst in doing so (see Use Cases).
- The BA must (or have access to resources that) understand the system or application, its business purpose and integrations, and its data and transactions, to provide context to the analysis.
- The BA may work with the system or application owner to explain risks and mitigation options, including impacts, and help define and track action plans.
- The BA would develop, maintain, and enhance Threat Risk Analysis processes and methodologies, and assist with technical solutions to ensure standardization of the service across the organization.
- The BA should be familiar with commonly used TRA models and frameworks as well as Threat Modelling and related methodologies.

3.3.2 Key Terms and Definitions

- **Cyber Threat:** The possibility of a malicious attempt to damage or disrupt a computer network or system; a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.
- **Vulnerability:** The intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.
- **Threat Risk Assessment:** Analyzes a software system for vulnerabilities, examines potential threats associated with those vulnerabilities, and evaluates the resulting security risks.
- **Controls or Countermeasures:** Safeguards to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets; should strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.
- **Threat Modelling:** A process by which potential threats can be identified, enumerated, and prioritized – all from a hypothetical attacker's point of view.
- **Application Threat Modelling:** A structured approach for analyzing the security of an application; enables you to identify, quantify, and address the security risks associated with an application.

$$\text{Risk} = ((\text{Vulnerability} + \text{Threat}) / (\text{Countermeasure})) \times \text{AssetValueRisk}$$

1

1. International Organization for Standardization (ISO). *ISO 3100: Risk Management-Guidelines*. ISO. 2018.

3.3.3 Use Cases

- As part of the deployment of a new system an analysis is required to assist in identifying potential threats to the system's assets and information. Controls must be built into the design where possible, and mitigation plans created for the balance.
- A new cyber threat becomes known; the potential risks to the entire organization must be analyzed.
- Any change to the security infrastructure can create a potential for new risks; a threat risk assessment can assess the security posture based on the changes.
- An incident or event occurs, triggering a threat risk assessment on related areas of the business, similar systems, network, etc.
- Mature organizations may employ Cyber Threat Intelligence tools – advanced analytics that use data to predict potential attacks and warn the security team proactively.

3.3.4 Related Risks

- Without a tool or process in place for conducting threat risk assessments, an organization may not become aware of preventable risks, therefore leaving the organization vulnerable.
- Not using a comprehensive framework or methodology that guides analysis of all possible exposure points of a system may leave potential threats and risks undiscovered.
- Assessments identify and quantify risks that can be tracked and reported upon, as well as mitigation plans and actions taken to address the risks.
- Threat intelligence points out unusual patterns in systems and other valuable data, but it won't stop an attack; that takes human intervention and the deployment of the right technology tools to block or at least mitigate an attack.¹

3.3.5 Methodology

- Whether an automated tool or manual process or framework is used to conduct a TRA, there are some key steps that are taken. The exact number of steps will vary across models, but in general, a Threat Risk Assessment will require you to:
 - Determine the scope of your Threat Risk Assessment: which assets will be included.
 - For each asset, identify potential vulnerabilities that can lead to threats.
 - For each vulnerability, identify the threats that could potentially lead to a breach.

1. Robb, Drew. *Threat Intelligence and Analytics: Staying Ahead of Cyber Criminals*. eSecurity Planet. March 2017. <https://www.esecurityplanet.com/network-security/threat-intelligence.html>.

- Using pre-defined assessment scales, rate the threats in terms of severity and impact to the organization, should they be realized; the product is the overall risk for that threat.
- Prioritize the risks and develop treatment plans to address the highest ranked first, striving to eliminate (or mitigate) risks where possible.

3.3.6 Technology Controls

- There are several software solutions available on the market for managing threat risk assessments and outcomes, and some that encompass and/or integrate with Security Information and Event Management (SIEM) tools.
- Cyber Threat Intelligence:
 - is the analysis of an adversary's intent, opportunity, and capability to do harm,
 - it is actionable information that answers a key knowledge gap, pain point, or requirement of an organization,
 - involves collection, classification, and exploitation of knowledge about adversaries, and
 - gives defenders an upper hand and forces them to learn from intrusions and evolve.

1

3.3.7 Process Controls

- There are many manual methodologies and frameworks available that organizations can use, customize, and potentially automate or more efficient utilization.
- A few of these common methodologies are:
 - Application Threat Modelling
 - Operational Threat Modelling
 - The Process for Attack Simulation and Threat Analysis (PASTA)
 - STRIDE Methodology: threat classification model developed by Microsoft

1. Gartner. *Digital business brings new risks*. <https://www.gartner.com/en/information-technology/insights/cybersecurity>.

3.4 Risk Analysis: Vulnerability Assessments

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

3.4.1 Business Analysis Practitioner (BA) Focal Points

- Business Analysis Practitioners (BA) working within a Security team may conduct Vulnerability Scans and Assessments themselves, or act as the liaison between the business/development team and the Security Analyst who would conduct the scan.
- The BA may prepare the Vulnerability Assessment (VA) or provide an interpretation of the results to the application owner.
- If the VA is being used as an input to a Threat Risk Assessment, the BA may coordinate the integration of the assessment pieces and provide the business owner with a summary of the results and engage in planning next steps.
- The BA would be responsible for ensuring project documentation and requirements are satisfied, related to assessments.
- The BA would be responsible for establishing and maintaining the VA process, and any tools used to conduct it, and staying current on standards and advances in technology around the process.

3.4.2 Key Terms and Definitions

- **Vulnerability:** A cybersecurity term that refers to a flaw in a system that can leave it open to attack; any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.
- **Vulnerability discovery:** A process that uses algorithms, known as vulnerability discovery models (VDMs), once software is designed to identify any existing vulnerabilities.
- **Vulnerability remediation:** Process to reduce the impact of an attack from critical to non-critical effect.
- **Vulnerability Assessment/Vulnerability Analysis:** A method of recognizing, categorizing and characterizing the vulnerabilities among the network infrastructure, computers, hardware system, and software.

- **Vulnerability Scanning:** An inspection of the potential points of exploit on a computer or network to identify security holes; also used by attackers looking for points of entry.
 - detects and classifies system weaknesses in computers, networks, and communications equipment
 - predicts the effectiveness of countermeasures
- **Unauthenticated Vulnerability Scanning:** Reveals vulnerabilities that can be accessed without logging into the network; the tester performs the scan as an intruder would, without trusted access to the network.
- **Authenticated Vulnerability Scanning:** The tester logs in as a network user, revealing the vulnerabilities that are accessible to a trusted user, or an intruder that has gained access as a trusted user.
- **Penetration Testing/Pen Testing:** Testing to find vulnerabilities that an attacker could exploit; includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or actually), and reporting back the findings.

1

3.4.3 Use Cases

- The primary objective of cybersecurity is to reduce vulnerabilities so that attackers have fewer opportunities and ways to gain access to information.
- Common ways information security professionals achieve this is by keeping current on vulnerabilities relevant to in-use software and finding ways to remove them, and by ensuring that security patches are maintained on all software.
- Penetration tests are used to:
 - identify security weaknesses;
 - evaluate compliance to security policies;
 - assess user security awareness; and,
 - test incident detection and response capabilities.

3.4.4 Related Risks

- Vulnerability scans can cause operational errors and trigger performance interruptions as they intrude upon code running on the target computer.
- False positives are a likely result of unauthenticated vulnerability scans which cannot be further analyzed due to the lack of detailed information about the scanned asset's software.

2

1. International Organization for Standardization (ISO). *ISO 3100: Risk Management-Guidelines*. International Organization for Standardization (ISO). 2018.

2. Open Web Application Security Project (OWASP). *Vulnerability Scanning Tools*. https://owasp.org/www-community/Vulnerability_Scanning_Tools.

3.4.5 Technology Controls

- Vulnerability scanning technology solution attributes include:
 - SaaS offerings with significant scan information
 - Customizable reporting and host information such as installed software and certificates
- Vulnerability scanning technology solutions typically provide customization capabilities to more precisely define the host, such as installed certificates and software, open ports, and reports.
- Penetration testing technology solutions are available commercially as well as free-of-charge.

3.4.6 Process Controls

- Many software development and delivery methodologies require Vulnerability Scanning as a deliverable, and results must be accepted by IT Security before they will approve the software to progress to the next stage of development.
- Vulnerability Assessments are often an input to a more comprehensive Threat Risk Assessment for the initiative, before a new system is accepted into production.

3.5 Business Case Development

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Enterprise Business Cases
5. Infrastructure & Application Business Cases
6. Related Risks
7. Technology and Process Expertise

3.5.1 Business Analysis Practitioner (BA) Focal Points

- Demonstrate understanding of the purpose and rationale for the business case, and how to promote the business case to stakeholders.
- Understand the importance of promoting security to “C” level executives.
- Demonstrate continuous efforts to make security a priority within your organization by integrating security into the business case processes.
- Show the value of aligning the business case with the organization’s visions and goals.
- Understand the importance of building consensus across stakeholders when there are competing interests.
- For initiatives that are cybersecurity centric, it may be more challenging to determine the ROI without tangible benefits, such as institutional reputation.

3.5.2 Key Terms and Definitions

- **Executive Summary:** A brief but comprehensive synopsis of a business plan which highlights its key points and is generally adapted for an external audience
- **SWOT:** Strengths, Weaknesses, Opportunities, Threats
- **Financial Analysis:** The examination of financial information to reach business decisions
- **Risk Assessment:** The identification of hazards that could negatively impact an organization's ability to conduct business
- **COTS:** Commercial Off the Shelf

3.5.3 Use Cases

- The Business Analysis Practitioner (BA) should consider cybersecurity costs and benefits when developing a business case for a business initiative, such as shared infrastructure costs and the funding for those assets.
- Understanding the budget and risk tolerance is a key factor when building business cases with cybersecurity impacts and objectively stating the costs and benefits.
- The law of diminishing returns needs to be considered as the cost can increase exponentially while the returns may not.
- Developing a high-level work plan can provide the stakeholder with a view of a convincing timeline and set of milestones.

3.5.4 Enterprise Business Cases

- The BA may support or lead enterprise cybersecurity business cases.
- These business cases likely involve senior and executive leadership teams.
- The scope of enterprise cybersecurity business cases may include a combination of organizational restructuring, infrastructure investments, capability and value-chain assessment, governance and policy definition and revision.
- The costs and benefits analyzed at this level require thorough understanding of potential risks and opportunities. This requires a significant amount of expertise in business case development with specialization in cybersecurity.
- If insufficient knowledge and expertise is available, outsourcing is an option to ensure proper advisory services are available.

3.5.5 Infrastructure & Application Business Cases

- Infrastructure business cases are likely driven by the IT team. These initiatives need similar rigour to understand the options available to secure the layers they support.
- A BA may be tasked to develop the infrastructure business case with very technical stakeholders, ensuring SWOT analysis is performed and related metrics are defined.
- Application business cases are performed more routinely, but they should contain elements of cybersecurity, when done properly. Change impacts need to be considered when implementing an application.
- An understanding of cybersecurity is critical in our global marketplace and should be considered from the very beginning of a technology initiative.
- Elements such as access controls, and ownership of application and infrastructure security must be continually considered and refined.

3.5.6 Related Risks

- The security organization may not be perceived positively by leadership, making the business case a tougher sell.
- If the business case doesn't represent or is not aligned with the company's goals and objectives, it may not be approved.
- Often with security-related initiatives, there are little to no immediate tangible cost savings, so justification for the stated solution doesn't offset the cost of the requested resources.
- Promoting the wrong solution approach can jeopardize the security posture of the organization.

3.5.7 Technology and Process Expertise

- Knowledge of cybersecurity tools, techniques and processes will inform the business about realistic options and costs.
- Understanding how to perform and evaluate financial analysis and cyber risk assessments will provide a more compelling position to support the business case.
- The BA who understands the organization's culture and attitudes towards security spending will enable the author of the business case to tailor the objectives that appeal to stakeholders' concerns and interests.
- Technical writing skills will give the BA the ability to write efficiently and effectively.

3.6 Disaster Recovery and Business Continuity

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Building Disaster Recovery and Business Continuity into the Lifecycle
6. Technical Controls
7. Process Controls

3.6.1 Business Analysis Practitioner (BA) Focal Points

- Define the recovery process with a broad scope as the nature of a disaster cannot be predicted.
- Define procedures for controlled recovery from a disaster with considerations for legal and regulatory requirements.
- Define Recovery Point Objectives (RPO) based on criticality of the related system. This defines how current the restored data and configuration must be (i.e. restore up to one minute before the disaster, or the day before the disaster, for example).
- Define Recovery Time Objectives (RTO) based on criticality of the related system. This defines how long it will take to restore systems to the RPO (i.e. is there a hot backup ready to go or will it take days to acquire and setup hardware and related systems?).
- Definition of cybersecurity procedures during the recovery, such as access controls, network configuration, version controls, integration and synchronization of components. As this is an ongoing process, it should be adopted as part of change management.
- Coordinate and/or support regularly scheduled disaster recovery (DR) simulations.

3.6.2 Key Terms and Definitions

- **Business Continuity (BC):** A general term used to describe measures implemented by an organization to enable it to continue operating after a major incident. This will include service levels, key business functions, protocol for decision making, critical staff members and their training. Depending on DR, separate procedures may be in place for operational activities.
- **Disaster Recovery (DR):** Refers to the steps to be taken after a disaster to restore infrastructure and technical capabilities including networks, servers, applications and data.
- **MOSCOW technique:** Defines requirement priority (Must Have, Should Have, Could Have, Won't Have).

3.6.3 Use Cases

- Information security requirements should be determined when planning for business continuity and disaster recovery.
- Definition of governance for how and when to initiate various recovery responses.
- Definition of continuity, post-recovery, consisting of members from across the organization so there is sufficient breadth of knowledge to deal effectively with whatever situation occurs, along with senior members with authority to take decisions.
- Implementation of a tested disaster recovery response and business continuity plan.
- Key personnel should be trained how to initiate and perform steps to be taken during and post-recovery.

3.6.4 Related Risks

- Absence of disaster recovery and business continuity plans can affect the confidentiality, integrity and/or availability of information assets and may threaten the very existence of the organization.
- Disaster recovery and business continuity plans require on-going management and improvement, and not a one-time process. Failure of the plans during a disaster may lead to manifestation of security breaches and overall business risks.

3.6.5 Building Disaster Recovery and Business Continuity into the Lifecycle

- The BA must ensure Disaster Recover (DR) and Business Continuity (BC) are considered throughout the lifecycle of cybersecurity initiatives.
- During planning activities, consider the impacted stakeholders and infrastructure related to cybersecurity initiatives.
- During elicitation and analysis activities, ensure you have included the identified stakeholders and obtain their input and approval related to DR and BC. Understand which groups, systems and hardware are critical to support the organization.
- Design and development phases must consider these requirements for DR and BC, understanding priority using techniques like MOSCOW.
- Production operation and support teams must be trained and prepared to identify and respond to incidents requiring Disaster Recovery and Business Continuity.

3.6.6 Technical Controls

- A standard form for recording events and incidents to ensure all the necessary information is captured and communicated to all necessary teams.
- Monitoring, detecting, analyzing and reporting information security events and incidents.
- Effective and efficient controls, mandating data encryption, controlled system access, authentication, server configuration settings, firewalls, remote access, guarantee of integrity, accountability for processing, audit trails etc., as applicable.
- To quantify types, volumes and costs of information security incidents.
- Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

3.6.7 Process Controls

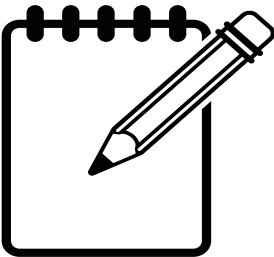
- Incident Response Team (IRT) and all members of the team report and respond in accordance with the documented procedures.
- Accountability for recovery plan invocation decisions depending on the magnitude of the problem, anticipated duration, and operational impact.
- Implementation of all the five main phases of incident management – Reporting, Investigation, Assessment, Corrective Actions and Review.
- Control activities to include approvals and authorizations, verifications and reconciliations, reviews of operating performance, security of assets and segregation of duties.¹
- Fulfilling legal and regulatory requirements, as applicable, in their respective countries.
- Implement internal controls for example the Committee of Sponsoring Organization (COSO) model to achieve:
 - Effectiveness and efficiency of operations;
 - Reliability of financial reporting; and
 - Compliance with applicable laws and regulations.

2

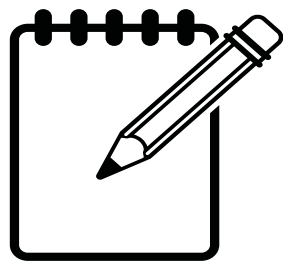
1. Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management - Integrate Framework Executive Summary*. COSO. September 2004. <https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf>.

2. Ibid.

NOTES



Area with horizontal dashed lines for taking notes.



NOTES

4

Module 4: Cybersecurity Risks and Controls

1. Understanding Security Controls and IT Risk: Part 1
2. Understanding Security Controls and IT Risks: Part 2
3. CIA Triad
4. Applying Controls
5. Cybersecurity Threats: Part 1
6. Cybersecurity Threats: Part 2
7. Cybersecurity Vulnerabilities: Part 1
8. Cybersecurity Vulnerabilities: Part 2
9. Adverse Impacts
10. Risks and Controls – Putting It All Together

4.1

Understanding Security Controls and IT Risk: Part 1

1. Introduction
2. Key Terms and Definitions
3. Use Cases

4.1.1

Introduction

- Cybersecurity Risks and Controls begins to dive deeper into the technical application of the information covered in the previous three parts.
- In very general terms, cybersecurity is about identifying IT Risk: where your systems and information are vulnerable to known and unknown threats and putting countermeasures – or controls – in place to mitigate those risks.
- In this module, we will introduce some key concepts around IT Risk and Security Controls and provide a high-level overview of how the key components of risk models relate and are applied to reduce overall organizational cyber risk.

- In the subsequent modules in this part, we will focus a little deeper on each of the key components, to provide a comprehensive view of these important concepts.

4.1.2 Key Terms and Definitions

- **Controls:** Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.
- **CIA:** Confidentiality, Integrity, Availability of information; these are the aspects of information which controls aim to protect. Also known as the CIA Triad.
- **Threat:** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit an information system vulnerability.¹
- **Vulnerability:** A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.²
- **Incident:** Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service.³
- **Impact:** The result of an unwanted incident; the extent or severity of the harm.
- **Risk:** The combination of the probability of an event and its impact.⁴
- **Predisposing Condition:** A condition that exists within a business process, enterprise architecture, information system, or environment of operation, which affects the likelihood that threat events, once initiated, will result in adverse impacts to organizational operations and assets.
- **Non-Repudiation:** One party of a contract cannot deny having received a transaction, nor can the other party deny having sent a transaction.

1.National Institute of Standards and Technology (NIST). *NIST SP 800 30: Information Security: Guide for Conduction Risk Assessments*. U.S. Department of Commerce. September 2012.

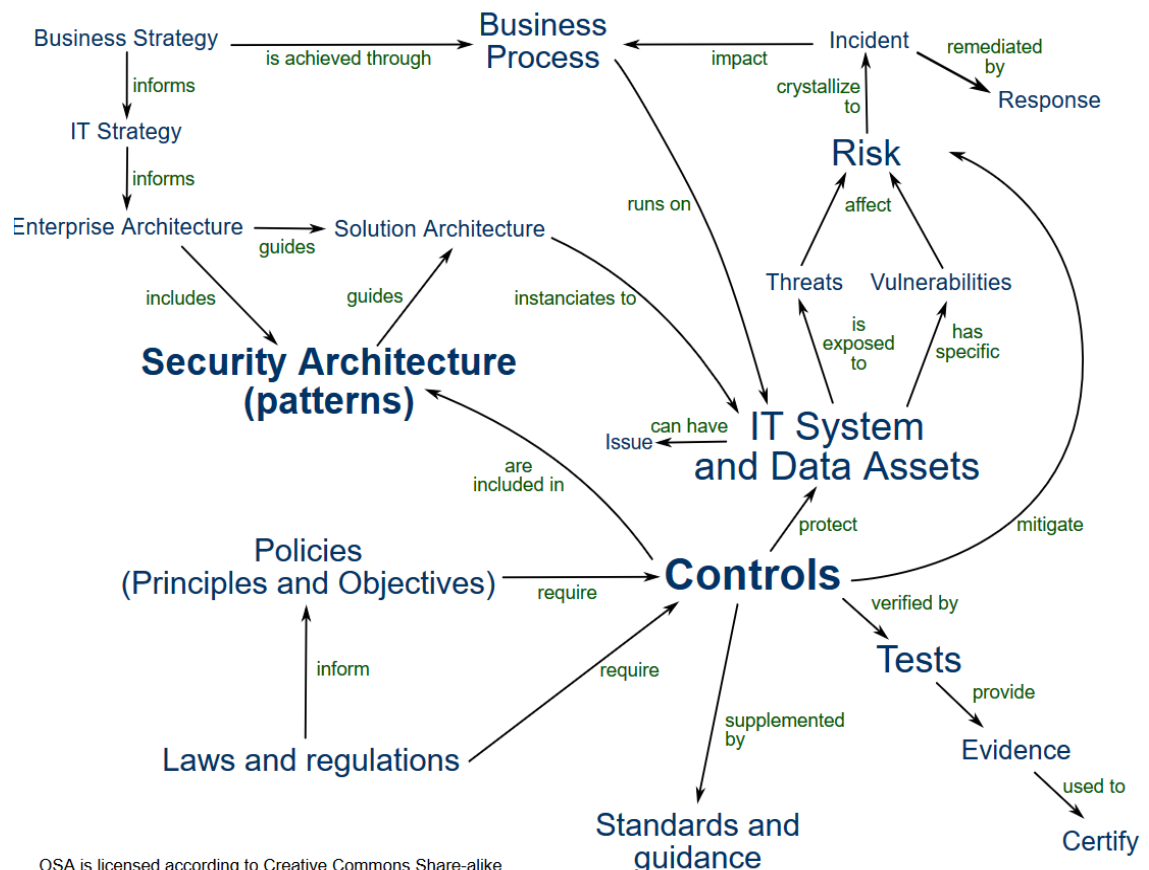
2.Ibid.

3.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

4.Ibid.

4.1.3 Use Cases

- The following diagram illustrates how the IT Security entities relate to each other practically; as you read through these points, have a look at the model (the right side in particular) to see how.
 - Organizations rely on IT Systems and Data Assets to operate.
 - Systems and Assets can have Issues (some are inherent, some are defects or side-effects).
 - Many issues with systems cause weaknesses, known as Vulnerabilities to harm, when exposed to threats.
 - Harm results from actualization of Threats, which may come from adversarial (malicious attacks), or non-adversarial (inadvertent) sources.
 - When an asset is vulnerable to a threat, it is at Risk. The level of risk depends on the severity, or pervasiveness of the vulnerability, and the likelihood of the threat occurring.
 - When a threat successfully exploits a vulnerability, an Incident occurs. An incident may have several impacts, each of varying severity, to the business.
 - Controls are used to protect business assets from the realization of risks, or to mitigate the impact to the business should an incident occur.
 - Some controls can be included in Security Architecture, at Enterprise, and Solution levels.



OSA is licensed according to Creative Commons Share-alike.
 Please see: <http://www.opensecurityarchitecture.org/cms/about/license-terms>.

4.2 Understanding Security Controls and IT Risks: Part 2

1. Control Frameworks
2. Control Framework Characteristics
3. Control Categories
4. Control Types
5. Control Selection Aspects

4.2.1 Control Frameworks

- A control framework is a set of controls that protects data within the IT infrastructure of a business or other entity. The control framework acts as a comprehensive security protocol that protects against fraud or theft from a spectrum of outside parties, including hackers and other kinds of cybercriminals.¹
- A few common examples of IT Control Frameworks include:
 - NIST: National Institute of Standards and Technology; a non-regulatory agency of the U.S. Department of Commerce. Its mission is to promote innovation and industrial competitiveness. Its Cybersecurity Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk; its 19 control families contain 285 controls.²
 - ISO 27001: Best known part of the ISO/IEC 27000 family of standards; provides requirements for an information security management system (ISMS), a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes, and IT systems by applying a risk management process.³
 - COBIT®: Control Objectives for Information and Related Technology; manual for IT Governance, for guaranteeing security, quality and compliance in information technology.
 - ITIL®: The IT Infrastructure Library; contains broad and publicly available professional documentation on how to plan, deliver, and support IT service features.

1.Techopedia.com. Definition - What does Control Framework mean?. <https://www.techopedia.com/definition/23913/control-framework>.

2.National Institute of Standards and Technology (NIST). NIST Mission, Vision, Core Competencies, and Core Values. www.nist.gov. January 26, 2017. <https://www.nist.gov/about-nist/our-organization/mission-vision-values>.

3.International Organization for Standardization (ISO). *The ISO/IEC 27000 family of standards*. ISO.org. <https://www.iso.org/isoiec-27001-information-security.html>.

4.2.2 Control Framework Characteristics

- Although control frameworks vary based on the needs and characteristics of the organization, some key components are often part of these plans:
 - objective setting
 - event identification and development of response plans
 - compliance with government requirements or industry guidelines
 - monitoring processes: transaction reviews, quality assurance checks, audits
 - control activities: authorizations, reviews and verifications of IT processes, hardware setups
- To aid in ensuring security and privacy requirements are met, many organizations adopt control frameworks to provide a governance program that is:
 - Comprehensive
 - Consistent
 - Measurable
 - Modular
 - Standardized

1

4.2.3 Control Categories

- Controls may be organized into categories to facilitate their consideration and appropriate use. Controls may be in the form of an approach, a technical solution, or a process that follows a specific methodology. The following table shows one example of how controls can be categorized, with the intended functionality or utility for each.

Control Category	Designed Utility
Compensating Controls	Substitute for the loss of primary controls and mitigate risk down to an acceptable level.
Corrective Controls	Remedy circumstance, mitigate damage, or restore controls.
Detective Controls	Signal a warning when a security control has been breached.
Deterrent Controls	Discourage people from violating security directives.
Directive Controls	Specify acceptable rules of behavior within an organization.

1. National Institute of Standards and Technology (NIST). *NIST Cybersecurity Framework*. U.S. Department of Commerce. February 2014. <https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.

Control Category	Designed Utility
Preventive Controls	Prevent a security incident or information breach.
Recovery Controls	Restore conditions to normal after a security incident.

1

4.2.4 Control Types

- Access controls may also be classified into the methods by which they are implemented, and this arrangement can be applied to the controls once they have been categorized as in the section above.

Control Type	Implementation Control Types
Administrative Controls (or Management Controls)	Substitute for the loss of primary controls and mitigate risk down to an acceptable level.
Physical Controls (or Operational Controls)	Remedy circumstance, mitigate damage, or restore controls.
Technical Controls (or Logical Controls)	Signal a warning when a security control has been breached.

2

4.2.5 Control Selection Aspects

- There are many characteristics that should be considered when selecting a control as a countermeasure for a particular risk:
 - Accountability – can it be held responsible?
 - Auditability – can it be tested?
 - Is it from a Trusted source?
 - Does it act Independently (self-determining)?
 - Can it be Consistently applied?
 - Is it Cost-Effective?

1.Ibid.

2.ICS. *Official (ISC)² Guide to the CISSP CBK*, Fourth Edition. Auerbach Publications. March 2015.

- Is it Reliable?
- Is it independent from other countermeasures (no overlap)?
- Is it Easy to use?
- Is it Automated?
- Is it Sustainable?
- Is it Secure?
- Does it protect CIA (confidentiality, integrity, and availability) of assets?
- Can it be Backed-out in event of an issue?
- Does it create no additional issues during operation?
- Does it leave no residual data from its function?

1

1. ICS. *Official (ISC)² Guide to the CISSP CBK*, Fourth Edition. Auerbach Publications. March 2015.

4.3

CIA Triad

1. CIA: Confidentiality, Integrity, Availability
2. C: Confidentiality
3. I: Integrity
4. A: Availability

4.3.1

CIA: Confidentiality, Integrity, Availability

- The CIA triad is an information security benchmark model used to evaluate the information security of an organization.
- It was created to provide a baseline standard for evaluating and implementing information security regardless of the underlying system and/or organization.
- Its components: C-I-A, are the aspects of information which security controls aim to protect.¹
- The Guide to the CISSP® CBK®, (ISC) 2 states that:
“...information security program must ensure that the core concepts of availability, integrity and confidentiality are supported by adequate security controls designed to mitigate or reduce the risks of loss, disruption or corruption of information.”²

4.3.2

C: Confidentiality

- Ensures that data or an information system is accessed by only an authorized person.
- Ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.
- User IDs and passwords, access control lists (ACL) and policy-based security are some of the methods through which confidentiality is achieved.³
- NIST Special Publication 800-60v1r1 defines the Security Objective of the Confidentiality aspect of information:
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.⁴

1.Techopedia.com. *Definition - What does CIA Triad of Information Security mean?*. <https://www.techopedia.com/definition/25830/cia-triad-of-information-security>.

2.ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

3.Techopedia.com. *Definition - What does Access Control List (ACL) mean?*. <https://www.techopedia.com/definition/24766/access-control-list-acl>.

4.National Institute of Standards and Technology (NIST). *NIST SP 800 60: Information Security: Guide for Mapping Types of information and information Systems to Security Categories*. U.S. Department of Commerce. September 2008.

Table 4.1: Confidentiality Loss Impacts and Control Methods

Impacts of Information Confidentiality Loss	Control Methods Used to Protect Confidentiality
<ul style="list-style-type: none"> • Loss of privacy • Sensitive information exploited • Information used criminally • Identity theft • Fraud • Adverse effects experienced by an individual or organization • Legal liability • Loss of public confidence or reputation • Abuse of power, authority • Administrative burden 	<ul style="list-style-type: none"> • Access restrictions • Information categorization • Data classification • Awareness training • Password best practices • Data encryption • Multi-factor authentication • Biometric verification • Security tokens • Principle of Least Privilege • Identification, Authentication, Authorization through Access Controls

- NIST SP 800-60v1r1 provides questions to ask when assessing the Confidentiality factors of information types, to evaluate the level of security impact associated with unauthorized disclosure of the information:
 - How can a malicious adversary use the unauthorized disclosure of information to do limited/serious/severe harm to agency operations, agency assets, or individuals?
 - How can a malicious adversary use the unauthorized disclosure of information to gain control of agency assets that might result in unauthorized modification of information, destruction of information, or denial of system services that would result in limited/serious/severe harm to agency operations, agency assets, or individuals?
 - Would unauthorized disclosure/dissemination of elements of the information type violate laws, executive orders, or agency regulations?¹

4.3.3

I: Integrity

- Integrity assures that the data or information system can be trusted and is edited by only authorized persons and remains in its original state when at rest.
- Integrity means assuring the accuracy and completeness of data over its entire lifecycle.
- Data encryption and hashing algorithms are key processes in providing integrity.²

¹.Ibid.

².Techopedia.com. Definition - What does Integrity mean?.<https://www.techopedia.com/definition/10284/integrity>.

- NIST Special Publication 800-60v1r1 defines the Security Objective of the Integrity aspect of information:

Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.¹

Table 4.2: Integrity Loss Impacts and Control Methods

Impacts of Information Integrity Loss	Control Methods Used to Protect Integrity
<ul style="list-style-type: none"> • Unintentional changes • Unauthorized changes • Accidental changes • Inconsistent information • Inaccurate information • Data corruption • Data destruction • Untrustworthy information • Poor business decisions • Processing errors 	<ul style="list-style-type: none"> • Segregation of duties • Approval checkpoints • Testing • Change Management and Version Control • File permissions • Access controls • Detection • Response and Recovery • Backups and Redundancy • Secure storage • Log collection

- NIST SP 800-60v1r1 provides questions to ask when assessing the Integrity factors of information types, to evaluate the level of security impact associated with unauthorized disclosure of the information:
 - How can a malicious adversary use the unauthorized modification or destruction of information to do limited/serious/severe harm to agency operations, agency assets, or individuals?
 - Would unauthorized modification/destruction of elements of the information type violate laws, executive orders, or agency regulations?²

4.3.4

A: Availability

- Data and information systems are available when required; computing systems used to store and process information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.³
- Hardware maintenance, software patching/upgrading, and network optimization ensure availability.⁴

1.National Institute of Standards and Technology (NIST). *NIST SP 800 60: Information Security: Guide for Mapping Types of information and information Systems to Security Categories*. U.S. Department of Commerce. September 2008.

2.Ibid.

3.Ibid.

4.Techopedia.com. *Definition - What does Availability mean?*. <https://www.techopedia.com/definition/990/availability>.

- NIST Special Publication 800-60v1r1 defines the Security Objective of the Availability aspect of information:

Ensuring timely and reliable access to and use of information. ¹

Table 4.3: Availability Loss Impacts and Control Methods

Impacts of Information Availability Loss	Control Methods Used to Protect Availability
<ul style="list-style-type: none"> • Data loss • Unreachable data • Service interruption or loss (caused by Denial-of-Service Attacks) • Communication bottlenecks • Connection interruptions • Network intrusions • Loss of productivity • Loss of revenue 	<ul style="list-style-type: none"> • Hardware maintenance and repair • System upgrades • Provide adequate communication bandwidth • Redundancy and failover • High availability • Disaster Recovery • Business Continuity • Incident management • Data backups • Security equipment • Anti-malicious code detection

- NIST SP 800-60v1r1 provides questions to ask when assessing the Availability factors of information types, to evaluate the level of security impact associated with unauthorized disclosure of the information:
 - How can a malicious adversary use the disruption of access to or use of information to do limited/serious/severe harm to agency operations, agency assets, or individuals?
 - Would disruption of access to or use of elements of the information type violate laws, executive orders, or agency regulations?

1. National Institute of Standards and Technology (NIST). NIST SP 800 60: Information Security: Guide for Mapping Types of information and information Systems to Security Categories. U.S. Department of Commerce. September 2008.

4.4 Applying Controls

- 1. Control Families (NIST)
- 2. Cybersecurity Functions and Activities (NIST)
- 3. Cybersecurity Functions and Activities (ISO)

4.4.1 Control Families (NIST)

- NIST Control Application and Example

• AC – Access Control	• IA – Identification and Authentication	• PS – Personal Security
• AW – Awareness and Training	• IR – Incident Response	• RA – Risk Assessment
• AU – Audit and Accountability	• MA – Maintenance	• SA – System and Services Acquisition
• CA – Security Assessment and Authorization	• MP – Media Protection	• SC – System and Communications Protection
• CM – Configuration Management	• PE – Physical and Environmental Protection	• SI – System and Information Integrity
• CP – Contingency Planning	• PL – Planning	• PC – Privacy Controls

NIST Control Application and Example

- The approach described in NIST Special Publication 800-53 instructs organizations to first categorize their systems in terms of impact to Confidentiality, Integrity, and Availability, then establish a security control baseline of Low, Moderate, or High according to the associated risk levels. A Low Baseline requires the fewest number of controls be implemented, and the number increases up to the High baseline requirements. Controls suggested within each family are also prioritized, to assist in sequencing decisions for control implementation.

Control #	Control Name	Priority	Control Baselines		
			Low	Mod	High
Access Control					
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P2	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11	AC-11

- In this example, a system of Low Impact in this organization would only require implementation of control AC-8. A system of High Impact would require AC-8, followed by AC-10, then AC-11. Control AC-9 would not be required at all; it states, “The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access).”

1

4.4.2 Cybersecurity Functions and Activities (NIST)

- The NIST Cybersecurity Framework provides another way to view risk management. Appendix A, the Framework Core, represents a common set of activities used across all critical infrastructure sectors, for managing cybersecurity risk. NIST has grouped their 118 activities into 23 categories and 108 subcategories, which roll up into five functions:

Identify	Protect	Detect	Respond	Recover
Asset Management	Identity Management and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Protective Technology			

1.National Institute of Standards and Technology (NIST). *NIST SP 800: 53, 54, 55, 56, 57, 58*. U.S. Department of Commerce. 2015, 2019, 2008, 2018, 2016, 2005.

NIST Framework Application Example

- The following samples of NIST Cybersecurity Framework Function-Category-Subcategory groupings represent outcomes and activities that could be implemented to address risk associated with use of company-issued mobile devices:

Function	Category	Subcategories
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-3: Remote access is managed. PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
PROTECT (PR)	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-2, -3, -4, -5: Privileged users, third-party stakeholders, senior executives, physical and cybersecurity personnel understand their roles and responsibilities.

1

4.4.3 Cybersecurity Functions and Activities (ISO)

- The ISO 27001 Standard provides a list of 114 security controls organized within 14 sections of its Annex A. Implementation of the Information Security Management System prescribed by the Standard requires a risk assessment of the organization, and subsequent information security risk treatment plan. The controls necessary to implement the treatment plan are selected from the list based on the risk

1.National Institute of Standards and Technology (NIST). *NIST SP 800 53: Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*. U.S. Department of Commerce. December 2014.

they are intended to treat, known as the control objective.

• A.5 Information Security Policies	• A.10 Cryptography	• A.15 Supplier Relationships
• A.6 Organization of Information Security	• A.11 Physical and Environmental Security	• A.16 Information Security Incident Management
• A.7 Human Resource Security	• A.12 Operations Security	• A.17 Information Security Aspects of Business Continuity Management
• A.8 Asset Management	• A.13 Communications Security	• A.18 Compliance
• A.9 Access Control	• A.14 System Acquisition, Development, and Maintenance	

ISO 27001 Control Application Example

An asset-based Risk Assessment was being conducted; the asset group PII (personally identifiable information) was being examined for potential threats and vulnerabilities. Once the risk level was determined to be Medium for a particular threat, the treatment option chosen was to MITIGATE, and the proposed controls were identified to treat the risks associated with that risk.

Asset Group	PII
Threat	Data held on mobile or removable devices is prone to loss or theft of the device, or unauthorized access.
Vulnerabilities	No guidance is given to employees about how to protect their mobile devices.
Proposed Controls and Control Objectives	A.6.1 Internal Organization Control Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization. Control A.6.1.1 All information security responsibilities shall be defined and allocated.
	A.6.2 Mobile Devices and Teleworking Control Objective: To ensure the security of teleworking and use of mobile devices. Control A.6.2.1 A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices. Control A.6.2.2 A policy and supporting security measures shall be implemented to protect information accessed, processed, or stored at teleworking sites.

1

1. International Organization for Standardization (ISO). *The ISO/IEC 27000 family of standards*. ISO.org. <https://www.iso.org/isoiec-27001-information-security.html>.

4.5 Cybersecurity Threats: Part 1

1. Definitions and Key Terms
2. How Cyber Threats Work
3. Adversarial Threat Events
4. Adversarial Threat Characteristics
5. Non-Adversarial Threat Sources and Events
6. Threat Identification
7. Attack Tree Threat Identification Model

4.5.1 Definitions and Key Terms

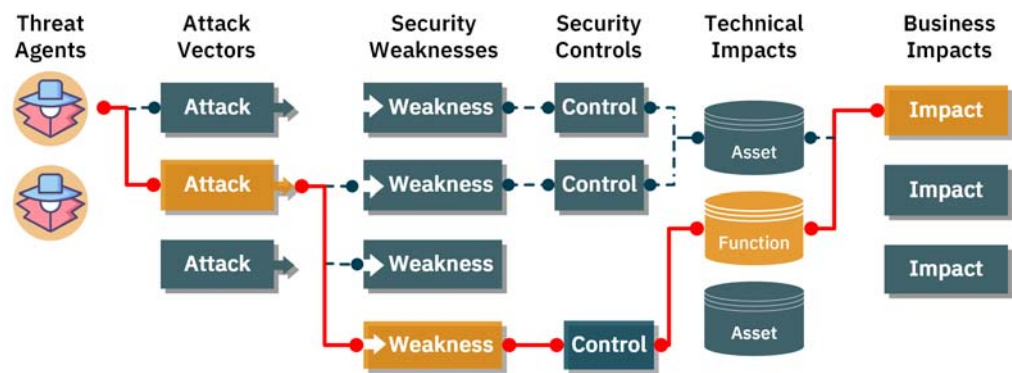
- **Cyber Threat:**
 - **ISO 27005:** A potential cause of an incident, that may result in harm of systems and organization.
 - **FIPS 200 (by NIST):** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit an information system vulnerability.
 - **National Information Assurance Glossary:** Any circumstance or event with the potential to adversely impact an Information System through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
- **Threat Event:** An event or situation that has the potential for causing undesirable consequences or impact.
 - Threat events are either intentional, known as Adversarial, or accidental, known as Non-Adversarial.
- **Threat Source:** The intent and method targeted at the intentional exploitation of a vulnerability, or a situation and method that may accidentally exploit a vulnerability.
- **Threat Agent:** An individual or group that can manifest a threat.
- **Adversarial Threat Sources:** Individuals, groups, organizations, or states that seek to exploit the organizations dependence on cyber resources:
 - Information in electronic form
 - Information and communication technologies
 - Communications and information-handling capabilities provided by the technologies

1

1. Committee on National Security Systems. *National Information Assurance (IA) Glossary*. Homeland Security Digital Library. April 2010.

4.5.2 How Cyber Threats Work

- Relationship between threat agent and business impact



4.5.3 Adversarial Threat Events

- Threats generally follow a flow where certain tactics, techniques, and procedures (TTP) are deployed to advance the attack through to realization of an event¹:

Adversarial Threat Event/Campaign Stages	Example Tactics, Techniques and Procedures (TTP)
Perform Reconnaissance and Gather Information	Perimeter network scanning, open source info discovery, surveillance, malware-directed internal reconnaissance.
Craft or Create Attack Tools	Craft phishing and other attacks and counterfeit entities, create and operate false-fronts to inject malicious components.
Deliver/Insert/Install Malicious Capabilities	Deliver known malware into internal systems, insert tampered hardware, install sniffers, insert subverted individuals.
Exploit and Compromise	Exploit physical access and vulnerabilities, compromise information systems, critical information, and components.
Conduct and Attack (Direct/Coordinate Attack Tool activities)	Conduct attacks: interception, Denial of Service, physical, data scavenging, session hijacking, network traffic, social engineering.

1.National Institute of Standards and Technology (NIST). NIST SP 800 30: Information Security: Guide for Conduction Risk Assessments. U.S. Department of Commerce. September 2012.

Adversarial Threat Event/Campaign Stages	Example Tactics, Techniques and Procedures (TTP)
Achieve Results (Cause adverse impacts, Obtain Information)	Obtain information, cause degradation and integrity loss, cause disclosure, obtain unauthorized access.
Maintain a presence or set of capabilities	Obfuscate adversary actions, adapt attacks based on surveillance.
Coordinate a Campaign	Multi-staged, continuous, adaptive attacks, spread attacks.

4.5.4

Adversarial Threat Characteristics

- When conducting a threat risk analysis, it is useful to assess the potential threat agent, or adversary, to factor in another measure of risk to the equation. Three characteristics can be scored to help define the power of the threat posed by the adversary: their Capability, their Intent, and Targeting. An assessor would assign overall value of High, Moderate or Low for each, considering what is known about the adversary's characteristics below.

Capability	Intent	Targeting
<ul style="list-style-type: none"> Level of expertise Resource availability Ability to generate opportunities 	<ul style="list-style-type: none"> The severity of harm and scope of impact the adversary seeks to cause (undermine, impede, destroy, obtain, modify, usurp, disrupt, deface) The degree of intrusion it intends to achieve (exploit a presence, maintain a presence, establish a foothold) When the adversary intends to exploit or carry out the attack (immediate, future, over a long time period) The level of concern the adversary has for being detected, or for disclosure of their tradecraft 	<ul style="list-style-type: none"> Any classifying the adversary does on the organization, their assets, mission or business functions, employees or partners The extent of analysis the adversary conducts The sources the adversary uses to obtain analysis information, and the methods they use to obtain it

4.5.5 Non-Adversarial Threat Sources and Events

- The following table provides common examples of non-adversarial (accidental) threat sources and non-adversarial threat events that tend to occur, which should also be considered in risk assessments.

Non-Adversarial Threat Sources	Non-Adversarial Threat Events
Accidental: erroneous actions taken during execution of daily tasks	<ul style="list-style-type: none">• Authorized user erroneously spills or mishandles sensitive information, or assigns incorrect privileges to another user• Degraded communications performance due to contention
Environmental: natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization	<ul style="list-style-type: none">• Natural disaster: fire, flood, earthquake, hurricane, tornado
Structural: failures of equipment, environmental controls, resource depletion	<ul style="list-style-type: none">• Degraded processing performance due to resource depletion• Corrupted storage due to disk errors, caused by aging devices• Introduction of vulnerabilities into software products due to inherent weaknesses in programming languages and development environments• Unreadable display due to aging equipment

1

4.5.6 Threat Identification

- When conducting a threat assessment, you want to make sure you are including all possible threats that pose relevant risk to your organization. There are a few models that prompt teams to consider a range of categories to maximize outputs.
- STRIDE was developed by Microsoft and is a mnemonic for identifying computer threats in six categories. It is often used by security experts to help answer the question, “What can go wrong in this system we’re

1.National Institute of Standards and Technology (NIST). NIST SP 800 30: Information Security: Guide for Conduction Risk Assessments. U.S. Department of Commerce. September 2012.

working on?”. Each threat is a violation of a desirable property for a system.

Initial	Threat Category	Desired System Property Violated
S	Spoofing of User Identity	Authenticity
T	Tampering	Integrity
R	Repudiation	Non-reputability
I	Information Disclosure (privacy breach or data leak)	Confidentiality
D	Denial of Service (D.o.S.)	Availability
E	Elevation of Privilege	Authorization

1

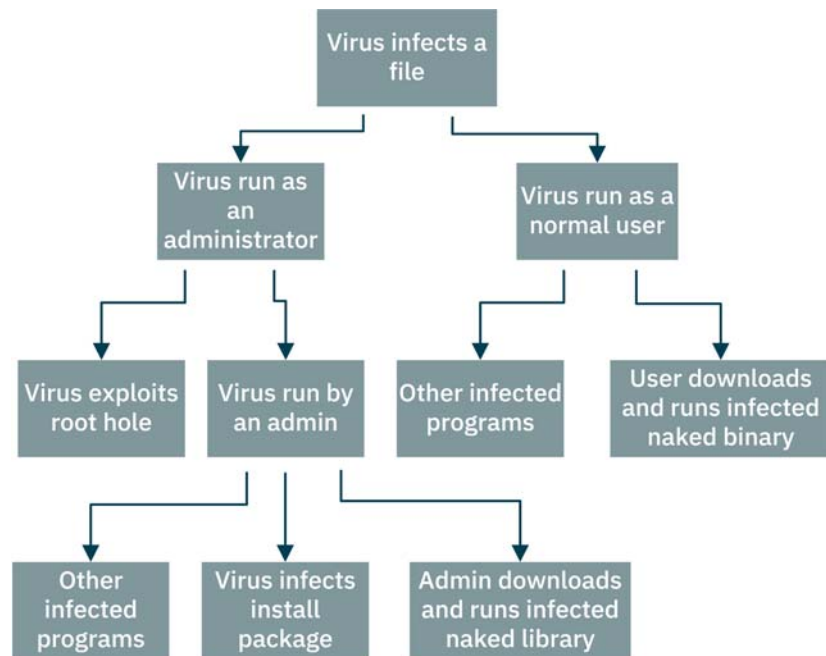
4.5.7 Attack Tree Threat Identification Model

- Attack Tree is another model, which uses multi-level conceptual diagrams to show how an asset, or target, might be attacked.
- A tree consists of one root, leaves, and children; from the bottom up, child nodes are conditions which must be satisfied to make the direct parent node true.
- When the root is satisfied, the attack is complete. Each node may be satisfied only by its direct child node(s).
- A node may be a child of another node, in which case multiple steps must be taken to carry out an attack.
- An attack described in a node may require one or more of many attacks described in a child node to be satisfied.

2

1.Praerit Garg and Loren Kohnfelder. *The STRIDE Threat Model*. Microsoft Corporation. November 2009. [https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878\(v=cs.20\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN).
 2.Bruce Schneier. *Attack Trees*. Dr. Dobb's Journal. December 1999. https://www.schneier.com/academic/archives/1999/12/attack_trees.html.

- Microsoft cybersecurity professionals used Attack Tree analysis to develop STRIDE.



4.6 Cybersecurity Threats: Part 2

1. Threat Likelihood
2. Threat Likelihood Assessment Scales
3. Determining Overall Likelihood
4. Threat Relevance
5. Threat Modelling for Application Development

4.6.1 Threat Likelihood

- Understanding the threats that pose risk to your organization is critical to building a secure infrastructure. However, investing in all the controls that a risk assessment may recommend can be quite costly. An important factor when sizing and prioritizing which controls to implement is Likelihood, and there are two aspects of it to consider:
 - The likelihood of a threat event occurring within your system – ATTACK INITIATION LIKELIHOOD; and then,
 - The likelihood that an event, should it occur, results in an adverse impact – INITIATED ATTACK SUCCESS LIKELIHOOD.
- Likelihood can be measured by the capabilities of the threat and the presence or absence of countermeasures. Likelihood can also be based on historical evidence and trends of threat events occurring in environments like yours, and the typical impacts they have resulted in. NIST provides an assessment scale for each consideration of likelihood, to factor into overall risk calculations.

1

2

1. National Institute of Standards and Technology (NIST). *NIST SP 800 30: Information Security: Guide for Conduction Risk Assessments*. U.S. Department of Commerce. September 2012.

2. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

4.6.2 Threat Likelihood Assessment Scales

- This NIST table shows how qualitative or quantitative scales can be used to factor in likelihood to risk assessments.

Qualitative Values	Quantitative Values	Likelihood of ATTACK INITIATION Descriptions	Likelihood of INITIATED ATTACK SUCCESS Descriptions (IF the threat event is initiated or occurs...)
Very High	10	Adversary is almost certain to initiate the threat event.	It is almost certain to have adverse impacts.
High	8	Adversary is highly likely to initiate the threat event.	It is highly likely to have adverse impacts.
Moderate	5	Adversary is somewhat likely to initiate the threat event.	It is somewhat likely to have adverse impacts.
Low	2	Adversary is unlikely to initiate the threat event.	It is unlikely to have adverse impacts.
Very Low	0	Adversary is highly unlikely to initiate the threat event.	It is highly unlikely to have adverse impacts.

1

4.6.3 Determining Overall Likelihood

- The Overall Likelihood is needed for later use, when combined with the Impact of an adverse event, to determine the Risk Level of each identified threat

Likelihood of Threat Event Initiation or Occurrence	Likelihood of Threat Events on Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

2

- 1.National Institute of Standards and Technology (NIST). *NIST SP 800 30: Information Security: Guide for Conduction Risk Assessments*. U.S. Department of Commerce. September 2012.
- 2.National Institute of Standards and Technology (NIST). *NIST SP 800 30: Information Security: Guide for Conduction Risk Assessments*. U.S. Department of Commerce. September 2012.

- These examples show that a threat event with High Likelihood of Initiation, but Low Likelihood that it would result in Adverse Impact, is considered to have a MODERATE Overall Likelihood, and a threat event with Low Likelihood of Initiation, but Very High Likelihood of it resulting in an Adverse Impact, is also considered to have a MODERATE Overall Likelihood.

4.6.4 Threat Relevance

- Relevance is another factor that can be included in an Adversarial Risk Assessment, perhaps if there is further prioritization between two threats that otherwise score the same overall risk; it is a measure of how relevant a potential threat Tactic, Technique, or Procedure (TTP) is to an organization.¹

Relevance Value Assigned	Description of the threat Tactic, Technique, or Procedure (TTP) Relevance to the Organization
Confirmed	It has been seen by the organization.
Expected	It has been seen by the organization's peers or partners.
Anticipated	It has been reported by a trusted source.
Predicted	It has been predicted by a trusted source.
Possible	It has been described by a somewhat credible source.
N/A	The threat event, tactic, technique, or procedure is not currently applicable.

4.6.5 Threat Modelling for Application Development

- Threat modeling is a threat identification and prioritization process which is conducted from the perspective of a potential attacker.
 - Its outputs include systematic analysis of an attacker's profile, probable attack vectors, most vulnerable areas, and the assets most likely to be targeted, which are typically the highest in value.
- (ISC)² provides a step process to follow when applying the model:
 1. Define Assessment Scope: assets, capabilities
 2. Identify Threat Agents and Possible Attacks
 3. Understand existing countermeasures
 4. Identify exploitable vulnerabilities
 5. Prioritize Identified Risks
 6. Identify Countermeasures to Reduce Threat

2

1. National Institute of Standards and Technology (NIST). *NIST SP 800 30, 32, 94*. U.S. Department of Commerce. 2012, 2001, 2007.

2. ICS. Official (ISC)² Guide to the CISSP CBK, Fourth Edition. Auerbach Publications. March 2015.

4.7 Cybersecurity Vulnerabilities: Part 1

1. Definitions
2. Identifying Vulnerabilities
3. Classification of Vulnerabilities
4. Causes of Vulnerabilities
5. Vulnerability Assessments

4.7.1 Definitions

- **Vulnerability:**

- A weakness of an asset or group of assets that can be exploited by one or more threats, where an asset is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission. ¹
- A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. ²
- A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events. ³

4.7.2 Identifying Vulnerabilities

- NIST suggests identifying vulnerabilities at three tiers/levels of the business:
 - Organization Level: governance, missions, functions, policies, procedures, relationships
 - Mission/Business Process Level: enterprise architecture segments, infrastructure, support services, common controls
 - Information System Level: technologies, system components, applications, networks, environments

4

1. International Organization for Standardization (ISO). *ISO 27005: Information technology — Security techniques — Information security risk management*. International Organization for Standardization (ISO). 2018.

2. National Institute of Standards and Technology (NIST). *NIST SP 800 53: Recommended Security Controls For Federal Information Systems And Organizations*. August 2009.

3. ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

4. National Institute of Standards and Technology (NIST). *NIST SP 800 30: Information Security: Guide for Conduction Risk Assessments*. U.S. Department of Commerce. September 2012.

- It is also common to identify vulnerabilities as they relate to five key categories:
 - People
 - Process
 - Data
 - Technology
 - Facilities

1

4.7.3 Classification of Vulnerabilities

- To further assist in thorough analysis to identify vulnerabilities, they can be classified according to the asset class to which they are related:
 - Hardware
 - susceptibility to humidity
 - susceptibility to dust
 - susceptibility to soiling
 - susceptibility to unprotected storage
 - Software
 - insufficient testing
 - lack of audit trail
 - design flaw
 - Network
 - unprotected communication lines
 - insecure network architecture
 - Personnel
 - inadequate recruiting process
 - inadequate security awareness
 - Physical site
 - area subject to flood
 - unreliable power source
 - Organizational
 - lack of regular audits
 - lack of continuity plans
 - lack of security

2

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

2. International Organization for Standardization (ISO). *ISO/IEC FIDIS 27005. Information technology - Security techniques - Information Security risk management 3rd Edition*. International Organization for Standardization (ISO). 2018.

4.7.4 Causes of Vulnerabilities

- Human error: designers, operations, users
- System complexity
- Use of code that is very common and therefore familiar to attackers
- Quantity and access frequency of connection points, like ports, privileges, services, protocols
- Flaws in password standards and management
- Fundamental design flaws in the operating system, such as less than optimal access policies
- Exposure to viruses and malware via web browsing
- Exploitable software bugs that are not remediated
- Unchecked user input

4.7.5 Vulnerability Assessments

- The primary purpose of vulnerability assessments is to understand the nature and degree to which organizations, mission/business processes, and information systems are vulnerable to threat sources and the threat events that can be initiated by those threat sources.
- Multiple threat events can exploit a single vulnerability, and conversely, multiple vulnerabilities can be exploited by a single threat event.
- Vulnerabilities can be identified at varying degrees of granularity and specificity.
- The level of detail provided in any vulnerability assessment should be consistent with the purpose of the risk assessment and the type of inputs needed to support follow-on likelihood and impact determinations.
- Many risk assessments tend to rely on threat-vulnerability pairs as the focal point of the assessments.
- Organizations determine which vulnerabilities are relevant to which threat events in order to reduce the space of potential risks to be assessed.

1

1.National Institute of Standards and Technology (NIST). *NIST SP 800 30: Information Security: Guide for Conduction Risk Assessments*. U.S. Department of Commerce. September 2012.

4.8 Cybersecurity Vulnerabilities: Part 2

1. Predisposing Conditions
2. Types of Predisposing Conditions
3. Severity and Pervasiveness
4. Vulnerability Assessments vs Scans
5. Vulnerability Scanning
6. Penetration Testing

4.8.1 Predisposing Conditions

- Predisposing condition: A condition that exists within a business process, enterprise architecture, information system, or environment of operation, which affects the likelihood that threat events, once initiated, result in adverse impacts to organizational operations and assets. Predisposing condition examples include:
 - the location of a facility in a hurricane- or flood-prone region (increasing the likelihood of exposure to hurricanes or floods)
 - a stand-alone information system with no external network connectivity (decreasing the likelihood of exposure to a network-based cyber-attack)
- Predisposing conditions are tied to vulnerabilities in risk assessments in that they are a characteristic of a known vulnerability, but it is the likelihood that threat events will result in adverse impacts that they influence. In other words, they affect susceptibility to vulnerabilities. Examples of Vulnerabilities resulting from predisposing conditions include:
 - gaps in contingency plans
 - weaknesses/deficiencies in information system backup and failover mechanisms

1

1.Ibid.

4.8.2 Types of Predisposing Conditions

- The following table provides common examples of predisposing conditions that should be considered in risk assessments.

Types of Predisposing Conditions	Examples
INFORMATION RELATED Needs to handle information in a specific manner due to its sensitivity, legal requirements, contractual obligations, etc.	<ul style="list-style-type: none">• Classified Information• Controlled Unclassified Information• Personally Identifiable Information (PII)• Agreement-Determined
TECHNICAL Needs to use technologies in specific ways.	<ul style="list-style-type: none">• Architectural: compliance with technical standards, allocation of security functionality• Functional: networked multi-user, single-user, stand-alone, restricted
OPERATIONAL/ENVIRONMENTAL Ability to rely upon physical, procedural, and personnel controls provided by the operational environment.	<ul style="list-style-type: none">• Mobility: fixed-site, semi-mobile, mobile• Population with physical and/or logical access to components of the information system, process, etc.

- Where other risk factors are measured by severity, predisposing conditions are measured by pervasiveness of the condition; in other words, the breadth of organizational processes or systems to which the predisposing condition applies.

1

4.8.3 Severity and Pervasiveness

- In risk assessment, once vulnerabilities and predisposing conditions are identified, they are assigned a score using a scale such as described in the NIST tool:

Qualitative Values	Quantitative Values	Vulnerability SEVERITY	PERVASIVENESS of Predisposing Conditions
Very High	10	Relevant security control or other remediation is not implemented and not planned.	Applies to all organizational missions/business functions, processes or information systems.
High	8	Control or remediation is <i>planned</i> but <i>not implemented.</i>	Applies to most missions, functions, processes or systems.

1.Ibid.

Qualitative Values	Quantitative Values	Vulnerability SEVERITY	PERVASIVENESS of Predisposing Conditions
Moderate	5	Control/remediation is partially implemented and somewhat effective .	Applies to many missions, functions, processes or systems.
Low	2	Control/remediation is fully implemented and somewhat effective.	Applies to some missions, functions, processes or systems.
Very Low	0	Control/remediation is fully implemented, assessed and effective.	Applies to few missions, functions, processes or systems.

1

4.8.4 Vulnerability Assessments vs Scans

- Where a Vulnerability Assessment includes all aspects of a business, including people, processes, and technology, Vulnerability Scans focus on technology solutions that are already in place, or about to be implemented.
- Vulnerability scanners are automated tools which contain extensive databases of specific known vulnerabilities and can analyze system and network configuration information to predict where a system might be vulnerable to different types of attacks.
- Vulnerability Scan results are combined with the results of the more business-focused Vulnerability Assessment, to gain a comprehensive understanding of the organization's actual vulnerabilities.

2

4.8.5 Vulnerability Scanning

- Vulnerability scanner:
 - A computer program designed to identify and detect vulnerabilities arising from mis-configurations or flawed programming within a network-based asset
 - Typically available as SaaS (Software as a Service)
 - Often attempts to determine if a system has the latest security patch in place
 - Allows for both authenticated and unauthenticated scans

3

1.Ibid.

2.ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

3.ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

- Authenticated scans:
 - Directly access network-based assets using secure shell (SSH) or remote desktop protocol (RDP)
 - Authenticate using provided system credentials
 - Provide detailed and accurate information about the operating system and installed software, including configuration issues and missing security patches ¹
- Unauthenticated scans:
 - Typically used by threat actors or security analysts trying to determine the security posture of externally accessible assets
 - Unable to provide detailed information about the asset's operating system and installed software

2

4.8.6 Penetration Testing

- A penetration test, also known as a pen test, is a specific type of vulnerability scan:
 - An authorized, simulated attack to gain assurance in the security of an IT system by attempting to breach some or all of its security, using the same tools and techniques that an adversary might.
 - Used to identify the level of technical risk emanating from software and hardware vulnerabilities, which are known on the day of the test.
 - Can give confidence that the implemented controls have been configured effectively, and suggest countermeasures for those that are not.
 - Ideally the system's vulnerabilities should already be known, so the test results should be as expected, and simply act as a verification.

3

1. Scarfone, Karen, Murugiah Souppaya, Amanda Cody, and Angela Orebaugh. *Special Publication 800-115, Technical Guide to Information Security Testing and Assessment, Recommendations of the National Institute of Standards and Technology*. NIST. September 2008. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>

2. Ibid.

3. National Cyber Security Centre. *Penetration Testing: Advice on how to get the most from penetration testing*. August 2017. <https://www.ncsc.gov.uk/guidance/penetration-testing>.

- The process of penetration testing may be simplified into five phases:
 - Reconnaissance: The act of gathering important information to better attack a target system.
 - Scanning: Uses technical tools to further the attacker's knowledge of the system.
 - Gaining Access: Using the data gathered in the reconnaissance and scanning phases, the attacker can use a payload to exploit the targeted system.
 - Maintaining Access: Requires taking the steps involved in being able to be persistently within the target environment in order to gather as much data as possible.
 - Covering Tracks: The attacker must clear any trace of compromising the victim system, any type of data gathered, log events, in order to remain anonymous.

1

- Once an attacker has exploited one vulnerability, they may gain access to other machines, so the process repeats i.e. look for new vulnerabilities and attempt to exploit them. This process is referred to as pivoting.

1. Ryan. *Summarizing the Five Phases of Penetration Testing*. Cybrary. May 2015.
<https://www.cybrary.it/2015/05/summarizing-the-five-phases-of-penetration-testing/>

4.9 Adverse Impacts

1. Overview
2. Risk-Controls Model
3. Determining Impacts
4. Types of Adverse Impacts
5. Impact Assessment Scales

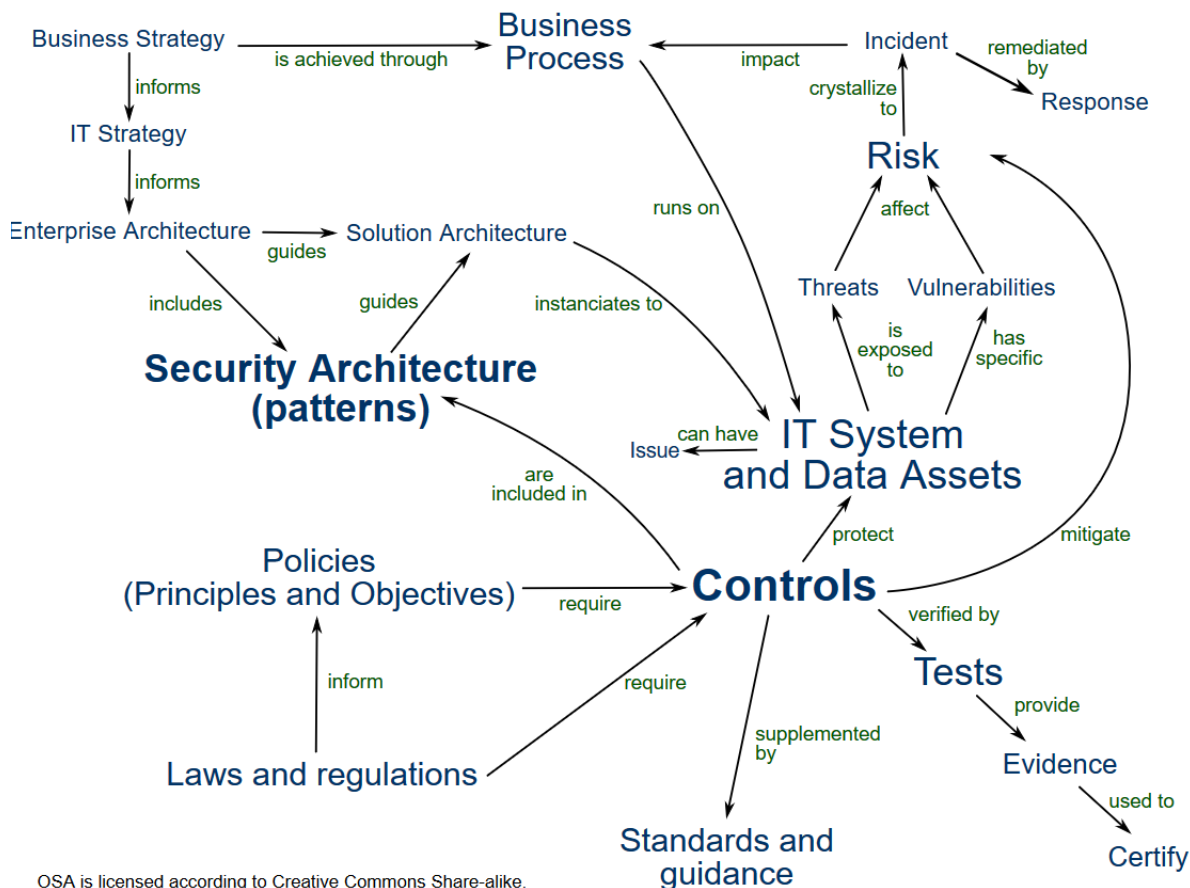
4.9.1 Overview

- Impact to business operations or assets is a factor when identifying controls to treat risks.
- The higher the negative potential impact, the more controls required to protect against the associated threats.
- Overall risk posed by a threat is a product of the likelihood of its occurrence and the severity of its potential adverse impact on the organization.
- Organizations can describe adverse impacts in terms of:
 - the potential harm caused to organizational operations and assets, individuals, other organizations, or
 - failure to achieve one or more security objectives (i.e., confidentiality, integrity, or availability)
- When conducting Impact Analysis, NIST goes on to suggest that organizations state:
 - the process used to conduct impact determinations;
 - assumptions related to impact determinations;
 - credible sources and methods for obtaining impact information; and
 - the rationale for the conclusions reached regarding impact determinations.

1

1. National Institute of Standards and Technology (NIST). *NIST SP 800 30: Information Security: Guide for Conduction Risk Assessments*. U.S. Department of Commerce. September 2012.

4.9.2 Risk-Controls Model



4.9.3 Determining Impacts

- The impact of any threat, whether Adversarial or Non-Adversarial, is assessed for each identified threat in the assessment. Impact of a potential threat should be determined by considering the three tiers of business:
 - Tier 1: Organization Level
 - Impact information related to organizational governance, core mission/business functions, management and operational policies, procedures and structures, external mission/business relationships.
 - Tier 2: Mission/Business Process Level
 - Impact information related to mission/business processes, enterprise architecture segments, common infrastructure, support services, common controls, and external dependencies.

- Tier 3: Information System Level
 - Information affecting information systems, technologies, components, applications, networks, environments. Sources are historical data, security assessment reports.

1

4.9.4 **Types of Adverse Impacts**

- NIST SP 800-30 provides a comprehensive list of examples of Adverse Impacts for reference while organizations are coming up with impacts to identified threats.

Type of IMPACT	Examples
HARM TO OPERATIONS	<ul style="list-style-type: none">• Inability to perform current or future missions/business functions• Harms due to noncompliance (e.g. financial costs, sanctions)• Direct financial costs• Relational harms: damage to trust relationships or reputation
HARM TO ASSETS	<ul style="list-style-type: none">• Damage to or loss of physical facilities, information systems, networks, technology, equipment, component parts or supplies, or information assets• Loss of intellectual property (IP)
HARM TO INDIVIDUALS	<ul style="list-style-type: none">• Identity theft or loss of Personally Identifiable Information (PII)• Injury or loss of life; physical or psychological mistreatment• Damage to image or reputation
HARM TO OTHER ORGANIZATIONS	<ul style="list-style-type: none">• Harms due to noncompliance (e.g. financial costs, sanctions)• Direct financial costs• Relational harms: damage to trust relationships or reputation
HARM TO THE NATION	<ul style="list-style-type: none">• Damage or incapacitation of a critical infrastructure sector• Loss of government continuity of operations• Relational harms: damage to trust relationships or reputation

2

1.National Institute of Standards and Technology (NIST). *NIST SP 800 30: Information Security: Guide for Conduction Risk Assessments*. U.S. Department of Commerce. September 2012.
2.Ibid.

4.9.5 Impact Assessment Scales

- NIST provides assessment scales for two attributes of Impact when assigning an overall Impact score in a risk analysis; the overall Impact combined with overall threat likelihood produce the overall risk level:

Qualitative Values	Quantitative Values	Impact SEVERITY of Threat Events	RANGE of Impacts of Threat Events
Very High	10	Threat expected to have multiple severe or catastrophic adverse effects.	Effects are sweeping, involving almost all organizational cyber resources.
High	8	Threat expected to have severe or catastrophic adverse effects.	Effects are extensive, involving most organizational cyber resources, including many critical resources.
Moderate	5	Threat expected to have a serious adverse effect.	Effects are substantial, involving significant organizational cyber resources, including some critical resources.
Low	2	Threat expected to have a limited adverse effect.	Effects are limited, involving some organizational cyber resources, but no critical resources.
Very Low	0	Threat expected to have a negligible adverse effect.	Effects are minimal or negligible, involving few if any organizational cyber resources, and no critical resources.

1

1.Ibid.

4.10 Risks and Controls – Putting It All Together

1. Business Analysis Practitioner (BA) Focal Points
2. Overview
3. Calculating Risk
4. Overall Likelihood and Level of Impact
5. Risk Level = Likelihood x Impact
6. Risk-Controls Model
7. Assigning Targeted Controls
8. Technology Controls
9. Process Controls

4.10.1 Business Analysis Practitioner (BA) Focal Points

- As a Business Analysis Practitioner (BA) you may lead or participate in Security Risk Assessments.
- The assessments may be at an organizational level, business unit level, mission level, or as part of a project-specific solution design initiative.
- Use a methodology that aligns with the organization's standard approaches or formats.
- Use the set of controls that has been approved by IT Security leadership.
- Ensure all key stakeholders are identified and engaged in the identification of threats, vulnerabilities and determination of treatment options.
- Prioritize control assignment and implementation with business objectives and priorities, getting appropriate input and approval from those accountable.
- Strive to engage in Security Risk and Control analysis activities early and often in solution design projects' lifecycles.
- Seek to align control strategies with enterprise architecture roadmaps.
- Be prepared to conduct cost-benefit analysis on control selection and prioritization efforts.
- Risk Assessments and Control Plans are living documents and need to be updated regularly, at least annually, to ensure risks remain current and applied controls remain valid and have not degraded in effectiveness over time.

4.10.2

Overview

- Security controls are technical and/or process tools that are implemented to provide targeted protection against specific threats to organizations’ assets and business operations.
- Control selection requires thorough analysis of system vulnerabilities, the threats that put systems at risk, and the impact on business should a threat event occur.
- There are various tools and methodologies available to aid in conducting these IT Security Risk assessments.
- A common framework is the NIST SP 800-30 Guide for Conducting Risk Assessments.
- The ISO 27001 standard, Annex A provides an extensive list of common controls that are designed to target and be assigned to each threat risk identified.
- The preceding modules in Part 4 of this course described each factor of risk calculations and how they can be derived.
- The following table shows how to tabulate the factors to determine risks, which can then be prioritized for targeted control assignment.

4.10.3

Calculating Risk

- For each identified Threat Event, establish a risk level using the values determined in previous steps, as shown below:

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood of Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								
	↓					↓	↓	↓		↓		↓
	...that could initiate the event				Likelihood one or more of the threat sources initiates the threat event	...which could be exploited	...of vulnerabilities and of predisposing conditions		...that an event will be initiated and will result in adverse impact			Risk = Likelihood x Impact

1

1.Ibid.

4.10.4 Overall Likelihood and Level of Impact

- Risk posed by a threat event is the product of overall likelihood and the level of impact that event would have on the organization; take these two values from previous assessment steps:

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood of Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								

1

4.10.5 Risk Level = Likelihood x Impact

- Risk Level is assessed as a combination of Overall Likelihood and Impact:

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	<i>Very Low</i>	<i>Low</i>	<i>Moderate</i>	<i>High</i>	<i>Very High</i>
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

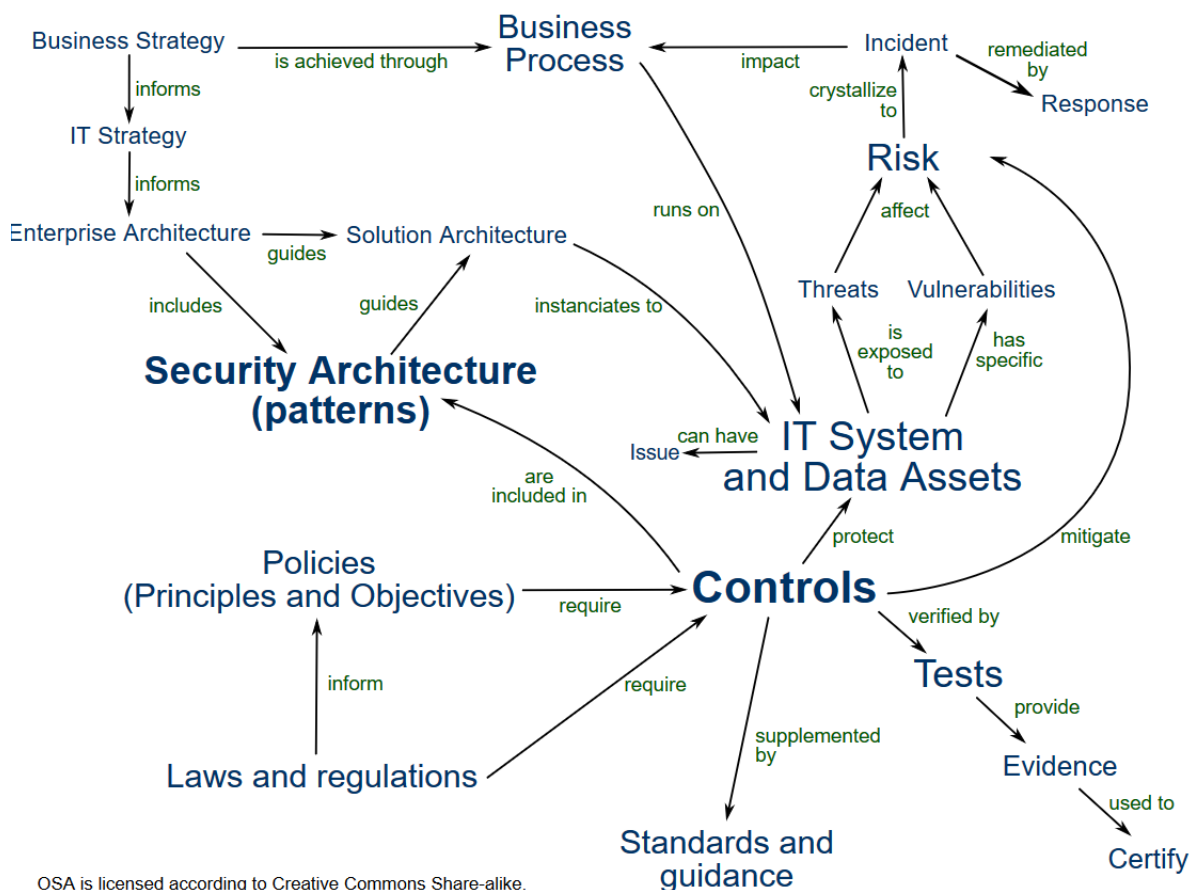
- Two examples above illustrate how the Risk Level is determined:
 - A threat event with Moderate Overall Likelihood, which would result in a Very High level of adverse impact, is considered a HIGH Risk; and
 - A threat event that has a Very Low Overall Likelihood and would cause Moderate impact, is considered a VERY LOW risk.
- Risk levels are used to prioritize risk treatment and control assignment for each threat.

2

1.Ibid.

2.Ibid.

4.10.6 Risk-Controls Model



4.10.7 Assigning Targeted Controls

- Some examples of ISO 27001 Annex A Controls, recommended for specific threats:

Threat	Vulnerability	Risk Type	Annex A Control	Control Type
It is not clear who should be doing what with respect to information security	Roles and responsibilities for information security have not been clearly defined	Confidentiality, Integrity and Availability	A.6.1.1 Information security roles and responsibilities	Process
Logon to secure systems is possible by unauthorized users	Some potentially sensitive HR information is available via a hyperlink without logging on	Confidentiality and Integrity	A.9.4.2 Secure log-on procedures	Technology

Threat	Vulnerability	Risk Type	Annex A Control	Control Type
Systems are affected by malware e.g. ransomware or spyware, having a serious effect on service delivery and security	The anti-malware program in use does not have a good reputation for effectiveness	Confidentiality, Integrity and Availability	A.12.2.1 Controls against malware	Technology
The processor uses sub-contractors that do not provide adequate protection for PII	Little due diligence is performed when engaging sub-contractors	Confidentiality, Integrity and Availability	A.7.1 Disclosure of sub-contracted PII processing	Process

1

4.10.8 Technology Controls

- Some common examples of Technology-enabled Information Security Controls:

NIST Examples		ISO 27001 Examples	
Family	Controls	Annex	Controls
Access Control	<u>AC-2</u> Account Management <u>AC-11</u> Session Lock <u>AC-19</u> Access Control for Mobile Devices	A.9 Access Control	<u>A.9.2.2</u> User Access Provisioning <u>A.9.3.1</u> Use of Secret authentication information
Audit and Accountability	<u>AU-2</u> Auditable Events <u>AU-8</u> Time Stamps	A.12 Operations Security	<u>A.12.1.4</u> Separation of Dev, Test, and Operational Environments <u>A.12.2.1</u> Controls against Malware

1. International Organization for Standardization (ISO). *ISO/IEC 27000: Information technology, SC 27, IT Security techniques*. International Standards Organization (ISO). 2018.

NIST Examples		ISO 27001 Examples	
Family	Controls	Annex	Controls
Identification and Authentication	<u>IA-3</u> Device Authentication and Authorization	A.13 Communications Security	<u>A.13.1.1</u> Network Controls
	<u>IA-7</u> Cryptographic Module Authentication		<u>A.13.2.3</u> Electronic Messaging
System and Communications Protection	<u>SC-5</u> Denial of Service Protection	A.14 System Acquisition, Development and Maintenance	<u>A.14.1.2</u> Securing Application services on Public Networks
	<u>SC-17</u> Public Key Infrastructure		<u>A.14.2.9</u> System Acceptance Testing
	<u>SC-28</u> Protection of Information at Rest		
	<u>SC-32</u> Information System Partitioning		

1

2

4.10.9 Process Controls

- Some common examples of Process-enabled Information Security Controls:

NIST Examples		ISO 27001 Examples	
Family	Controls	Annex	Controls
Awareness and Training	AT-1 Security Awareness and Training Policy and Procedures	A.7 Human Resources Security	A.7.1.1 Screening
	AT-4 Security Training Records		A.7.2.2 Information Security awareness, education, and training
Security Assessment and Authorization	CA-2 Security Assessments	A.11 Physical and Environmental Security	A.11.1.2 Physical Entry Controls
	CA-5 Plan of Action and Milestones		A.11.2.3 Cabling Security
	CA-6 Security Authorization		A.11.2.9 Clear Desk and Screen Policy

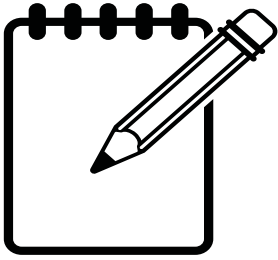
-
- 1.National Institute of Standards and Technology (NIST). *NIST SP 800 30: Information Security: Guide for Conduction Risk Assessments*. U.S. Department of Commerce. September 2012.
 - 2.International Organization for Standardization (ISO). *ISO/IEC 27000: Information technology, SC 27, IT Security techniques*. International Standards Organization (ISO). 2018.

NIST Examples		ISO 27001 Examples	
Family	Controls	Annex	Controls
Configuration Management	CM-1 Configuration Management Policy and Procedures	A.15 Supplier Relationships	A.15.1.1 Information Security Policy for Supplier Relationships
	CM-8 Information System Component Inventory		
Physical and Environmental Protection	PE-7 Visitor Control	A.16 Information Security Incident Management	A.16.1.3 Reporting Information Security Weaknesses
	PE-13 Fire Protection		
	PE-18 Location of Information Systems Components		A.16.1.5 Response to Information Security Incidents
Personnel Security	PS-2 Position Categorization	A.18 Compliance	A.18.1.4 Privacy and Protection of Personally Identifiable Information
	PS-3 Personnel Screening		

1

2

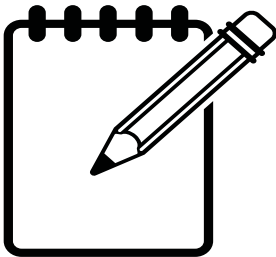
-
- 1.National Institute of Standards and Technology (NIST). *NIST SP 800 30: Information Security: Guide for Conduction Risk Assessments*. U.S. Department of Commerce. September 2012.
 - 2.International Organization for Standardization (ISO). *ISO/IEC 27000: Information technology, SC 27, IT Security techniques*. International Standards Organization (ISO). 2018.



NOTES

[illegible]

NOTES



A series of horizontal dashed lines for taking notes.

5

Module 5: Securing the Layers

1. Physical Security
2. Endpoint Security
3. Network Security: Security Architecture
4. Network Security: Firewalls
5. Network Security: Anti-Virus/Anti-Malware
6. Network Security: Segregation
7. System Security: Servers
8. Platform Security
9. Product Security: Threat Models
10. Product Security: Embedded Systems
11. Product Security: Internet of Things

5.1

Physical Security

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

5.1.1

Business Analysis Practitioner (BA) Focal Points

- Understanding, development, and implementation of Physical Security Policies, Processes, and Controls
- Understanding of applicable regulatory and industry-specific requirements
- Requirements analysis for IAM, PKI, solutions
- Disaster Recovery, Business Continuity Planning

5.1.2 Key Terms and Definitions

- **Assets:** In this context, assets are pieces of IT equipment, including network infrastructure components, security infrastructure components, physical buildings/rooms/racks, laptops and personal computers, mobile devices, etc.
- **Physical Access:** Access into a network connection or wiring area or to proximity to LAN resources or systems.

5.1.3 Use Cases

- The following use cases pertaining to physical security are taken from the NIST Cybersecurity Framework v1.0
 1. IDENTIFY (ID)-ASSET MANAGEMENT (AM)-1 Physical devices and systems within the organization are inventoried; -5 Resources (hardware, devices) are prioritized based on their classification, criticality, and business value
 2. IDENTIFY-RISK ASSESSMENT (RA)-1 Asset vulnerabilities are identified and documented
 3. PROTECT (PR)-ACCESS CONTROL (AC)-1 Identities and credentials are managed for authorized devices and users; -2 Physical access to assets is managed and protected
 4. PROTECT-AWARENESS and TRAINING (AT)-5 Physical and information security personnel understand roles and responsibilities
 5. PROTECT-DATA SECURITY (DS)-3 Assets are formally managed throughout removal, transfers, and dispositions
 6. PROTECT-INFORMATION PROTECTION (IP)-5 Policy and regulations regarding the physical operating environment for organizational assets are met; 9 Response plans (incident response and business continuity) and recovery plans (incident recovery and disaster recovery) are in place and managed
 7. PROTECT-MAINTENANCE (MA)-1 Maintenance and repair of organizational assets is performed and logged in a timely manner with approved and controlled tools
 8. PROTECT-PROTECTIVE TECHNOLOGY (PT)-2 Removable media is protected, and its use restricted according to policy

1

1.National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity version 1.0*. U.S. Department of Commerce. February 2014.

5.1.4 Related Risks

- Compromise of equipment functionality from malicious activity can put confidentiality, integrity and availability at risk
- Damage of physical IT assets due to natural causes, such as weather events, can prevent data and system availability
- Malicious access to systems
- Theft

5.1.5 Technology Controls

- Public Key Infrastructure (PKI) to issue and manage certificates
- Identity and Access Management (IAM) Tools
- Physical Access Swipe Keys
- Surveillance Systems
- Redundant Systems
- Remote Access Controls

5.1.6 Process Controls

- PKI Governance Certificate Policy and Certificate Practice Statements
- Access Control Governance and Processes
- User credential standards
- Removable media policies and controls
- Employee awareness

5.2 Endpoint Security

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

5.2.1 Business Analysis Practitioner (BA) Focal Points

- Business case and requirements analysis for endpoint security solutions
- Understanding of applicable standards, regulatory considerations, and endpoint security controls

5.2.2 Key Terms and Definitions

- **Endpoint:** The term used to describe any device through which users connect to information, systems, and networks, for example laptops, smart phones, printers, tablets.
- **Encryption:** The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext).¹
- **Full Disk Encryption:** Automatic and transparent encryption of all hard-drive data storage.
- **File Level Encryption:** Manual encryption of specific files where the user must initiate an action before the file is encrypted and stored.
- **Self-Encryption Device:** Hard drive that self-encrypts data to a media storage device and then automatically decrypts the data from the media.
- **Malware (Malicious Software):** Designed to infiltrate, damage or obtain information from a computer system without the owner's consent.²

5.2.3 Use Cases

- Endpoint device is taken off work premises
- Endpoint device is lost or stolen
- Endpoint device is hacked

1.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

2.Ibid.

5.2.4 Related Risks

- Exposure of mobile devices, desktops, laptops and tablets to loss or theft which leaves data on those devices vulnerable to access from unauthorized users.
- Potential of Malicious software (Malware) infecting a corporate device.
- Potential data breach by unscrupulous persons accessing the data on stolen devices.

5.2.5 Technology Controls

- IAM – Identity and Access Management Tools
- FDE – Full Disk Encryption
- FLE – File Level Encryption
- SED – Self-Encryption Device
- AMP – Anti-Malware Protection

5.2.6 Process Controls

- Device Handling and Management Policies
- IAM Governance

5.3 Network Security: Security Architecture

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

5.3.1 Business Analysis Practitioner (BA) Focal Points

- Understand how the security architecture ties back to the organization and existing operational processes, and the impact decisions will have on stakeholders.
- Understand what is within the scope of the security architecture; as it is not possible to cover all business aspects, it is important to focus and keep scope clear to avoid unnecessary complexity.
- Where architecture requirements are transferred between development efforts, understand the rationale behind the original component selection decision to ensure it fits with the current security architecture.¹
- Understand how selected security controls relate to the four factors which should drive architectural decisions:
 - Risk Management
 - Benchmarking and Good Practice
 - Financial
 - Legal and Regulatory

5.3.2 Key Terms and Definitions

- **Security Architecture:** The set of disciplines used to design solutions to address security requirements at a solution or system level.²
- **OSI Reference Model:** A prescriptive model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard for its underlying internal structure and technology. It is comprised of seven layers: 1) Physical, 2) Data-link, 3) Network, 4) Transport, 5) Session, 6) Presentation, 7) Application.
- **TCP/IP or DoD Model:** A descriptive model for modelling current internet architecture, as well as providing a set of rules that govern all forms of transmission over a network. It is comprised of four layers: 1) Link, 2) Network, 3) Transport, 4) Application.

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

2. Ibid.

- **Network Access Control (NAC):** The concept of controlling access to an environment through strict adherence to, and implementation of, security policy. The goals of NAC are to prevent/reduce zero-day attacks, enforce security policy throughout the network, and use identities to perform access control.¹
- **Network Topology:** The physical layout and organization of computers and networking devices. Logical topology is the grouping of networked systems into trusted collectives. Physical topology is not always the same as logical topology. The four basic physical topologies are: ring, bus, star and mesh.²
- **Defence in Depth:** The practice of layering defenses to provide added protection. Defense in depth increases security by raising the effort needed in an attack. This strategy places multiple barriers between an attacker and an enterprise's computing and information resources.³

5.3.3 Use Cases

- **Business Context:** Attackers will typically go after the weakest point in a network or system. This weak point is rarely a security feature or function. When a secure system or network is being designed, it is important to consider the weakest link in the system and ensure it is secure enough.⁴
- **Solution Scope:** The idea behind defence in depth is to manage risk with diverse defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense will hopefully prevent the breach.⁵
- **Threat Risk and Vulnerability Assessments:** Insecure systems tend to suffer from the same sorts of threats and vulnerabilities. Common vulnerabilities include poor memory management, the existence of covert channels, insufficient system redundancy, poor access control and poor protection of key components.⁶

5.3.4 Related Risks

- Like all system layers, networks are subject to risks that arise out of constant changes in the environment, in all aspects: people, process, and technology.
- Designing security for a service must consider all connected systems or sub-systems, regardless of the layer in which they reside, otherwise any that are outside of the defined architecture can introduce vulnerabilities into and architecture if data or connections from those external sources is not validated and secured.

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

2. Ibid.

3. ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

4. McGraw, Gary. *Thirteen principles to ensure enterprise system security*. TechTarget. January 2013. <https://searchsecurity.techtarget.com/opinion/Thirteen-principles-to-ensure-enterprise-system-security>.

5. Ibid.

6. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

- When privileged access is provisioned to users who require special access to restricted or sensitive information, there is a risk of abused privileges; the risk increases if the access is not audited and maintained on a regular basis.

5.3.5 Technology Controls

- Network Segregation
- Penetration Testing
- Defense in Depth

5.3.6 Process Controls

- Principle of Least Privilege
- Design and Architecture Reviews
- System and Security Audits

5.4 Network Security: Firewalls

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

5.4.1 Business Analysis Practitioner (BA) Focal Points

- Understand the network connectivity requirements for applications being deployed behind a firewall.
- Understand the logging and audit requirements for firewall deployments.
- Understand the policies which form the basis for firewall rule implementation. In the absence of documented policy, defining these is the first step to a successful deployment.

5.4.2 Key Terms and Definitions

- **Stateless Firewall:** A type of firewall filter that watches end-to-end traffic flow and tracks packet sources and destinations; uses network connection state information to make traffic control decisions dynamically. Stateful firewalls can tell if packets have been forged or have broken down, and are able to perform security functions such as encryption.
- **Stateful Firewall:** Watch traffic streams from end-to-end. They are aware of communication paths and can implement various IP Security (IPsec) functions such as tunnels and encryption. Stateful firewalls are better at identifying unauthorized and forged communications.¹
- **Next Generation Firewall:** A deep-packet inspection firewall that moves beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention and bringing intelligence from outside the firewall.²
- **Network Address Translation (NAT):** A methodology of modifying network address information in IP datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another.³

1. Gartner. *Gartner Information Technology Glossary: Next-generation Firewalls (ngfws)*. <https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws>.

2. Ibid.

3. ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

- **Host Based Firewall:** Software which is installed on individual computers, to protect the end host, or operating system, as opposed to at the network level.
- **Network Based Firewall:** A hardware appliance that is deployed on the network and filters traffic going between networks (e.g. Internet and LAN). Placed at the perimeter or border of the network.
- **Rule Set:** A set of access control rules defined in firewalls, which control which traffic is permitted through and which must be blocked.
- **Ingress Traffic:** Traffic moving towards the firewall, regardless of destination (e.g. internet or LAN).
- **Egress Traffic:** Traffic moving away from the firewall, regardless of destination (e.g. internet or LAN)

5.4.3 Use Cases

- The definition of Corporate Security Policy and/or Acceptable Use Policy are the first steps in defining the network security, application, and traffic policies that should be enforced. Without defined policies, a firewall configuration can end up being little more than an ad hoc listing of perceived needs.
- After end-to-end application security requirements and risk factors are identified, firewalls can be deployed as one component to help meet those security requirements.¹
- While a firewall should always be placed at internet gateways, there are also internal network considerations and conditions where a firewall could be deployed, such as network zoning.²
- Firewalls should be placed between entities that have different trust domains.³

1. Robinson, Chad. *Best Practices for Firewall Deployments*. CSO. October 2002. <https://www.csoonline.com/article/2113273/best-practices-for-firewall-deployments.html>.

2. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

3. Ibid.

5.4.4 Related Risks

- If improperly managed or deployed, a firewall can leave gaps in an organization's security that attackers can use to infiltrate your network. Gartner has projected that in the next three years, 99% of firewall breaches would be caused by misconfigurations.¹
- Firewalls provide only limited protection against vulnerabilities caused by application flaws in server software on other hosts. For example, a firewall will not prevent an attacker from manipulating a database to disclose confidential information.²

5.4.5 Technology Controls

- Firewall Analyzer
- Network Segmentation
- Anti-Virus
- Data Backup and Disaster Recovery

5.4.6 Process Controls

- Policy
- Formalized Change Control Process for Firewall Rule Management
- Principle of Least Privilege
- Defense in Depth

1.Firewall Security Company India. *20 Top Most Problems in Firewalls Which Impact Business*. WordPress. 2020. <http://firewall.firm.in/category/firewall/page/3/>.

2.ISC. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

5.5 Network Security: Anti-Virus/Anti-Malware

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

5.5.1 Business Analysis Practitioner (BA) Focal Points

- Be familiar with existing and emerging types of malware and their attack vectors.
- Understand the types of devices and endpoints on the network and what level of Anti-Virus/Anti-Malware (AV/AM) coverage is required.
- Understand the level of operational/management overhead is required to maintain the deployed AV/AM infrastructure.
- Understand how the various AV/AM components interact with each other and how data can be aggregated for reporting.

5.5.2 Key Terms and Definitions

- **Whitelist:** A list of email or Internet addresses that someone knows as “good”. Items on a whitelist are permitted.
- **Blacklist:** A list of email or internet addresses that someone knows as “bad”. Items on a blacklist are blocked.
- **Grey list:** A list of email or Internet addresses that are neither good nor bad on first glance but require additional levels of validation before communication is permitted.
- **Sandboxing:** A form of software virtualization that lets programs and processes run in their own isolated environments.¹
- **Honeypot:** A decoy computer system for trapping or tracking hackers or new hacking methods. They are designed to intentionally engage and deceive hackers and identify malicious activities.
- **Trojan:** A program that pretends to be legitimate code but conceals other unwanted functions.
- **Worm:** A program that is capable of copying itself onto other computers or devices without user interaction.
- **Zero Day:** A vulnerability that is unknown to those who would be interested in mitigating it. Until the vulnerability is mitigated or AV/AM software is updated to detect it, hackers can exploit it.

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

5.5.3 Use Cases

- For malware to spread, it needs to be installed on the target device or computer. Some of the most common infection techniques are phishing, websites/drive-by attacks and removable media such as memory sticks.
- Minimizing zero-day endpoint infections by pre-emptively blocking known, unknown, and targeted attacks at all endpoints, online and offline, on network and off.
- Coordination of AV/AM policy enforcement across network, endpoints, and cloud services.
- Protection of desktops, laptops, servers, and workstations from malware, ransomware, exploits and file-less attacks.

5.5.4 Related Risks

- USB memory sticks, CDs, DVDs and other removable media devices provide an effective way of spreading malware onto additional computers. When the media is inserted into the machine, the malware will either run and infect the target or will copy itself onto the removable media in order to prepare to infect the next machine it is plugged into.
- The widespread use of mobile code such as JavaScript on websites has provided attackers with another route to infect computers with malware. Increasingly, legitimate websites are being compromised and made to host malware without the owner's knowledge, making this type of attack very difficult for the user to avoid.

5.5.5 Technology Controls

- Defence in Depth
- Workstation and network-based AV/AM software
- Security Information and Event Management (SIEM) software
- Intrusion Detection and Prevention Software

5.5.6 Process Controls

- Hunt Teams
- Security Operations Center
- Information Security Policies (Acceptable Use, AV/AM, Software, Backup, etc.)
- Security Awareness Training
- Principle of Least Privilege

5.6 Network Security: Segregation

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

5.6.1 Business Analysis Practitioner (BA) Focal Points

- Understand the security requirements of various servers and applications on the network for them to be properly classified.
- Understand the sensitivity of data and criticality of applications to facilitate the segregation activities.
- Understand what data from a zone may need to be transmitted to another zone and if, based on data sensitivity, that communication flow should be permitted and under what conditions.
- Understand organizational business and security requirements to ensure that any segregation strategy doesn't impede the business.

5.6.2 Key Terms and Definitions

- **Network Segregation:** Assets are grouped together based on common security requirements, and then each group is placed into its own isolated network zone, so that traffic flowing into each zone will be subject to the security policies defined by the zone's security requirements, and filtered accordingly.
- **Network Segmentation:** The partitioning of a network into smaller networks.
- **Micro-Segmentation:** Through the use of software, placing security controls between individual servers in a virtual environment.
- **Security Perimeter:** The first line of protection between networks of different zones. In general, it can include firewalls as well as proxies and devices such as intrusion detection systems (IDS) to warn of suspicious traffic.¹
- **Flat Network:** A network in which all computers (hosts) are able to communicate directly with all others within it; the network is not segmented at all.
- **Whitelisting:** The practice of explicitly allowing identified people, groups, or services access to a particular privilege, service, or recognition.

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

5.6.3 Use Cases

- Users are no longer confined to an office. Conventional data protection models do not apply in a world where users can be anywhere, using any device, and connecting through wired, wireless or mobile infrastructure.
- The segregation of sensitive information, hosts and services from the environment in which users access external resources (e.g. web, email) can minimize the impact of any potential breach due to user behavior.
- A segregated network architecture is incomplete if an organization does not have full visibility into it. This visibility is achieved by collecting, inspecting and analyzing traffic at the various security zones between segregated networks.
- Security Operations Centers and threat hunting teams can be more effective in a well-structured network. Traffic that may be normal in the user segment could be malicious in the server segment. This would be very hard to detect in a flat network.

5.6.4 Related Risks

- Flat networks are easy to manage and save money; however, with minimal controls between servers and data of different classification and security levels, an attacker who gains access to one system is able to use it as a staging ground for other environments across the network.
- More than 50% of cyber-attacks are not detected by the organization for months. Without full visibility into the network, an organization does not know who is accessing it, what they are doing, where they are coming from, and how they are traversing from one part of the network to another.
- Hostile actors are increasingly targeting internal networks using techniques such as spear-phishing and social engineering. This, coupled with an increase in the use of mobile and remote working, provides additional attack vectors for access to a company's internal network.

5.6.5 Technology Controls

- Disabling of non-essential services on servers and workstations
- Firewalls and Security Appliances
- Separation of management and operational networks
- Network traffic whitelisting
- Physical network isolation

5.6.6 Process Controls

- Principle of Least Privilege
- Need to Know

5.7 System Security: Servers

5.7.1 Business Analysis Practitioner (BA) Focal Points

- Understand sensitivity and classification as it relates to server access controls.
- Understand how users with a requirement for administrative access, whether IT staff or business workers, should be assigned only those privileges necessary for them to accomplish their required tasks.¹
- Understand what is required for the server to meet technical requirements and what features are unnecessary and can be disabled.
- Understand physical and technological controls required to control and monitor access to the server room or data center.

5.7.2 Key Terms and Definitions

- **Security Baseline:** A set of basic security objectives which must be met by any given service or system. Details depend on the operational environment a service/system is deployed into, and might thus, creatively use and apply any relevant security measure. Derogations from the baseline are possible and expected and must be explicitly marked.²
- **Trusted Platform Module (TPM):** An international standard (ISO 11889) for a secure crypto-processor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.³
- **Trusted Computing Base (TCB):** Trusted Computing Base (TCB) is a group of trusted system assets consisting of software, hardware, and other controls, which together enforce security policies.
- **Security Perimeter:** The boundary that defines the area of security concern and security policy coverage.⁴
- **Emanations:** Unintentional electrical, mechanical, optical or acoustical energy signals that contain information or metadata about the information being processed, stored or transmitted in a system.⁵
- **Virtualization:** The hosting of one or more operating systems (servers) within the memory of a single host server.⁶
- **Security Boundary:** The line of intersection between any two areas, subnets or environments that have different security requirements or needs.⁷

1.ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

2.ITSRM. *Mandatory Security Baselines*. CERN Computer Society. June 2010. <https://security.web.cern.ch/security/rules/en/baselines.shtml>.

3.International Standards Organization. *ISO/IEC 11889-1:2015 Information Technology - Trusted platform module library - Part 1: Architecture*. ISO. August 2015.

4.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

5.ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

6.Ibid.

7.Ibid.

- **Defence in Depth:** Multiple layers or levels of access controls to provide layered security. In server defence the outer layer may often be physical access controls followed by logical and technical controls and finally administrative access controls.¹
- **Domain Name System (DNS):** A hierarchical database that is distributed across the internet that allows names to be resolved into IP addresses (and vice versa) to locate services such as web and e-mail servers.²
- **Dynamic Host Configuration Protocol (DHCP):** A protocol used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask and IP addresses of domain name system (DNS) servers from a DHCP server; ensures that all IP addresses are unique.³
- **Peer-to-Peer (P2P):** Style of networking in which computers communicate directly with one another rather than routing traffic through managed central servers and networks. Typically used for sharing resources amongst each other.⁴

5.7.3 Use Cases

- Improving Server Security can have a positive impact on Access Control security by the very nature of limiting the opportunities for potential access.
- Unpatched servers are another major source of security problems. There are often many patches that come thru for servers, and determining which server patches must be applied and how much validation testing must be completed is an important to decide. Critical patches would need to be applied and testing expedited to assure they are put to production at the earliest validated time.
- Having a security model that is representative of the system being designed is an effective way to illustrate the methods that will be used to actualize the security policy requirements.

5.7.4 Related Risks

- Servers may end up running services unintentionally and not be aware of it, which introduces potential risks that do not get identified. This can happen when administrators install an operating system, which turns on additional, unwanted services automatically with the base configuration.
- P2P applications, while possessing many legitimate applications, are associated with piracy and abuse of copyright and other forms of intellectual property.⁵

1.Ibid.

2.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

3.Ibid.

4.Gartner. *Gartner Information Technology Glossary: P2p*. <https://www.gartner.com/en/information-technology/glossary/p2p-peer-to-peer>.

5.ISC. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

- P2P applications are often designed to open an uncontrolled channel through network boundaries, thus providing a way dangerous content, such as botnets, spyware, and viruses to enter an otherwise protected network.
- Due to the overlapping nature of P2P node structure, it can be very difficult to fully detect and shut down the controlling botnet, allowing it to continue operating unimpeded.¹

5.7.5 Technology Controls

- SSH Keys
- Firewalls
- VPN and Private Networks
- Public Key Encryption and SSL/TLS Encryption
- Service and File Auditing
- Isolated Execution Environments

5.7.6 Process Controls

- Policies and Procedures related to employee behaviours
- Audits and Spot Checks
- Principle of Least Privilege
- Segregation of Duties
- Physical Access Controls
- Proactive Patching and Lifecycle Management

1.Ibid.

5.8 Platform Security

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

5.8.1 Business Analysis Practitioner (BA) Focal Points

- Understand the pros and cons of platform security, and its fit (or not) to business and security requirements.
- Understand the platform being deployed and the applicable security controls to be applied.
- Understand the use cases for the platform and if they may require additional security measures.
- Understand how platforms will have required security patches applied and at what frequency.

5.8.2 Key Terms and Definitions

- **Infrastructure as a Service (IaaS):** Offers the capability to provision processing, storage, networks and other fundamental computing resources, enabling the customer to deploy and run arbitrary software, which can include operating systems (OSs) and applications.¹
- **Platform as a Service (PaaS):** PaaS is built on top of the IaaS model as, in addition to providing the services from IaaS, a PaaS provider will also provide operating systems, middleware, and other runtime environments.
- **Software as a Service (SaaS):** Software that is owned, delivered and managed remotely by one or more providers. The provider delivers software based on one set of common code and data definitions that is consumed by all contracted customers at anytime on a pay-for-use basis or as a subscription based on use metrics.²
- **Platform Security:** A security model that is used to protect an entire platform by using a centralized security architecture or system. Unlike a layered security approach in which each layer/system manages its own security, platform security secures all components and layers within a platform. This enables the elimination of individual security measures and use of multiple applications/services to secure different layers of an IT environment.³

1.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

2.Gartner. *Gartner Information Technology Glossary: Software as a Service (SaaS)*. <https://www.gartner.com/en/information-technology/glossary/software-as-a-service-saas>.

3.Techopedia.com. *Definition - What does Platform Security mean?*. <https://www.techopedia.com/definition/4053/platform-security>.

5.8.3 Use Cases

- An organization upgrading or deploying an application may choose to purchase PaaS from a provider rather than acquire and manage hardware and underlying infrastructure.
- An organization has periodic spikes in application usage, requiring temporary increased computing power.
- An organization has chosen to outsource its data center to a cloud platform provider.
- The technology used to secure a platform in this context is very similar (or identical) to what it would take to secure a physical on-premise environment: Anti-Virus/Anti-Malware (AV/AM), firewalls, Intrusion Detection/Prevention System (IDS/IPS), etc.
- An underlying virtualization platform, such as VMware or Hyper-V, is used to isolate environments.
- An isolated environment, referred to as a Sandbox in this context, enables users to run programs or execute files without affecting the underlying system which they run on. In the case of PaaS, the sandbox is typically a virtualized environment (VMware, Hyper-V, Citrix).

5.8.4 Related Risks

- Platform as a Service creates some unique security requirements, as it is about the delivery of the platform layers with a generally complete development tool set, such as Microsoft Azure or other similar services. With the whole platform layer comes security built in which is convenient, but if the platform is compromised the entire infrastructure is vulnerable.
- With the usual implementation being virtual, the whole process of access control and authentication needs to be consistent across the platform layers. Like a captive data center, the vulnerabilities are largely the same. The entire platform must be reviewed and examined for risk consistent with the needs of the business.
- It is common to also create links to other corporate networks who will use the platform. The access standards should be established so that access controls and authorizations are consistent for sign ons and data exchanges. The weakest link could expose the entire platform to vulnerabilities. This may impact the network and interface design requirements and security considerations.

1

1.Shinder, Thomas. *Security Considerations for Platform as a Service (PaaS)*. Microsoft TechNet. April 2016. <https://social.technet.microsoft.com/wiki/contents/articles/3809.security-considerations-for-platform-as-a-service-paas.aspx>.

5.8.5 Technology Controls

- Anti-Virus/Anti-Malware
- Identity and Access Management
- Network Segregation
- Privileged Account Management
- Firewalls
- Virtual Private Networks (VPN)
- Intrusion Detection and Prevention Systems (IDS/IPS)

5.8.6 Process Controls

- Internal and External Audit
- Architecture Standards and Policies
- System Hardening Policy
- Patch Management Process and Policy

5.9 Product Security: Threat Models

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Basic Process Steps
5. Related Risks
6. Technology Controls
7. Process Controls

5.9.1 Business Analysis Practitioner (BA) Focal Points

- Understand the business cases and usage scenarios that will feed into the threat modelling activity.
- Understand how risks will be ranked for likelihood and impact
- Understand how risks will be addressed after prioritization.
- Understand how the security objectives of the organization align to the defined threat prioritization.

5.9.2 Key Terms and Definitions

- **Threat Modelling:** Threat modeling is a procedure for optimizing network/application/internet security by identifying objectives and vulnerabilities and then defining countermeasures to prevent, or mitigate the effects of, threats to the system.¹
- **Information Asset:** A body of knowledge that is organized and managed as a single entity. Like any other corporate asset, an organization's information assets have financial value.²
- **Threat Event:** Any event during which a threat element/actor acts against an asset in a manner that has the potential to directly result in harm.³
- **Attack Surface:** Components available to be used by an attacker against the product itself.⁴
- **Exploit:** The use of an identified vulnerability to violate security objectives such as confidentiality, integrity and availability.⁵

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

2. OWASP. *Threat Modeling Cheat Sheet*. https://owasp.org/www-project-cheat-sheets/cheatsheets/Threat_Modeling_Cheat_Sheet.html.

3. ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

4. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

5. National Institute of Standards and Technology (NIST). *NIST SP 800 154: Guide to Data-Centric System Threat Modeling*. U.S. Department of Commerce. September 2016.

5.9.3 Use Cases

- When performed early in a development cycle, threat modelling can assist with identifying potential issues and reduce the effort and complexity of resolving them.
- Cyber-physical systems integrate software technology into physical infrastructure such as smart cars or smart grids. Cyber-physical systems are often vulnerable to threats that manufacturers of traditional physical infrastructure may not consider.¹
- Simply following general “best practices” for security is insufficient for safeguarding high-value data. Best practices are largely based on conventional wisdom intended to mitigate common threats and vulnerabilities. By their very nature, such best practices are generalized, especially for ubiquitous products (web browsers, server and desktop operating systems, etc.) They do not take into account the unique characteristics of each system.²

5.9.4 Basic Process Steps

- Determine assessment scope: tangible assets, application capabilities, reputation and goodwill attributes.
- Identify threat agents and possible attacks: characterize groups of potential attackers – inside and outside, malicious and inadvertent.
- Understand existing countermeasures already deployed within the organization.
- Identify exploitable vulnerabilities: focus on those that connect the identified possible attacks to the identified negative consequences.
- Prioritize identified risks: for each threat, estimate a number of likelihood and impact factors to determine overall risk/severity level.
- Identify countermeasures to reduce threat: to reduce risk to acceptable levels based on the enterprise risk appetite.

3

1. Shevchenko, Nataliya. *Threat Modeling: 12 Available Methods*. Carnegie Mellon University: Software Engineering Institute. September 2018. https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html.

2. National Institute of Standards and Technology (NIST). *NIST SP 800 154: Guide to Data-Centric System Threat Modeling*. U.S. Department of Commerce. September 2016.

3. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

5.9.5 Related Risks

- Cybersecurity teams encounter new threats constantly, and adapting to the latest threats could protect the company from a large data breach and associated impacts.
- No system is 100 percent secure; every system has vulnerabilities. At any given time, a system may not have any known software flaws, but security configuration issues and software feature misuse vulnerabilities are always present.¹
- Older systems may be vulnerable to different threats than newer systems and due to their age, they may often be overlooked when developing threat models.

5.9.6 Technology Controls

- Security Operating Center (SOC)/Security Information and Event Management (SIEM)
- Intrusion Detection and Prevention Systems
- Next Generation Firewalls
- Audit logging

5.9.7 Process Controls

- Vulnerability and Threat Risk Assessment Procedures
- Secure Development
- Policies and Controls
- Internal and External Audits

1.Ibid.

5.10 Product Security: Embedded Systems

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

5.10.1 Business Analysis Practitioner (BA) Focal Points

- Understand how the technical and functional requirements meet the required security for critical embedded systems.
- Understand how and where embedded systems will be deployed as part of a project.
- Understand what mitigating controls can be deployed to account for embedded systems that are not secure on their own.

5.10.2 Key Terms and Definitions

- **Embedded System:** Embedded systems are used to provide computing services in a small form factor with limited processing power. They embed the necessary hardware, firmware, and software into a single platform that can be used to provide a limited range of computing services, usually around a single application.¹
- **Data Isolation:** Data within partitioned applications which cannot be read or modified by other applications.²
- **Damage Limitation:** If an attack damages a partitioned application, this damage cannot spread to other partitions/applications.³
- **Pyramid of Trust:** Each layer can rely on the effective security of its underlying layer without being able to verify it directly.⁴
- **Hardware Security Module (HSM):** A physical device that safeguards the cryptographic infrastructure by securely managing, processing and storing cryptographic keys inside a tamper-resistant external device that attaches directly to a computer.

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015

2. EDN. *Embedded Systems Security - Part 1: Security requirements*. February 2013. <https://www.edn.com/embedded-systems-security-part-1-security-requirements/>.

3. Ibid.

4. Wolf, Marko and André Weimerskirch. *Hardware Security Modules for Protecting Embedded Systems*. ESCRYPT Inc. <https://pdfs.semanticscholar.org/54c2/485b78e0e084225c0d3a04bc7a7a5deef727.pdf>.

- **Wrapper:** Encapsulation solutions that manage, configure, and update embedded systems through a controlled channel; their security may be enhanced through addition of authentication and integrity features.

5.10.3 Use Cases

- Embedded systems are often not only enabled with internet access but also with means to remotely modify and patch software. By compromising the embedded system, the hostile actor could install malware or even replace the operating system itself.
- In-vehicle computing systems can include embedded systems to monitor engine performance, optimize braking, steering and suspension, but can also include in-dash elements related to driving, environmental controls, and entertainment.¹
- An embedded system provides very little, if any, allowance for security, especially for size, weight and power considerations; thus, security must not impose excessive overhead on the protected system.²

5.10.4 Related Risks

- It is often not financially and/or technically feasible to retrofit security capability into a system that was not originally designed for it. This can leave older embedded systems vulnerable to attack.
- Parts from multiple manufacturers may comprise a finished product which leads to the problem that no single manufacturer has any incentive, expertise or even ability to patch the software on the embedded system once it is shipped.
- Many embedded systems are designed with a focus on minimizing cost and extraneous features. This often leads to a lack of security and difficulty with upgrades and patches. Because an embedded system is in control of a mechanism in the physical world, a security breach could cause harm to people and property.³

5.10.5 Technology Controls

- Anti-Virus and Anti-Malware software
- Firewall
- Intrusion Detection and Prevention Software
- Virtual Private Network (VPN)
- Key authentication
- Hardware Security Modules (HSM)
- Network Segregation

5.10.6 Process Controls

- Software Development Lifecycle
- Security by Design

1.Ibid.

2.Gipper, Jerry. *Securing embedded systems based on Open System Architectures*. Vita Technologies. <http://vita.mil-embedded.com/articles/securing-based-open-system-architectures/>.

3.ISC. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

5.11 Product Security: Internet of Things

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

5.11.1 Business Analysis Practitioner (BA) Focal Points

- Understand the data being transmitted through Internet of Things (IoT) devices, and connectivity requirements.
- Understand the security objectives for the IoT product(s) and the relevant threats to those objectives.
- Understand how information about IoT devices, such as serial numbers, will be protected.
- Understand how firmware will be managed and updated on deployed IoT devices.

5.11.2 Key Terms and Definitions

- **Internet of Things (IoT):** The Internet of Things (IoT) refers to systems that involve computation, sensing, communication, and actuation. The IoT involves the connection between humans, non-human physical objects, and cyber objects, enabling monitoring, automation, and decision making.¹
- **Firmware Over-the-Air:** Technology used by manufacturers of mobile devices after distribution, to remotely install software and services, or resolve issues wirelessly.
- **Near-Field Communications (NFC):** A wireless technology that enables a variety of contactless and proximity-based applications, such as payments, information retrieval, mobile marketing and device pairing.²
- **Smart Meter:** A digital data collection and communication device used in the energy sector. Energy consumption data is tracked and made available to the provider and customer.
- **Application Programming Interface (API):** A set of routines, protocols and tools referred to as "building blocks" used in business application software development; also thought of as an interface between a server and a client.³

1.Voas, Jeffery (NIST). *NIST 800-183: Networks of 'Things'*. National Institute of Standards and Technology (NIST). July 2016.

2.Gartner. Gartner. *Information Technology Glossary: Near Field Communication (nfc)*. <https://www.gartner.com/en/information-technology/glossary/near-field-communication-nfc>.

3.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

5.11.3 Use Cases

- IoT devices contain and collect a lot of sensitive information about their physical surroundings. Garage door openers and access control systems collect data on when you arrive and leave; smart speakers listen to private conversations in the background; vacuum cleaners develop a detailed floorplan of the area they clean. All of this data, coupled with low levels of security integrated into them, make them a target for attack.
- IoT devices being connected to the internet but not adequately secured has resulted in incidents such as hackers accessing in-home monitoring devices, and botnets shutting down entire parts of the internet.

5.11.4 Related Risks

- Where many IoT devices use embedded systems made with components from multiple manufacturers, the risk applies where no single manufacturer has any incentive, expertise or even ability to patch the software on the embedded system once it has shipped.
- A compromised IoT device on a network can give an attacker a foothold within the network to attack other portions of the network and collect sensitive data.
- Traditionally, Bring Your Own Device (BYOD) applied to smartphones, but as employees work away from the office and have other connected devices like digital assistants or fitness devices connected to the same network, there are new concerns around data security; if one of those devices is compromised, hackers can move laterally to compromise a connected corporate asset such as a laptop.¹

5.11.5 Technology Controls

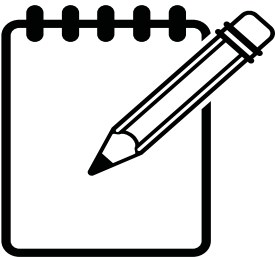
- Anti-Virus and Anti-Malware software
- Firewall
- Intrusion Detection and Prevention Software
- Virtual Private Network (VPN)
- Key Authentication
- Network Segregation

5.11.6 Process Controls

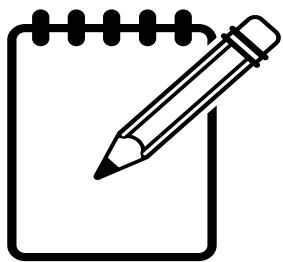
- Software Development Lifecycle
- Security by Design
- Security Awareness Training

1. Salgy, Susan. *7 ways to secure the IoT in your enterprise*. Techbeacon. <https://techbeacon.com/security/7-ways-secure-iot-your-enterprise>.

NOTES



A series of horizontal dashed lines for taking notes.



NOTES

Area with horizontal dashed lines for taking notes.



Module 6: Data Security

1. Data Security At Rest: Information Classification & Categorization
2. Data Security In Transit: Encryption and Keys
3. Data Security In Transit: SSL/TLS
4. Data Security In Transit: Digital Signature and Identification

6.1

Data Security At Rest: Information Classification & Categorization

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

6.1.1

Business Analysis Practitioner (BA) Focal Points

- Understand the typical levels of an information classification and categorization schema and how information falls into the various levels.
- Understand the data privacy requirement of the organization to allow for the definition of an appropriately sized classification and categorization schema.
- Understand how information classification and information categorization are interconnected.
- Understand how a correctly applied classification and categorization scheme can protect information assets while not unnecessarily inhibiting access to information assets.

6.1.2 Key Terms and Definitions

- **Information Classification:** The process by which organizations assess the data they hold and the level of protection it should be given based on its risk to loss or harm from disclosure.
- **Security Category:** The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, or the nation.¹
- **Information Categorization:** Information is categorized according to its information type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, executive order, directive, policy, or regulation.²
- **NIST SP 800-53:** A series of Security and Privacy control standards for US Federal Information Systems and Organizations that is often used as a foundational piece by private organizations developing their own information classification and categorization systems.
- **NIST SP 800-60:** A guide for mapping the types of information and information systems within an organization to security categories.

6.1.3 Use Cases

- To properly control access to information and mitigate the risk of sensitive information being disclosed, all information within an organization should be categorized and have an appropriate classification level applied. This information is a foundational building block for information security and mitigation of risk due to unauthorized data disclosure.
- Categorizing Information:
 - An organization must first identify all applicable information types that are representative of input, stored, processed, and/or output data from each system. Then for each information type, use criteria to assign levels of impact to confidentiality, integrity and availability, and assign a system security category based on the aggregate of information types.³

1. Federal Information Processing Standards. *Standards for Security Categorization of Federal Information and Information Systems*. U.S. Department of Commerce. February 2004.

2. National Institute of Standards and Technology (NIST). *NIST SP 800 60: Guide for Mapping Types of Information and Information Systems to Security Categories*. U.S. Department of Commerce. August 2008.

3. Ibid.

- Classifying Information:
 - Once information and systems have been categorized, classification is used to determine appropriate security initiatives to protect the categorized information, i.e. how documents, data, and systems containing the categorized information must be handled, stored, transmitted, accessed, published, destroyed, etc.¹
- Identifying and applying project specific security controls within a Software Development Lifecycle (SDLC).
- Defining and updating a baseline set of security controls, based on industry standards, for an organization.

6.1.4 Related Risks

- Organizations create documentation and data as part of regular operations. Some documentation/data is benign with little risk to the organization if disclosed beyond authorized users, whereas other documents may have customer data, trade secrets or other information with varying levels of impact if disclosed.
- Classifying data too high can be unnecessarily costly and restrictive, resulting in lower productivity and efficiency.
- Classifying data too low increases the risk of unauthorized disclosure of sensitive company information.

6.1.5 Technology Controls

- Data Loss Prevention (DLP) on Endpoints and Network Devices such as Firewalls.
- Tools have been developed to help organizations establish and manage information and system sensitivity requirements and controls.
- Algorithms can be written and implemented to automatically assign classifications to information when user profiles and information content and context are provided.

6.1.6 Process Controls

- NIST SP 800-53 – Recommended Security Controls for Federal Information Systems (USA)
- NIST SP 800-60 – Guide for Mapping Types of Information and Information Systems to Security Categories (USA)
- ITSG-33 IT Security Management: A Lifecycle Approach (Canada)
- ISO/IEC 27001 Information Security Management

1.Ibid.

6.2 Data Security In Transit: Encryption and Keys

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

6.2.1 Business Analysis Practitioner (BA) Focal Points

- Understand the difference between symmetric and asymmetric encryption and how keys are exchanged, stored, generated, and revoked.
- Understand the sensitivity of the data being transmitted and received to determine the correct type of encryption and key strength to ensure data security.
- Understand how keys are used to generate and verify digital signatures.
- Understand how public and private key pairs form the underpinning of various Internet security standards including TLS (Transport Layer Security) and S/MIME (Secure/Multipurpose Internet Mail Extensions).

6.2.2 Key Terms and Definitions

- **Encryption Key:** A piece of information, in a digitized form, used by an encryption algorithm to convert the plaintext to the ciphertext. ¹
- **Symmetric Key Algorithm:** An encryption method that relies on a "shared secret" key that is distributed to all members who participate in communications. The key is used by all parties to both encrypt and decrypt messages. It is primarily used to perform bulk encryption and provides only for the security service of confidentiality. ²
- **Asymmetric Key Algorithm:** An encryption method where each user has two keys: a public key which is shared with all users and a private key which is kept secret and known only to the user. Keys must be used in tandem to encrypt and decrypt. i.e. if a public key encrypts a message, the private key must be used to decrypt, and vice versa. ³

1.ISACA. Cybersecurity Fundamentals Glossary. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

2.ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

3.Ibid.

- **Key Pair:** Comprised of a public and a private key. The keys are generated at the same time and are associated with one another. The public key can be freely shared with any party and, due to a mathematical relationship, can be used to encrypt messages that only the private key can decrypt. This is a one-way ability, meaning that the public key has no ability to decrypt anything it writes. The private key should be kept entirely secret and should never be shared with another party. The private key is the only component capable of decrypting messages using the associated public key.
- **Hash Function:** Takes what are potentially long messages and generates a unique output value derived from the content of the message. The output is commonly referred to as the message digest and is used to validate that a message originated from a particular user and to ensure that the message was not modified in transit between the two parties.¹
- **Public Key Infrastructure (PKI):** An infrastructure that enables users of a basically nonsecure public network (such as the Internet) to exchange data and money securely and privately through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.²

6.2.3 Use Cases

- A piece of information that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of plain text into ciphertext or vice versa during decryption.³
- The most common application of public and private keys is in the encrypting of communications to provide confidentiality.
- Non-repudiation systems use digital signatures to ensure that one party cannot dispute their authorship of a document or communication.

6.2.4 Related Risks

- Various cryptographic attacks:
 - Analytic
 - Implementation
 - Statistical
 - Brute Force
 - Man in the Middle
 - Replay

1.Ibid.

2.Norton. *Norton Glossary: PKI public key infrastructure*. <https://us.norton.com/online-threats/glossary/p/pki-public-key-infrastructure.html>.

3.Norton. *Norton Glossary: key*. <https://us.norton.com/online-threats/glossary/k/key.html>.

- A compromise of the underlying digital certificate infrastructure and associated root certificates would call into question the security and validity of all digitally signed artifacts (documents, code, communications, etc.).
- Disclosure of private key (intentional or unintentional).

6.2.5 Technology Controls

- Certificate Authorities (CAs)
- Encryption of Data at Rest
- Hardware Security Modules (HSMs)
- Offline/Cold Storage of Private Key or Root Certificate

6.2.6 Process Controls

- Principle of Least Privilege
- Cryptographic Policy Management

6.3 Data Security In Transit: SSL/TLS

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

6.3.1 Business Analysis Practitioner (BA) Focal Points

- Understand the types of data that will be transmitted between systems and if that data is classified as sensitive enough to require encryption.
- Understand any applicable legal requirements for in-transit data security.
- Understand how certificates are used for encryption of data in transit.

6.3.2 Key Terms and Definitions

- **Secure Socket Layers (SSL):** A cryptographic protocol designed to provide authentication and data encryption between servers, machines, and applications over a network. It was replaced by the TLS protocol; however, the term is still used frequently in discussions of TLS.
- **Transport Layer Security (TLS):** A cryptographic protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.¹
- **Data In Transit:** Data that is sent over a network (cellular, Wi-Fi, or other network) or is located in active memory.
- **Cleartext:** Data which is in a form that is immediately understandable to a human without additional processing. May also be referred to as unencrypted data.
- **Secure/Multipurpose Internet Mail Extensions (S/MIME):** Provides cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption) to provide a consistent way to send and receive MIME data.²

1.ISACA. Cybersecurity Fundamentals Glossary. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

2.Ibid.

6.3.3 Use Cases

- Web browsers use HTTPS to encrypt e-commerce transactions. Almost all HTTPS transmissions use TLS as the underlying encryption protocol.
- Sensitive data, such as a user's login credentials, credit card details, email information, health information, must never be revealed over the network, and are therefore encrypted.
- Email, by its nature, is not secure. Email should not be used as a method of transmission of confidential data unless additional email encryption, such as S/MIME is used.

6.3.4 Related Risks

- Malicious users may intercept or monitor clear text data being transmitted across an unencrypted connection and gain unauthorized access to it, jeopardizing the confidentiality of sensitive data. Types of sensitive data may include (but are not limited to):
 - Passwords
 - Data stream from corporate applications (ERP)
 - Documents being stored on corporate servers
 - Email contents
 - Financial or health data
- Data being sent unencrypted can be intercepted during transmission and changed, making it difficult or impossible to validate its accuracy.

6.3.5 Technology Controls

- SSL/TLS encryption capability is provided by certificates which can be purchased from:
 - Certificate Authorities
 - A domain name registrar
 - Website hosting provider
- Certificates may be purchased in various formats:
 - Certificates as a Service (CaaS)
 - Via a Self-Service application
 - As a fixed quantity but flexible pool which can be reassigned to entities over time

6.3.6 Process Controls

- Risk Assessment and Mitigation Process and Strategy

6.4 Data Security In Transit: Digital Signature and Identification

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

6.4.1 Business Analysis Practitioner (BA) Focal Points

- Understand what data being transmitted will be used for and if non-repudiation will be required.
- Understand the process for how data will be signed before transmission and identified and validated upon receipt.
- Understand how the management and use of certificates for signing and identification will be performed.

6.4.2 Key Terms and Definitions

- **Certificates.** There are 5 types of certificates:
 - **Client SSL Certificate:** Used to identify clients to servers via SSL. Client SSL certificates can also be used for form signing and as part of a single sign-on solution.
 - **Server SSL Certificate:** Used to identify servers to clients via SSL. Server authentication can be used with or without client identification. Server authentication is a requirement for an encrypted SSL session.
 - **S/MIME Certificate:** Used for signed and encrypted email. A single certificate may be used as both an S/MIME certificate and an SSL certificate. S/MIME certificates can also be used for form signing and as part of a single sign-on solution.
 - **Object-Signing Certificate:** Used to identify signers of program code, scripts and other signed files.
 - **Certificate Authority (CA) Certificate:** Used to identify CAs. Client and server software use the CA certificates to determine what other certificates can be trusted. Also sometimes referred to as Root Certificates.

1

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

- **Public Key Infrastructure (PKI):** A set of roles, policies and procedures used to create, use and manage digital certificates for public key encryption.
- **Certificate Chain:** A series of certificates issued by successive CAs. A certificate chain traces a path of certificates from a branch in the hierarchy to the root of the hierarchy. ¹
- **Digital Signature:** A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and non-repudiation. A digital signature is generated using the sender's private key or applying a one-way hash function. ²
- **Non-Repudiation:** The assurance that a party cannot later deny originating data; provision of proof of the integrity and origin of the data and that can be verified by a third party. ³

6.4.3 Use Cases

- **Enable Single Sign-On:** A user could log in once, using a single password to the local client's private-key database, and get authenticated access to all SSL-enabled servers that the user is authorized to use without sending any passwords over the network. ⁴
- **Email Authenticity:** Messages that include a digital signature provide some assurance that it was sent by the person whose name appears in the header, thus providing authentication of the sender. ⁵
- **Laws and regulations frequently set standards for the electronic archiving of important records, such as corporate records or financial documents. Digital signatures and trusted time-stamps are used to assure the authenticity, authorship, and integrity of records so that they may not be altered or manipulated retrospectively. Signing may occur by individuals or central automation.** ⁶
- **Software purchased in a traditional retailer comes in a shrink-wrapped package which clearly shows the publisher and if the package has been tampered with. Individuals who download software from the Internet need similar assurances. Code Signing provides an assurance that the publisher of the software is who they say they are, and that the software has not been altered prior to or during distribution.**

1.Ibid.

2.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

3.Ibid.

4.ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

5.Ibid.

6.Digicert and QuoVadis. *Digital Certificate Use Cases*. QuoVadis. https://www.quovadisglobal.co.uk/DigitalCertificates/UserCertificates/Digitalcertificate_Uses.aspx.

6.4.4 Related Risks

- A compromise of the underlying digital certificate infrastructure and associated root certificates would call into question the security and validity of all digitally signed artifacts (documents, code, communications, etc.).
- Data that is not digitally signed cannot be 100% validated as authentic and would have difficulty being supported in any legal challenge of its authenticity.
- Data that has not been digitally signed is easier to impersonate when electronic transactions take place remotely.

6.4.5 Technology Controls

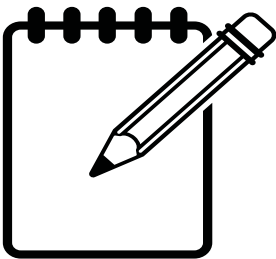
- Public Key Infrastructure (PKI)
- Digital Certificates
- Virtual Private Network (VPN)
- Single Sign-On

6.4.6 Process Controls

- Threat Risk Assessments
- Vulnerability Assessments
- Process for certificate issue, validation and revocation

This image shows a full page of a handwriting practice worksheet. It consists of multiple sets of three horizontal dashed lines, providing a guide for letter height and placement. The lines are evenly spaced across the entire page, which is otherwise blank.

NOTES



A series of horizontal dashed lines for taking notes.



Module 7: User Access Control

1. Directory Management
2. Authorization
3. Authentication and Access Control
4. Privileged Account Management
5. Users and Security Awareness

7.1 Directory Management

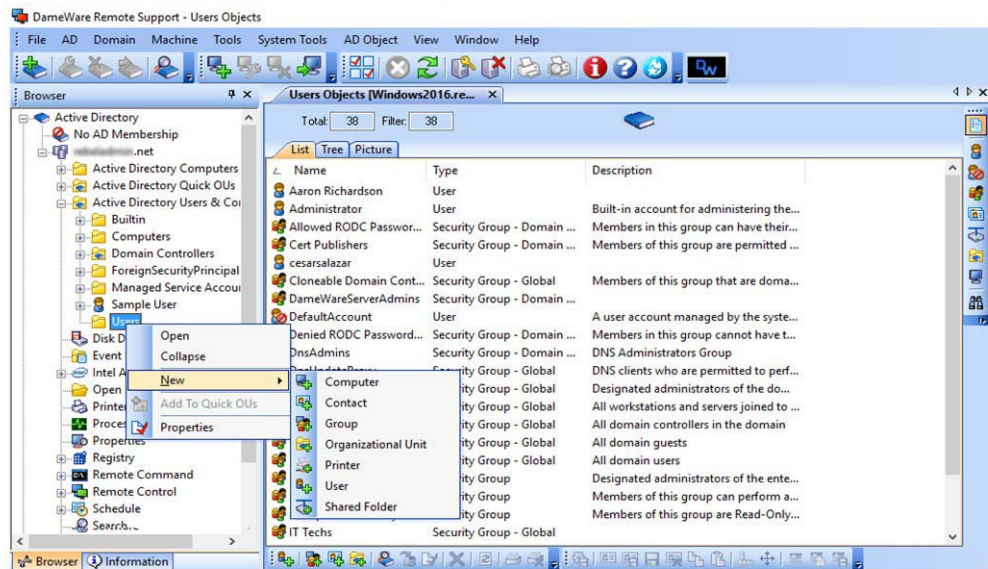
1. Overview
2. Business Analysis Practitioner (BA) Focal Points
3. Key Terms and Definitions
4. Use Cases
5. Related Risks
6. Technology Controls
7. Process Controls

7.1.1 Overview

- A directory is a comprehensive database designed to centralize the management of data about an assortment of company entities, and will typically contain a hierarchy of objects storing information about users, groups, systems, servers, printers, etc.¹
- Directory Management is the practice of creating, operating, and maintaining the entire directory file system, and is an enabler of user access control.
- In a hierarchical file system, a directory contained inside another directory is called a subdirectory. The terms parent and child are often used to describe the relationship between a subdirectory and the directory in which it is cataloged, the latter being the parent.

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

- The image on the following page is a good example of how a directory management system would appear. (Example uses a common directory management tool, Active Directory.)



7.1.2 Business Analysis Practitioner (BA) Focal Points

- Understand the principles associated with the two-step authorization process to directory management security systems.
- Understand the importance and value of applying the principle of least privilege access to resources within system directories.
- Understand the purpose of Access Control Entries (ACEs) and Access Control Lists (ACLs) as they apply to setting permissions and access controls on directory resources.
- Understand how security descriptors determine who can traverse folders to access resources within subfolders.
- Understand how different systems apply security to directory management.

7.1.3 Key Terms and Definitions

- **Access Control List (ACL):** An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals.¹
- **Authentication:** The act of verifying the identity of a user, the user's eligibility to access computerized information.²
- **Authorization:** Authorization is defined as a process ensuring that correctly authenticated users can access only those resources for which the owner has given them approval.³
- **Access Control Entry (ACE):** A single record in an access control list, which consists of the rights of a trustee's access. A security identifier is used to uniquely identify the access that is allowed or denied the trustee.
- **Directory Management System:** is the collection of software, hardware, and processes that store information about an enterprise, subscribers, or both, and make that information available to users⁴
- **Discretionary Access Control Lists (DACL):** Discretionary Access Control is a means of restricting access to objects based on the identity of subjects and/or groups to which they belong; a subject with a certain access permission is capable of passing that permission on to any other subject. A DAC List is a collection of the discretionary access controls defined for a particular object.⁵

7.1.4 Use Cases

- Files and directories must be secured to ensure that only authorized users have access to them.
- Directory Management Systems typically follow a two-step process of authentication, followed by authorization; access is granted first by validating the user identity, then allowing the user to access the resources defined by their pre-defined permissions.
- Authorization to access a file or directory is strictly controlled by the ACL in the security descriptor associated with each file or directory.
- When a file is created, unless a specific permission is applied, a default security descriptor is applied, or inherited from the parent directory. Resources that are copied to another directory maintain their original ACEs, by default.

1.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

2.ibid.

3.Gartner. *Gartner Information Technology Glossary: Authorization*. <https://www.gartner.com/en/information-technology/glossary?glossarykeyword=Authorization>.

4.Red Hat. *Red Hat Directory Server Chapter 1: Introduction to Directory Services*. https://access.redhat.com/documentation/en-US/Red_Hat_Directory_Server/8.1/html/Deployment_Guide/Deployment_Guide-Introduction_to_Directory_Services.html.

5.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

- Establishing the principle of least privilege enables administrators with the means to restrict access to files and folders by specific users and by security group membership.

7.1.5 Related Risks

- Unauthorized access to files can compromise confidential information.
- Misconfigured permissions can expose files and folders to unauthorized access and manipulation, allowing hackers to create, view, modify, copy and delete business information.
- Often, default permissions are set to be least restrictive, so that all the child objects (files and folders) stored within the container are exposed to unauthorized access.

7.1.6 Technology Controls

- Access Control Entries (ACEs) associated with each file and folder enable an administrator to enforce the principle of least privilege access.
- Access Control Lists (ACLs) establish specific, enforceable access controls to users who are members of specified security groups.

7.1.7 Process Controls

- Establishing policies to limit and control access enables system administrators to set user and group member access permissions to files and folders.
- Understanding how access controls and permissions are inherited by child objects is important for establishing standards and practices for managing directories.

7.2 Authorization

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Software Licensing
5. Related Risks
6. Technology Controls
7. Process Controls

7.2.1 Business Analysis Practitioner (BA) Focal Points

- Access Control Policy and Procedures
- Establishment of Group and Role Membership conditions
- Specify attributes for types of accounts
- Technology Solution Requirements would include enforcement of approved authorizations, and approved information flow controls

7.2.2 Key Terms and Definitions

- **Authorization:** Authorization is defined as a process ensuring that correctly authenticated users can access only those resources for which the owner has given them approval. ¹
- **Principle of Least Privilege:** Giving a user account only those privileges which are essential to perform its intended functions. ²
- **Separation of Duties:** Internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets. In a cybersecurity context, it is used so that no single person is in a position to introduce fraudulent or malicious code without detection. ³
- **Identity and Access Management (IAM):** A set of processes and policies for organizations to manage risks and maintain compliance with regulations and policies by administering, securing and monitoring identities and their access to applications, information, and systems.

1. Gartner. *Gartner Information Technology Glossary: Authorization*. <https://www.gartner.com/en/information-technology/glossary?glossarykeyword=Authorization>.

2. National Institute of Standards and Technology (NIST). *NIST Handbook 16: NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements*. U.S. Department of Commerce. November 2017.

3. ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

- **Role Based Access:** Restricts access based on an employee's role within an organization. Typically used in very large organizations with many users to simplify the security administration process with hundreds of users and thousands of permissions.¹

7.2.3 Use Cases

- Most user access to company assets requires authorization.
- Role Based Access granted for groups of employees based on job classification and function.
- Privileged Access granted for individuals requiring elevated administrative access.
- Access to only the assets for which the user is authorized.
- Manager and/or application owner review entitlements, and correct where required.
- Assignment and tracking of approval delegations.
- Authorizations for controlling the flow of information.
- Replacement of authorizers when incumbents leave or change roles.
- Removal of employee accounts upon departure or role change.

2

7.2.4 Software Licensing

- A software license grants permission to a defined set of users; one license is required for each user and it this license acts as the access control mechanism to that software for each user and legally governs the redistribution of the software. Use of the software without an issued license is considered copyright infringement.
- Licensing can be defined a number of ways such as named, concurrent users, by processors, by transaction, etc. Some controls appear as notifications which may lead one to believe it is a security control as opposed to a licensing issue.
- Licensing can control the privileges and permissions available to users and super-users. This can include access to specific modules and the access controls within them such as Create, Read, Update, Delete (CRUD).

1.Ibid.

2.Microsoft Azure. *Common use-cases and scenarios for Azure Active Directory Domain Services*. October 2019. <https://docs.microsoft.com/en-us/azure/active-directory-domain-services/scenarios>.

7.2.5 Related Risks

- Inappropriate access to classified information
- Fraudulent activity
- Loss of Data
- Unavailability of systems or information in the event of a compromise
- Misuse of shared/group accounts
- Misclassification of assets that do not require authorization.

7.2.6 Technology Controls

- Identity and Access Management Applications
- Directory Management
- Privileged Account Management Tools
- "Approval before Access" Controls
- Logging and Retention of Approved Data
- Certification
- Identity Management (system)
- Information Flow Enforcement
- Software Licensing

7.2.7 Process Controls

- Onboarding and Role Changes
- Approval Processes and Workflows
- Designation of Approvers and Delegates
- Audit of entitlements
- Identity Management (Manual)

7.3 Authentication and Access Control

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Access Control Matrix
4. Use Cases
5. Related Risks
6. Technology Controls
7. Process Controls

7.3.1 Business Analysis Practitioner (BA) Focal Points

- Understand how access controls are intended to protect the organization's proprietary information from accidental or intentional, internal or external threats; could take the form of information disclosure, modification, deletion, or misuse.
- Understand how access control gives an organization the capability to restrict, monitor, and audit access to information resources so that confidentiality, integrity, and availability can be preserved.
- Understand the stakeholder groups and their respective access needs; understand user types, both regular and privileged.
- Understand how governance (policies and processes) support access control technologies.
- Understand roles and responsibilities around the approval, provisioning, and de-provisioning of access.

7.3.2 Key Terms and Definitions

- **Authorization:** All users must have their access approved by the appropriate, designated level of authority. In most cases, this is their manager. For other specific applications, this might be the owner of the business application. Access to applications that contain sensitive data may also need approval by IT Security, and/or a higher-level of management.
- **Authentication:** The act of verifying the identity of a user, the user's eligibility to access computerized information; designed to protect against fraudulent logon activity; may be achieved via credentials, or it could be through other means¹
- **Multifactor Authentication:** Combination of more than one authentication method required for access, such as token and password (or personal identification number [PIN]) or token and biometric device.²

1.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

2.Ibid.

- **Virtual Private Network (VPN):** A secure private network that uses the public telecommunications infrastructure to transmit data.¹
- **Single Sign On (SSO):** Systems are integrated to enable the user to sign in only once and have access to all required applications. Although convenient for users and password management, it is not the most secure feature.
- **Principle of Least Privilege:** A user has access to ONLY the assets and data they require to perform their role – nothing more.
- **Segregation of Duties (SoD):** An internal control concept of having more than one person required to complete a task, intended to prevent fraud and error. For example, a user cannot approve their own expenses.
- **Privileged Account Management (PAM):** Establishing and maintaining access rights and controls for users who require elevated privileges to an entity for a particular administrative or support function. The four most common use cases for privileged access are; Root or Built-in Administrator; Service Account; Administrator Account; and, Power User.²

7.3.3 Access Control Matrix

- An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals.³
- The subject (1st column in the example below) would be a role or user and the object (top row across) would be the system entity or asset requiring protection.
- The entry in a cell – that is, the entry for a subject-object pair – indicates the access mode that the subject is permitted to exercise on the object. Each column is equivalent to an access control list for the object and each row is equivalent to an access profile for the subject.⁴
- Example:

	Asset 1	Asset 2	File	Device
Role 1:	read, write, execute, own	execute	read	write
Role 2:	read	read, write, execute, own		

1.Ibid.

2.ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

3.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

4.Bishop, Matt. *Computer Security: art and science*. Addison-Wesley. 2004. http://research.omicsgroup.org/index.php/Access_Control_Matrix.

7.3.4 Use Cases

- Defining system Access Requirements
- Vendors require access to an application via VPN or other secured gateway to provide support
- Privileged/Elevated Users require “write” access for troubleshooting, code changes, upgrades, data changes, custom reporting or data extraction
- Tracking, Reporting and Auditing on Access
 - Who has access to what
 - What is being done with the access
 - Does access align with principle of least privilege
- Create and maintain Authorization Matrix or Access Control Matrix to ensure the correct but minimal access is being provisioned to users in each role
- Business processes to de-provision access when no longer required

7.3.5 Related Risks

- When a user has access to more than they require to perform their work, exposure to threats opens to their full scope of access rather than just the required access.
- When a privileged user has unnecessary access to assets other than those required, this administrative access may be exploited if the privileged access is compromised.
- Those with authorization to approve access do not understand the user's access requirements or adopt an approach of "grant the same access as User X". This kind of 'role based' access makes administration simpler but may create security vulnerabilities if not done with caution.
- When user access is not managed reliably and users maintain unnecessary access, the organization is exposed to many potential threats:
 - Unauthorized changes to information or applications
 - Spread spam and malware
 - Illegal activities
 - Exploit the organization's resources to initiate outside attacks
 - Install malicious programs to destroy or modify files
 - Insert undetectable capabilities into applications
 - Create a backdoor that enables attackers' easy future access

7.3.6 Technology Controls

- Identity and Access Management (IAM) Tools
- Privileged Account Management (PAM) Tools
- VPN Access
- Password Vault

7.3.7 Process Controls

- Access Control Governance, Policies, and Procedures
- Authorization/Access Control Matrix Management
- User Provisioning and De-Provisioning Policies and Processes
- Regularly Scheduled Access Audits
- Change Approval Boards and Processes

7.4 Privileged Account Management

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

7.4.1 Business Analysis Practitioner (BA) Focal Points

- Understand the directory management system, its construction, and naming convention, the protocols for building and navigating its parts, and how directory management plays a role privileged account management.
- Understand the stakeholder groups and their respective access needs; understand user types, both regular and privileged, and the justification for the privileged access.
- Understand how excessive access privileges can create vulnerabilities.
- Understand how governance (policies and processes) support access control technologies.
- Understand roles and responsibilities around the approval, provisioning, and de-provisioning of access.

7.4.2 Key Terms and Definitions

- **Privileged user:** A user who requires elevated access to an entity to perform an administrative or support function.
- **Privileged Account Management (PAM):** Establishing and maintaining access rights and controls for users who require elevated privileges to an entity for a particular administrative or support function. The four most common use cases for privileged access are; Root or Built-in Administrator; Service Account; Administrator Account; and, Power User. ¹
- **Multi-Factor Authentication:** A combination of more than one authentication method, such as token and password (or personal identification number [PIN] or token and biometric device). ²
- **Principle of Least Privilege:** Practice of limiting user access to only the assets and data they require to perform their role – nothing more.

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

2. ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

- **Segregation of Duties:** Internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets. In a cybersecurity context, it is used so that no single person is in a position to introduce fraudulent or malicious code without detection.¹
- **Single Sign On (SSO):** An access control mechanism where a user logs in once and gains access to a number of applications and services without being prompted to log in again at each of them.²
- **Virtual Private Network (VPN):** A secure private network that uses the public telecommunications infrastructure to transmit data.³ For more information about VPN see: <https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html>.

7.4.3 Use Cases

- Vendors require access to an application via VPN to provide support.
- Privileged/Elevated Users require “write” access for user management, environment management, troubleshooting, code changes, upgrades, data changes, custom reporting or data extraction.
- Tracking and Reporting on Access
 - Who has access to what
 - Activity/audit logs: what is being done with the access
- Create and maintain an Authorization Matrix to ensure the right access is being approved
- De-provision access when no longer required, or when requirements change
- Change management may be required for users who lose excessive access

7.4.4 Related Risks

- When a user has access to more than they require to perform their work, exposure to threats opens up to the scope of access rather than just the required access. Common examples include:
 - A normal user is given full administrative access to their network account to enable use of a special application; it is easier and faster for an administrator to grant this, rather than for the single use case
 - A manager has broad access to employee files, other than just those within his/her portfolio

1.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

2.International Organization for Standardization (ISO). *IISO/IEC TR 26927:2011: Information technology — Telecommunications and information exchange between systems*. ISO.org. September 2011.

3.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

- A user leaves the organization or changes roles, but continues to have access to files and applications no longer required
- When a privileged user has unnecessary access to assets other than those required, this administrative access may be exploited if the privileged access is hijacked. Common examples include:
 - An application support administrator has access to more than the application(s) that he/she is responsible for
 - A vendor is given access to the network to support their application, without a gateway management tool to restrict their remote access
 - A database administrator has access to the actual data stored within the database they support

7.4.5 Technology Controls

- Identity and Access Management (IAM) Tools
- Privileged Account Management (PAM) Tools
- VPN Access
- Password Vault

7.4.6 Process Controls

- Policies and Procedures
- Authorization Matrix Management
- Change Approval Boards and Processes

7.5 Users and Security Awareness

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Users' Role in Cybersecurity
4. Risks Imposed by Related Threats
5. Technology Controls
6. Process Controls

7.5.1 Business Analysis Practitioner (BA) Focal Points

- Understand the role employees play in protecting organizational assets and information from cybercrime.
- Understand the types of threats that employees should be aware of, and the controls employees should employ to protect themselves from becoming a victim.
- Understand the policies and processes in place at an organization that are intended to increase employee awareness.
- Be able to locate, share, and create awareness material to all users across the organization.
- Be able to define and track metrics relative to awareness, such as compliance to training requirements, employee knowledge testing, behaviour analysis, etc.
- Be able to identify when additional training is required: topic, audience, etc.

7.5.2 Key Terms and Definitions

- **Risk:** The combination of the probability of an event and its consequence. ¹
- **Threat:** Anything that is capable of acting against an asset in a manner that can result in harm; a potential cause of an unwanted incident. ²
- **Phishing:** Spear phishers use highly personalized information in emails to try to gain your trust.
- **Malware:** Files or software that are designed to intentionally compromise a computer or device. Examples include Ransomware, Spyware, Bots.
- **HTTPS:** An encrypted (secure) URL versus HTTP which is not encrypted.
- **Social Engineering:** Attackers exploit human emotions and connection to gain access. Examples include creating a sense of urgency, impersonation, or claiming a prize has been won.
- **Tailgating:** Attackers watch employees keying in access codes.

1. International Organization for Standardization (ISO). *ISO GUIDE 73:2009 Risk management – Vocabulary*. ISO.org. September 2011..

2. International Organization for Standardization (ISO). *ISO/IEC 13335-1:2004: Information technology – Security techniques*. ISO.org. November 2004.

7.5.3 Users' Role in Cybersecurity

- Two thirds of security breaches can be traced back to employee behaviour, not technology.
- Most security breach causes that are attributed to employee behaviour are known, and therefore preventable.
- Technology controls can only do so much; employees are the first and last lines of defence against attacks.

7.5.4 Risks Imposed by Related Threats

- Spear phishers use highly personalized information in emails to try to gain an employee's trust, for example posing as an executive to trick employees into performing wire transfers.
- Malware can be used to gain information, monitor activity, restrict access, take control of a computer, overload a website, or destroy information.
- Passwords are easily hacked if a user does not change them regularly, use different passwords for all logins, or if they are too short or too simple.
- Public Wi-Fi can introduce risk when using networks that are not password protected or fake networks; without a VPN connection, commercial transactions become vulnerable.
- Mobile Devices: Malware can be distributed on mobile devices as easily as on a desktop; mobile devices introduce unique vulnerabilities.
- Attackers can easily create a fake website that is not encrypted and impersonate the real site, thereby gaining information provided by the user.
- Tailgaters or shoulder surfers can follow an employee into a controlled area or steal access keys and passwords.

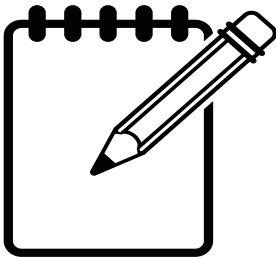
7.5.5 Technology Controls

- Enforced Password Criteria Compliance
- Automated Warnings, Spam Filters
- Anti-Virus and Anti-Malware Software
- Password Vault/Manager

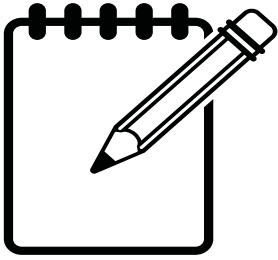
7.5.6 Process Controls

- Policies and Procedures related to employee behaviours
- Anti-reflective monitor screens
- Locking screens when leaving workstation
- Not writing down passwords
- Education and Campaigns
- Audits and Spot Checks

NOTES



A series of horizontal dashed lines for taking notes.



NOTES

[illegible]



Module 8: Solution Delivery

1. SDLC and Solution Security Planning
2. Requirements and Security Engineering
3. Requirements and Solution Development
4. Solution Security: Applications
5. Solution Security: Databases
6. Solution Security: Web
7. Change Impact Analysis

8.1

SDLC and Solution Security Planning

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Approaches
5. Technology Expertise
6. Process Expertise

8.1.1

Business Analysis Practitioner (BA) Focal Points

- Understand the role of the Business Analysis Practitioner (BA) in managing Software Development Life Cycle (SDLC) security requirements.
- Understand how information risk planning contributes to overall security best practices.
- Understand the current state of software development security practices within the organization and assess the maturity of those practices.
- Understand that risk analysis should occur at the beginning and throughout the SDLC.
- Support the development and implementation of standard assessments throughout the SDLC. This may be high level at the start and very specific as the solution is defined.

- Monitor and document residual risk to be reviewed and managed prior to deployment.
- Consider reporting requirements and their security implications, such as timing, aggregation.

8.1.2 Key Terms and Definitions

- **Software Development Life Cycle (SDLC):** A framework used to design, develop and test high quality programs. It is a process followed by development teams, which consists of a detailed plan describing how to develop, maintain and replace specific software.¹
- **Role-based access:** Definition of user roles that will have specific levels of access to perform actions within the solution. This is often related to Active Directory groups which can be assigned system roles.
- **Permissions:** Rights to perform specific actions within a system such as the typical CRUD activities.
- **Create, Read, Update, Delete (CRUD):** Actions performed to manipulate data within a system.
- **Log Auditing:** The ability to historically track activities performed within a system, to trace what changes were made and by whom, logged within the system.
- **Application Programming Interface (API):** Mechanism of calling functions, usually real-time, to access or update data.

8.1.3 Use Cases

- Threat risk assessments are a critical component of solution planning; a TRA should be done early in the cycle, and revisited at each stage to ensure risks are being designed out.
- Elicitation of security requirements will consider the life cycle of data and how we restrict manipulation of data (CRUD).
- Access controls should be included in the elicited requirements.
- Data may need to be entered by users, via User Interfaces or from another system using integration, such as batch file integration or real-time APIs, for example.
- Define the requirements to audit and track data movement.
- Ensure consistent application of data classifications and their governance:
 - Data classifications, such as confidentiality levels (public, restricted) are typically defined at the enterprise level
 - The BA will align project-level data elements to this classification
 - The BA will ensure the level of governance prescribed for the data type is defined

1.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

8.1.4 Approaches

- Security requirements will include access controls, data protection and performance expectations, such as enforcement or notifications and vulnerabilities within the enterprise or organization.
 - Waterfall
 - Security requirements are documented within non-functional requirements.
 - Agile
 - Security requirements can be expressed within the acceptance or success criteria to ensure developers and quality assurance tasks are aware of the security requirement.

8.1.5 Technology Expertise

- Although the technical team members are typically responsible for selecting effective security controls and designing the technology aspect of solution options, Business Analysts should have working knowledge of these concepts, and interact early and frequently with the designers and developers to ensure that security is built into solutions rather than bolted on right before implementation:
 - The seven layers of the OSI model, with focus on Endpoint, Application Network security
 - Common threats and vulnerabilities specific to the environment and business applications
 - Firewall technologies
 - Intrusion detection and prevention technologies
 - Antivirus and Anti-Malware technologies
 - Cryptography and Keys
 - Identity and Access Management and Privileges Account Management technologies
 - Certificates and Transport Layer Security
 - Service-based solutions such as SaaS, PaaS, IaaS

8.1.6 Process Expertise

- Through process analysis, potential vulnerabilities can be identified. For example, if a system has a requirement to be able to export a report to an Excel file, and also has a requirement to restrict access to the report, will emailing the exported report be managed or will it be a potential breach of the requirement?
- Consultation with security advisors can help to identify process risks within a solution. Users commonly employ work-arounds that might have opportunities to compromise security. Expertise to know about these work-arounds and potential solutions to restrict or monitor these breaches should be considered.

8.2 Requirements and Security Engineering

1. Overview
2. Business Analysis Practitioner (BA) Focal Points
3. Key Terms and Definitions
4. Use Cases
5. Approach
6. Technology Expertise
7. Process Expertise

8.2.1 Overview

- This module discusses one of the core Business Analysis practices – Requirements Gathering and Analysis – but in a very specific context. Some technical teams refer to this domain as Security Engineering.
- The degree of BA involvement in these activities will vary, but the key role of the BA who does participate is around Requirements Gathering and Analysis. Documenting and maintaining these requirements is key to ensuring the architecture and designs align with the organization's core goals and strategic direction.
- The next module discusses Requirements in the more typical context – Solution Development – and the BA's cybersecurity activities in that broader area.

8.2.2 Business Analysis Practitioner (BA) Focal Points

- The business analysis tools, techniques, tasks, practices, and competencies discussed in *A Guide to the Business Analysis Body of Knowledge® (BABOK® Guide)* regarding Requirements Gathering and Analysis are relevant and applicable in cybersecurity; they are all needed and used in the same way.
- The difference with Security Engineering is the Requirements are representative of a more enterprise-wide view of what the business deems appropriate for securing its information assets and systems.¹
- The stakeholders would still be engaged; they will just be representative of more executive level roles, and the outcomes of the analysis will still be verified, validated, tracked, and used for design. The product will just be infrastructural in size and scope.

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

8.2.3 Key Terms and Definitions

- **Security Requirement:** A specific prerequisite that need to be satisfied in order to achieve the security attributes of an IT system; defined at all three levels of perspective: Enterprise, Infrastructure, and Application.
- **Security Architecture:** Security architecture refers to the set of disciplines used to design solutions to address security requirements at a solution or system level.
- **Security Engineering:** fills in the details of the security architecture in a manner compatible with its fundamentals. Contains concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, applications, and those controls used to enforce confidentiality, integrity, and availability.

1

8.2.4 Use Cases

- Assess and mitigate the vulnerabilities of security architectures and designs.
- Apply secure principles to site and facility design.
- Provide framework and foundation to enable secure communication and protect information.
- Identify the basic services needed to provide security for current and future systems.
- Model behaviour rules and technologies required to protect assets.
- Document evolving models to connect business drivers to technical controls.
- Build using standardized methodologies

2

8.2.5 Approach

- Establish key design principles and guidelines
 - Fundamental statements of belief, mandatory elements (or optional guidelines) that will restrict the overall design and establish key priorities for protection
 - Provide the high level (business) requirements for secure design
- Establish detailed requirements: functional and non-functional
 - Functional requirements address what the design must do or accomplish: security services to include, assets to protect, common threats to address, vulnerabilities identified, and controls
 - Non-functional requirements focus on the qualities of the services, including reliability and performance

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

2. Ibid.

- When approved, these requirements are used to guide the next phase: the creation of security designs.

1

8.2.6 Technology Expertise

- There are some key information security architecture concepts that are important for a cybersecurity BA to be familiar with, if participating in security engineering or enterprise architecture activities; these were discussed in more detail in previous modules:
 - Directory Management
 - Networking
 - Platforms, Systems, Applications, and Databases
 - Servers and Communication
 - Data Classification
 - Internet, Web and Cloud
 - Authentication and Authorization
 - Encryption

8.2.7 Process Expertise

- Similarly, there are some key business practices and processes that the cybersecurity BA will use if involved in Security Engineering, which were also discussed in more detail in other modules:
 - System Development Lifecycle
 - Risk Analysis and Management
 - Auditing
- It is important to note that the BA will continue to employ all the requirements-related practices and tasks that are contained throughout the *BABOK® Guide*; they are just being applied to a very specific subject matter, and at a broader, higher, enterprise level:
 - Business Analysis Planning and Monitoring
 - Elicitation and Collaboration
 - Requirements Lifecycle Management ²

1.Ibid.

2.International Institute of Business Analysis. *A Guide to the Business Analysis Body of Knowledge® version 3*. International Institute of Business Analysis. 2015.

8.3 Requirements and Solution Development

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases: Requirement Hierarchy
4. Use of Business Analysis Core Concept Model in Cybersecurity
5. Related Risks

8.3.1 Business Analysis Practitioner (BA) Focal Points

- Within solution development, the BA must focus on security requirements including:
 - Log Requirements (see Log definitions next slide)
 - Access controls
 - Data protection and integrity
 - Identify and meet external regulatory and compliance requirements
 - Identify and meet internal governance requirements
 - Identify impacts to integrated systems within the value chain
 - Maintenance documentation including service support models
 - Communication of cyber requirements to impacted stakeholders
 - Identify process gaps and remediate through configuration, if possible, or redesign the process
 - Identify training and resourcing requirements related to new security requirements
 - Support the creation of test plans and acceptance criteria to perform security testing
 - Consult whether a Threat and Risk Assessment should be performed, typically for substantially changed or new solutions

8.3.2 Key Terms and Definitions

- **Security Requirements:** Individual security functions which must be provided by a product. As per the *BABOK® Guide*, these are typically part of non-functional requirements.¹
- **Security Assurance Requirements:** Steps taken during development and evaluation of the product to assure compliance with the claimed security functionality.²

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

2. Ibid.

- **Success Criteria:** In agile terminology, security requirements can be defined within success criteria to ensure they meet quality standards.
- **Logging Requirements:** a common subset of security requirements, although you may have worked with them outside of this domain.
 - **Logs:** Records about system access, incidents, user activities, etc.
 - **Event logs:** Record information about access and actions of users, errors, events, etc. in information systems.
 - **Administrator and operator logs:** Privileges of administrators and operators of systems are different from the normal user privileges, which means they can perform more actions on systems.

1

8.3.3 Use Cases: Requirement Hierarchy

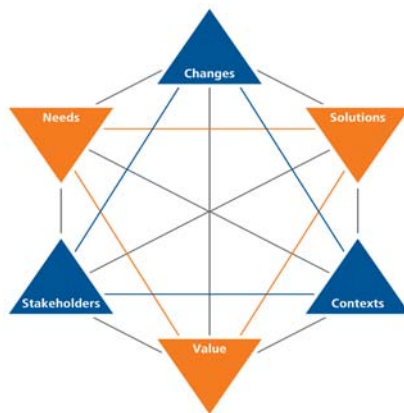
- Requirements gathering, analysis, and management throughout the software development lifecycle:
 - Business Requirements
 - Stakeholder Requirements
 - Solution Requirements
 - Functional Solution Requirements
 - Non-Functional Solution Requirements
 - i. Regulatory/Compliance Security Requirements
 - ii. Vendor Security Requirements (included in RFP)
 - User Experience
- Transition Requirements

2

1. International Organization for Standardization (ISO). *ISO/IEC 27001: Security Management*. ISO.org. 2013.

2. International Institute of Business Analysis. *A Guide to the Business Analysis Body of Knowledge® version 3*. International Institute of Business Analysis. 2015.

8.3.4 Use of Business Analysis Core Concept Model in Cybersecurity



Change	Business Change to Support Security Objectives
Context	Enterprise Risk Profile, Business Strategy
Stakeholders	Business Leaders, Customers, Partners
Value	Reputational Risk, Operational Value, \$\$\$
Needs	Business Need, Operational Need, Protect Assets
Solution	Design participation, Requirements, Fit for Purpose

8.3.5 Related Risks

- At early design phases, not enough of the solution is known to reliably identify security risks in time to design them out
- Cybersecurity immaturity among the solution development team
- Lack of an enterprise security architecture
- Cost of cybersecurity inhibits robust design
- Package and SaaS solutions may have insufficient cybersecurity controls
- Outsourced solutions may need to be more closely managed for security compliance

8.4 Solution Security: Applications

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

8.4.1 Business Analysis Practitioner (BA) Focal Points

- Understand application security needs and how they vary based on if the deployment is on-premise or cloud-based (IaaS, PaaS, SaaS).
- Understand the role of patch and application lifecycle management and how it is an essential part of enterprise software deployments.
- As applications increasingly move to the web, a new level of exposure and vulnerability has been created, requiring a more detailed understanding of the interconnectivity of systems and networks, and resulting documentation of requirements.
- Understand how various standards (e.g. NIST, ISO) and regulations (e.g. HIPPA, PCI) influence application security.
- Understand how security testing can be mapped back to controls and requirements.

8.4.2 Key Terms and Definitions

- **Cloud Computing:** Processing and storage are performed from a remote location over a network rather than locally. The main types of cloud computing are:
 - **Platform-as-a-Service (PaaS):** Computing platform and software solution as a virtual or cloud-based service which typically include operating system, database, webserver, etc. (e.g. Google App Engine)¹
 - **Software-as-a-Service (SaaS):** Software that is owned, delivered and managed remotely by one or more providers. The provider delivers software based on one set of common code and data definitions that is consumed by all contracted customers at anytime on a pay-for-use basis or as a subscription based on use metrics.²

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

2. Gartner. *Gartner Information Technology Glossary: Software as a Service (SaaS)*. <https://www.gartner.com/en/information-technology/glossary/software-as-a-service-saas>.

- **Infrastructure-as-a-Service (IaaS):** Complete outsourcing of computing infrastructure in either a physical or virtual format which typically includes storage, firewalls, load balancers, virtual networks, etc. (e.g. Amazon EC2)
- **Application Security Control (ASC):** A control to prevent a security weakness in an application. Some organizations may refer to these as application security requirements. Some may have regulatory contexts (e.g. PCI compliance).
- **Organization Normative Framework (ONF):** A company-wide repository of Application Security Controls and processes.
- **Application Level of Trust:** The confidence level required by an organization for a specific application.
- **Patch:** Fixes to software programming errors and vulnerabilities.¹
- **Logging:** The recording of operating system activity and specific events into various application logs.
- **Monitoring:** Software that reviews the logged events, and automatically detects problems.

8.4.3 Use Cases

- Combined logging and monitoring allow an organization to track, record and review application activities.
- Many applications can be configured to work with an Identity Provider for authentication, removing passwords as an area of weakness in a given application.
- In order to maintain a secure application environment, a process for the identification, assessment and implementation schedule of application software patches is critical. In addition, effective lifecycle management of deployed applications can ensure that applications and underlying systems are kept current.
- Configuration management and associated documentation helps ensure that systems are deployed in a secure consistent state and maintain this state throughout their lifetime.
- Malicious code, such as viruses, worms, trojans, spyware, and even spam use applications to permeate through, and represent potential security threats to the enterprise.

2

1.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

2.ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

8.4.4 Related Risks

- A botnet is a collection of compromised PCs organized into a network. Botnets are often used to launch attacks on other systems, or to send spam or phishing emails.
- Passwords are poor security. Compounding the risk is the fact that a single password is often re-used across multiple applications. A hostile actor acquiring a password from one compromised application has potentially gained access to others.
- Shadow IT: With the proliferation of cloud service providers, departments are no longer required to go through IT to deploy complex systems. Without proper oversight, this can often lead to stale or over-privileged accounts which can provide access to sometimes sensitive application data by hostile actors.
- Downloading and using apps on personal or improperly secured corporate mobile devices opens a large security hole related to stored credentials. Surveys have shown that 2/3 of people don't protect access to their phones with even a simple PIN, allowing anyone who picks up that device to potentially access restricted corporate applications.

1

8.4.5 Technology Controls

- Anti-Virus and Anti-Malware (AV/AM) tools
- Firewalls
- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) Platforms
- Application Whitelisting
- Logging and monitoring solutions such as Security Information and Event Management (SIEM) solutions

8.4.6 Process Controls

- Security Audits
- Design Review
- Application Patch and Lifecycle Management
- Secure coding/Secure by design

1.Ibid.

8.5 Solution Security: Databases

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

8.5.1 Business Analysis Practitioner (BA) Focal Points

- Understand the level of access to data required from the perspective of users, applications, and connected systems.
- Understand the confidentiality level(s) of the data being stored.
- Understand the potential threats to database security.
- Understand the interrelations between data sets in data warehouse implementations to be able to define process and procedures to minimize the risk posed by data aggregation or inference.
- Understand the full scope of database security and its related components beyond just the database itself.

8.5.2 Key Terms and Definitions

- **Data Warehouse:** A repository for information collected from a variety of data sources. Data stored in a data warehouse is not used for operational tasks but rather for analytical purposes.¹
- **Principle of Least Privilege:** A user has access to ONLY the assets and data they require to perform their role – nothing more.
- **Object Database:** Object Databases use objects to represent information rather than tabulated data, which is used in relational databases. They are often used for applications that involve very complex data.
- **Relational Database:** A database in which information is organized into rows and columns, forming one or more tables of data. Each row of data must have one unique key for identification.
- **Non-Relational Database:** A popular alternative to relational databases, non-relational databases are designed to store and manipulate large amounts of unstructured and semi-structured data. Often referred to as NoSQL databases.

1. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

- **Inference:** The ability to deduce sensitive or restricted information through observation of available information.¹
- **Database Management System (DBMS):** A product used for the storage and organization of data that typically has defined formats and structures. DBMSs are categorized by their basic structures and, to some extent, by their use or deployment.²
- **Data States:** There are three states in which data can exist:
 - **At Rest:** Data is stored in the database and not currently being accessed.
 - **In Transit:** Data is being transmitted over the network.
 - **In Use:** Data is in temporary storage buffers while in use by an application.

8.5.3 Use Cases

- **Data Classification:** When classifying the confidentiality level of a data warehouse, it must reside at the confidentiality level of the most sensitive data stored within it.
- **Database Access:** Many people within an organization manage, handle and use data, and they have different access requirements based on their roles.
- **Database Security Monitoring:** Some of the most common cybersecurity attacks can be detected by unusual access attempts and interactions on the database servers themselves.
- **Database Security Requirements:** Securing of information stored in databases includes planning for the protection of that data at rest, in transit, and in use.
- When multilevel security is required in databases it is essential that the security requirements of each dataset is known. Mixing data with different classification levels and/or need-to-know requirements can be a significant security challenge.

3

8.5.4 Related Risks

- Data stored in databases must remain secure even when in transit or in use. This requires securing both the network the data is being transmitted on and the application that is making use of the data.
- The underlying infrastructure and applications that databases rely on (DBMS, web server, operating system, etc.) present additional attack vectors for hostile actors. If the underlying systems are compromised, there exists the possibility that access to database(s) has also been obtained.

1.Ibid.

2.Gartner. *Gartner Information Technology Glossary: Dbms (database Management System)*. <https://www.gartner.com/en/information-technology/glossary/dbms-database-management-system>.

3.Ibid.

- In addition to the risk of compromise in live databases, the security of database backups must also be considered. The methods of backup and associated protection of backups are critical parts of comprehensive database security.

8.5.5 Technology Controls

- Database Management System (DBMS)
- Firewalls
- Data Encryption
- Application and DBMS patching
- Security Information and Event Monitoring (SIEM) tool

8.5.6 Process Controls

- Principle of Least Privilege
- Isolation of Sensitive Databases
- Separation of Duties
- Need to Know
- Comprehensive auditing policy and procedures

8.6 Solution Security: Web

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

8.6.1 Business Analysis Practitioner (BA) Focal Points

- Understand the data inputs that could be provided to web-based systems and what validation controls are required to secure against attack.
- Understand the methods and standards available for controlling access to web services.
- Understand the priority of web applications to allow for the most effective use of company resources.
- Understand the risk profile of the web environment and priority of web vulnerabilities to determine which are worth eliminating and which aren't too worrisome. Eliminating all vulnerabilities from all web applications is neither possible nor worth the time.¹
- Understand the security requirements including where web servers are deployed and data protection requirements.

8.6.2 Key Terms and Definitions

- **Web Server:** Using the client-server model and the World Wide Web's HyperText Transfer Protocol (HTTP), Web Server is a software program that serves web pages to users.²
- **Denial of Service Attack (DoS):** Any type of attack where the attackers attempt to prevent legitimate users from accessing the service. This type of attack is typically accomplished by flooding the targeted system with superfluous requests in an attempt to overload the system so legitimate requests cannot be fulfilled.³
- **Application Programming Interface (API):** A set of routines, protocols and tools referred to as "building blocks" used in business application software development; also thought of as an interface between a server and a client.⁴

1. Arsenault, Cody. *11 Web Application Security Best Practices*. Keycdn. March 2019. <https://www.keycdn.com/blog/web-application-security-best-practices>.

2. ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

3. ICS. *Official (ISC)² Guide to the CISSP CBK, Fourth Edition*. Auerbach Publications. March 2015.

4. ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

- **Cross-Site Scripting (XSS):** A type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites; occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.¹
- **SQL Injection:** Results from failure of the application to appropriately validate input. When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design.²
- **Web Service Description Language (WSDL):** A language formatted with extensible markup language (XML). Used to describe the capabilities of a web service as collections of communication endpoints capable of exchanging messages.³
- **Web Application Firewall (WAF):** A firewall specifically to protect communications with HTTP applications that run on web servers.
- **Cloud Access Security Broker (CASB):** On-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement.⁴

8.6.3 Use Cases

- Common Web applications include webmail, online retail shopping, online banking, etc.; some web apps are used in intranets, in companies and schools, for example.
 - Defining blueprint requirements: In order to stay on top of web application security best practices, a comprehensive blueprint is required. For larger organizations, the blueprint should name the individuals within the organization who will be involved in maintaining the web application security best practices going forward.⁵
 - Web application security requirements: web service security centers on the concepts of identification and authentication, authorization, integrity, non-repudiation, confidentiality, and privacy. All of these must be taken into account when designing or securing a web application.
- Organizations use APIs to connect services and transfer data. Broken, exposed or hacked APIs can be the source of major security breaches that could expose sensitive data such as medical, financial, and personal information that should not be exposed publicly.

1.Ibid.

2.Ibid.

3.Ibid.

4.Gartner. *Gartner Information Technology Glossary: Cloud Access Security Brokers (CASBs)*. <https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs>.

5.Arsenault, Cody. *11 Web Application Security Best Practices*. Keycdn. March 2019. <https://www.keycdn.com/blog/web-application-security-best-practices>.

8.6.4 Related Risks

- Because web-based systems are tied to production or internal systems (or both), they may provide a vector for intrusion into the private networks themselves. If a web server can be compromised, it offers a semi-trusted platform to mount probes or other malicious activities.¹
- Cookies allow for users to be remembered by sites they visit to speed up and personalize future visits. However, cookies can be manipulated by hackers to gain access to protected areas.²
- Misconfigurations of the application server as well as the database and database platform underlying the application can be exploited, especially when implemented with the known default settings. The exploits can be extremely varied due to the many configurations that could be misconfigured.³

8.6.5 Technology Controls

- Network Segregation/DMZ
- Web Application Firewalls (WAF)
- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) Platforms
- Logging and monitoring solutions such as Security Information and Event Management (SIEM) solutions
- Public Key Encryption and SSL/TLS Encryption
- Isolated Execution Environments

8.6.6 Process Controls

- Design Review
- Secure coding/Secure by design
- Security Audits
- Principle of Least Privilege
- Proactive Patching and Lifecycle Management
- Web Application Security Awareness Training

1.Ibid.

2.Gartner. *Gartner Information Technology Glossary: Cloud Access Security Brokers (CASBs)*. <https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs>.

3.Prescott, Susan. *The top 10 web application security risks*. AT&T Business. <https://www.business.att.com/learn/tech-advice/the-top-10-web-application-security-risks.html>.

8.7 Change Impact Analysis

1. Introduction
2. Business Analysis Practitioner (BA) Focal Points
3. Use Cases
4. Related Risks
5. Technology and Process Expertise

8.7.1 Introduction

- Impact Analysis (IA) is an important process in the overall strategy to become resilient against cyber threats and attacks. IA is a critical step in planning for a new solution and is generally required before performing a risk assessment and the resulting change to the business.
- Another goal of an IA is to identify the relationships and dependencies a business function has with other activities, both internal and external to the organization.¹
- A Solution IA identifies the considerations that will impact people, process, and technology within the organization. This step will be the foundation for developing the solution to minimize impact across the organization.
- This module focuses on the business impacts potentially introduced by requirements related to cybersecurity.
- The focus of this module is not to be confused with business impact analysis, the disaster recovery, or outage, impact analysis which is covered in another module.

8.7.2 Business Analysis Practitioner (BA) Focal Points

- Performing the impact assessment related to cybersecurity will identify specific changes that will impact people, processes, and technology:
 - Technology needs will be identified through the IA and may require purchasing, repurposing or reconfiguring hardware. Systems must be designed to align with security policies.
 - Planning is required to prepare the organization to have the right human resources to meet the needs of the solution. Skills assessments should be performed to understand the needs. Communication, readiness assessments, training and potentially recruiting, will be required.
 - New processes will be defined that need to be adopted as per the organization change management steps above which will enforce the security controls. Any residual risk should be considered as part of the new process.
 - Considerations of the impact to people, processes and technology may extend beyond the organization to customers, partners and vendors.

1..Business impact analysis (BIA) at heart of disaster recovery planning. ComputerWeekly.com. May 2011. <https://www.computerweekly.com/podcast/Business-impact-analysis-BIA-at-heart-of-disaster-recovery-planning>.

8.7.3 Use Cases

- Developing a customer facing solution will require more rigorous analysis of security controls to protect network traffic and data assets.
- In a Commercial-off-the-Shelf (COTS) application, there may be constraints that do not align with existing security policies. This could be a factor in solution selection, customization or configurations.
- Single Sign-on (SSO) authentication requirements for an organization may be compromised or difficult for specific SaaS or COTS solutions; even in-house development may have challenges with certain solutions.
- Identification of cyber impacts may be difficult for production maintenance or upgrade initiatives. Change management may enforce this assessment as part of the approval process.
- Digital solutions, such as Internet of Things (IoT), with changing endpoint security requirements will require impact assessments consistent with the rate of change within the environment.
- Changes to compliance policies, ownership, new geographic regions or regulations may require an impact assessment.

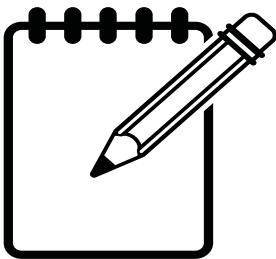
8.7.4 Related Risks

- Insufficient information or knowledge may make it difficult to identify impacted stakeholders or systems.
- Organizational Change Management (OCM) may not be equipped or prepared to address new and changing security requirements.
- Existing or legacy systems may not have undergone the same rigor as new systems and may have unknown security controls.
- In certain cloud environments (Software-as-a-Service, Infrastructure-as-a-Service, Platform-as-a-Service), the third party may not properly communicate or perform their own impact assessments when managing their solutions.

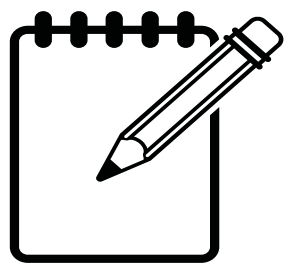
8.7.5 Technology and Process Expertise

- Business knowledge will enable the BA to facilitate formal and informal information gathering sessions to identify impacts to people, process and technology.
- General knowledge about how to collect information from stakeholders, legal and regulatory agents, financial statements, and from process flow maps and procedures. Research may require reviewing historical documents, contracts and diagrams.
- Knowledge of security concepts and their options will help to ensure high-quality impact assessments.
- Risk management expertise will help to quantify and qualify potential impacts.
- Understanding of OCM best practices will help to identify potential resistance and to employ strategies to increase adoption.
- Understanding of data storage and retrieval for the impacted system(s).

NOTES



A series of horizontal dashed lines for taking notes.



NOTES

Area with horizontal dashed lines for taking notes.

9

Module 9: Operations

1. Incident Response, Recovery, and Remediation
2. Metrics and Reporting
3. Risk Logging and Mitigation Tracking
4. Operational Risk Ownership
5. Computer Forensics: SOC, SIEM
6. Future Proofing your Security Posture

9.1 Incident Response, Recovery, and Remediation

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Cost of Cybersecurity Incidents and Breaches
5. Related Risks
6. Technology Controls
7. Process Controls

9.1.1 Business Analysis Practitioner (BA) Focal Points

- The business analysis practitioner (BA) may be asked to participate or lead the effort to draft an incident response plan for cybersecurity threats, breaches, and events.
- The BA may be asked to engage the leadership to secure approval and funding to enact a cybersecurity incident response plan and the subsequent training.
- The BA who is engaged in establishing processes and procedures related to incident response and recovery planning may be asked to lead the effort to identify vulnerabilities, and to identify ownership of data, systems, applications, and services that could be affected by a breach.

- The BA working in cybersecurity may be asked to establish documented processes to backup and restore vital systems, databases, computers, and network configurations, and to store these securely so that only authorized people can gain access.
- Working with the Risk and Governance officers, the BA may be asked to analyze recovery planning and restoration activities, and to recommend changes.

9.1.2 Key Terms and Definitions

- **Incident response and recovery:** The response of an enterprise to a disaster or other significant event that may significantly affect the enterprise, its people, or its ability to function productively, which followed by the phase in the incident response plan that ensures that affected systems or services are restored to a condition specified in the service delivery objectives (SDOs) or business continuity plan (BCP). ¹
- **Security Incident Response Team (SIRT):** Organization that enacts the company's established incident response plan when a threat has been detected.
- **Business Continuity Plan (BCP):** Measures taken to provide access to business resources, additional infrastructure and services such as VPN and secure gateways for remote access to critical business assets following an incident.
- **Breach:** Any incident that results in unauthorized access to data, applications, services, networks, and/or devices by bypassing underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters a private, confidential or unauthorized logical IT perimeter. ²
- **Cyber-attack:** A deliberate exploitation of computer systems, technology-dependent enterprises, and networks. Cyber-attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft. ³
- **Mean time to detect (MTTD):** The average amount of time it takes to discover an issue. It measures the period between the beginning of a system outage, service malfunction or any other revenue-generating activity and the amount of time a DevOps team needs to identify this issue. ⁴
- **Mean time to Resolve (MTTR):** The time it takes to fix a failed or compromised system. It is also known as mean time to resolution. ⁵

1.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

2.Techopedia.com. *Definition - What does Security Breach mean?*. <https://www.techopedia.com/definition/29060/security-breach>.

3.Techopedia.com. *Definition - What does Cyberattack mean?*. <https://www.techopedia.com/definition/24748/cyberattack>,

4.Alert Ops. *MTTD vs. MTTF vs. MTBF vs. MTTR*. May 2018.

5.Ibid.

- **Root Cause Analysis (RCA):** an approach for identifying the underlying cause of an incident so that the most effective solutions (to prevent the incident from recurring), can be identified and implemented¹

9.1.3 Use Cases

- In preparing for incident response planning, identify roles and responsibilities of the SIRT members, secure approval and funding, and ensure adequate training is available.
- Determine what process or processes will enable the SIRT to monitor for threats; identify a threat, breach or incident; how the incident is reported, when, where and by whom; the scope or degree of impact; and the duration of the incident.
- Containment management planning requires input from several sources and agencies within a business, in a timely and efficient manner to prevent additional and unnecessary damage or loss, i.e., changing passwords to all accounts with administrative access to prevent the spread of the threat.
- Establish a process for identifying the root cause of the breach and eliminating the threat without deleting or harming valuable business assets and data.
- Begin recovery and restoration of business systems without risking a repeated similar attack.
- Following the effective recovery and restoration of affected systems, analyze and evaluate what worked, what didn't work, the effectiveness of the Incident Response Plan and training, and strengthen the security from lessons learned.

9.1.4 Cost of Cybersecurity Incidents and Breaches

- Organizations spend more than ever to deal with the costs and consequences of more sophisticated attacks; the average cost of cybercrime for an organization increased US\$1.4 million to US\$13.0 million.²
- As the average costs of breaches increases, spending on cybersecurity will need to increase, and focus on establishing business resilience.
- The average cost of a malware attack on a company is \$2.4 million.³

1.IIBA. *A Guide to the Business Analysis Body of Knowledge® version 3*. International Institute of Business Analysis. 2015.

2.Ponemon Institute LLC. *Ninth Annual Cost of Cybercrime Study*. Accenture.March 2019. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50.

3.Accdnture. *Cybersecurity threats are growing. Attack them*. <https://www.accenture.com/us-en/about/security-index?src=SOMS#block-insights-and-innovation>.

- The most expensive component of a cyber-attack is information loss, which represents 43% of costs.¹
- The cost of establishing standards, governance, and risk assessments is prohibitive to many government and smaller non-governmental organizations without expert guidance and consultation.
- Companies with an incident response team that regularly and extensively tests their incident response plans experience significantly less in data breach costs than organizations that didn't have incident response in place.
- Breaches originating from a third party (such as a partner or supplier) cost \$370,000 more than average, emphasizing the need for companies to closely vet the security of the companies they do business with.

9.1.5 Related Risks

- Incomplete, inadequate or non-existent incident response plans lead to extended downtime, loss of business opportunities, higher risk to vulnerable and affected systems, and huge financial impact.
- Under-funded, under-trained and poorly equipped incident response teams are unable to perform necessary or even critical steps to identify, isolate, and remove threats; or may be unable to perform vital investigations into possible attacks.
- In addition to unexpected costs incurred from the loss of valuable data, system downtime, and missed opportunities, are the potential legal fees, damage to the company's reputation, and cost to recover valuable data.
- Recovery plans that don't include enterprise-wide backup communications and securing remote access to valuable company data impact the time to recovery and add to overall business losses.
- Prioritizing detection and protection schemes is complicated and challenging to many agencies and firms.

9.1.6 Technology Controls

- Incident response and recovery planning requires secure communications and a secured repository, so the plans are available only to those who are authorized to view and modify them.
- Modifications to incident response and recovery processes and procedures should be tracked and authorized.
- Incident response teams must have access to incident response plans and to various individuals and organizations during an incident, and this may require additional technology infrastructure including secure remote access (VPN), secure network gateways, backup communication tools, enterprise-wide alert and messaging systems.

1.Ibid.

9.1.7 Process Controls

- Managing processes to recover and restore affected business units requires engagement with all stakeholders and business partners; if the documented processes lack detail, substance or order, recovery time will be negatively impacted, and additional costs and loss could increase.
- Recovery planning and procedures must be updated and communicated to affected business partners, so they are aware of the processes during an incident to minimize the impact.
- Documented incident response and recovery training plans and training sessions may be required by compliance and regulatory offices to maintain compliance with governing agencies.
- Root cause analysis should be performed following an incident and measures taken to correct and prevent future similar incidents. Corrective actions could include training, or new or modified controls; for example, common techniques include fishbone (Ishikawa) or the 5 whys.

9.2 Metrics and Reporting

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

9.2.1 Business Analysis Practitioner (BA) Focal Points

- Understand how cybersecurity systems can be monitored, measured and analyzed, providing decision makers with accurate, quantifiable, and actionable data.
- Understand the value of collecting metrics, analyzing, and evaluating the data to enable decision makers to mature their systems and processes.
- Understand how quantifiable analysis of measurement data and tools can be applied throughout the Software Development Life Cycle (SDLC) of the systems being monitored.
- Understand how regulatory and legislative guidelines support security performance measurements and reporting, including Government Performance Results Act (GPRA), Federal Information Security Management Act (FISMA), and National Institute of Standards and Technology (NIST).
- Develop a business case to acquire resources needed to implement remediation actions; and based on industry practices and mandatory or regulatory guidelines.

9.2.2 Key Terms and Definitions

- **Enterprise Risk Management (ERM):** The discipline by which an enterprise in any industry assesses, controls, exploits, finances and monitors risk from all sources for the purpose of increasing the enterprise's short- and long-term value to its stakeholders.¹
- **Key Risk Indicators (KRIs):** A subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk.²
- **Key Performance Indicators (KPIs):** A measure that determines how well the process is performing in enabling the goal to be reached.³

1.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

2.Ibid.

3.Ibid.

9.2.3 Use Cases

- Risk managers must provide evidence that the security controls put in place are efficient and effective. Measuring and analyzing controls enables the security team to modify and adjust controls to meet changing conditions and are prioritized by business leaders.
- Risk managers report security performance to internal and external parties, such as boards, auditors and regulators, as well as provide value to internal and external entities, like fellow employees, investors, and customers by enabling target-driven metrics about the quality and effectiveness of the organization's security control systems.
- Security measures are used to facilitate decision making, and to improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. When business is engaged in monitoring, analyzing, and reviewing the metrics, they become willing and active partners in the enterprise security efforts.¹
- Risk assessments should measure the value of the organization's ERM, and identify gaps in process and methodology performance across the organization. Gauging the measuring systems should be an ongoing activity to ensure the right measurements are being performed and that reporting processes are effectively informing decision makers.

9.2.4 Related Risks

- Cyber threats are constantly evolving and new threats emerge on the landscape with increasing frequency. Planning for all possible types of threats isn't possible, which requires ongoing monitoring and reporting of existing security controls, as well as frequent and planned risk and gap assessments, followed by adjustments to monitoring and controls necessary to meet or mitigate new cyber threats.
- Business processes change and evolve to meet business needs, and with that the technology supporting the business processes change over time. Security controls must adapt with those changes to remain relevant, and if changes aren't performed in a timely or sufficient manner, the system may be exposed to cyber threats. Metrics support informed decisions about where, how much, and when to implement controls.
- Metrics must be analyzed and evaluated before they become meaningful, and if they are not properly stored, analyzed, and reported, decision makers won't be getting the best information available, or they may not receive information in time to prevent or mitigate a cyber threat.
- Data collection and measurement systems depend, in part, on the maturity of the security systems put in place and on the maturity of the ERM designed to analyze and report on the metrics. As the organization matures, and automation is introduced to data collection processes, efficiency and effectiveness will improve.

1.National Institute of Standards and Technology (NIST). NIST SP 800 55: *Performance Measurement Guide for Information Security*. U.S. Department of Commerce. July 2008.

- Resources are limited and the cost to implement an effective measurement system is difficult to justify and requires commitment and investment on the part of senior leadership. Without the investment and commitment, metrics to quantify the effectiveness and efficacy of security controls can be easily overlooked, and this greatly increases risk to the business.

9.2.5 Technology Controls

- Data collection points
- Monitoring systems
- Data storage and access controls
- Automated reporting tools

9.2.6 Process Controls

- Security audits
- Risk assessments
- Risk registers
- Cost-risk analysis

9.3 Risk Logging and Mitigation Tracking

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Risk Management
5. Risk Register
6. Mitigation Tracking
7. Technology and Process Controls

9.3.1 Business Analysis Practitioner (BA) Focal Points

- Perform risk assessment within a business unit, organization or the enterprise.
- Identify and classify risks into common groups.
- Establish risk mitigation plans and share with stakeholders for sign-off.
- Author the Risk Register and encourage its continued use.
- Prepare an exit strategy to accompany risk taking activities.
- Participate in ongoing risk mitigation monitoring.
- Understand and communicate the challenges and shortcomings of relying on risk mitigation strategies and tools.

9.3.2 Key Terms and Definitions

- **Risk:** A function of the likelihood of a given threat-source's exercising a particular, potential vulnerability, and the resulting impact of that adverse event on the organization.¹
- **Risk register/Risk log:** Record of information about identified risks.²
- **Risk management:** The identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events; or to maximize the realization of opportunities.³
- **Risk Mitigation Planning:** as mitigation is determined as the treatment for a risk, the mitigation options are discussed, effective controls and actions are identified, and a plan for implementation is determined.

1.National Institute of Standards and Technology (NIST). NIST SP 800 55: *Performance Measurement Guide for Information Security*. U.S. Department of Commerce. July 2008.

2.International Organization for Standardization (ISO). *ISO 3100: Risk Management-Guidelines*. International Organization for Standardization (ISO). 2018.

3.International Organization for Standardization (ISO). *ISO 3100: Risk Management-Guidelines*. International Organization for Standardization (ISO). 2018.

- **Risk Mitigation Implementation:** putting in place the mitigating controls identified to address a risk.
- **Risk Mitigation Progress Monitoring:** tracking, measuring and reporting on the implementation status and effectiveness of initiated mitigations, as well as evaluation of the risk being mitigated.

9.3.3 Use Cases

- Facilitate stakeholders through risk treatment and mitigation strategy exercises.
- Create and maintain risk register (risk log) at project, program, and organization levels.
- Planning and monitoring for risk mitigation to achieve compliance and increase resiliency.
- Update risk scores and metrics as treatments are implemented and risks are reduced
- Auditors will request evidence of risk logging and mitigation tracking.

9.3.4 Risk Management

- Risk logs may be used to track risks through their evolution.
- Four phases of a risk management plan are typically:
 - Risk Identification
 - Risk Analysis
 - Risk Evaluation
 - Risk Treatment
- Typically risk analysis and evaluation are documented in separate, supporting documents, and the logs will track the treatment status over time for each identified risk.

9.3.5 Risk Register

- A risk register is a living document that is created to list and track identified risks, and should include the following information for every risk:
 - unique identifier,
 - description,
 - likelihood of occurrence,
 - impact to business,
 - any associated threats or vulnerabilities that have been identified,
 - the planned treatment,
 - risk owner,
 - status, and
 - all significant dates.

9.3.6 Mitigation Tracking

- Risk assessment occurs periodically, sometimes annually; risk tracking occurs continuously and provides feedback into the other risk management activities, such as identification, analysis, mitigation planning, and mitigation plan implementation.¹

9.3.7 Technology and Process Controls

- Technology:
 - Software exists that can be used to track and manage Risk Logs; however, a simple spreadsheet can be just as effective and facilitates effective reporting and sharing across stakeholder groups.
- Process:
 - Risk Review teams should establish regular meetings to log new risks and update the status of ongoing ones.
 - Responsibility for maintaining the logs must be clearly identified.

1. Long, Richard. *Monitoring Risk: Tracking Your Risk Mitigation Strategies*. MHA Consulting. November 2017. <https://www.mha-it.com/2017/11/07/monitoring-risk/>.

9.4 Operational Risk Ownership

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Responsibilities
4. Use Cases
5. Related Risks
6. Technology Controls
7. Process Controls

9.4.1 Business Analysis Practitioner (BA) Focal Points

- The business analysis practitioner (BA) should have a broad understanding of enterprise risk management strategies, and recognize which ones are appropriate for the organization.
- Understand the roles and responsibilities associated with the risk owner or risk custodian.
- Understand the role or impact that an organization's culture plays in establishing an effective risk treatment plan, and how it enables risk owners' effectiveness.
- Able to review and assess the risk register for risk ownership activities and summarize those in leadership reports.

9.4.2 Key Terms and Definitions

- **Risk management strategy:** The approach that addresses how an organization intends to assess risk, respond to risk, and monitor risk, establishes a foundation for managing risk, and delineates the boundaries for risk-based decisions within organizations.¹
- **Risk factors:** A condition that can influence the frequency and/or magnitude and, ultimately, the business impact of IT-related events/scenarios.²
- **Risk response plan:** An organization's plan to address identified risks, through risk avoidance, risk acceptance, risk sharing/transfer, and risk mitigation, leading to a situation that as much future residual risk as possible falls within risk appetite limits.³
- **Risk Owner:** The person or held position who is ultimately accountable for managing an identified risk, coordinating mitigation efforts, and reporting on the status of the risk and mitigation plans.

1.National Institute of Standards and Technology (NIST). *NIST SP 800 30: Information Security: Guide for Conduction Risk Assessments*. U.S. Department of Commerce. September 2012.

2.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

3.Ibid.

9.4.3 Responsibilities

- Typically the Risk Owner is responsible for:
 - Either following the organization's level of risk tolerance, or establishing a risk tolerance level appropriate for their domain
 - Identifying risks within their business unit, assessing them, and determining treatment plans
 - Ensuring risks and mitigation plans are documented, communicated and reported appropriately
 - Tracking, monitoring risks and mitigation effectiveness, and remediating any gaps
 - Integrating risk identification and management into operational activities, and fostering a culture of risk awareness
 - Stay aware of internal and external changes and advancements and how risks may be introduced or affected

9.4.4 Use Cases

- Critical risks and risks that exceed the tolerance levels identified by the organization's risk assessment should be assigned to a person who is accountable and responsible to manage the risk on a day-to-day basis.
- Risk ownership assignment should consider the maturity and capabilities of the organization to manage their risk, based on the risk management plan. Not all risks need an owner.
- Risk owners need to have clearly defined roles; a common, consistent language; and adequate training to effectively manage the risk assigned to them.
- Risk owners may assign risks or sub-risks to team members within their business unit, not only to balance the work load and responsibilities involved, but as a way to foster the risk awareness culture more broadly.

9.4.5 Related Risks

- If risk ownership roles are vaguely or loosely defined, the accountable and/or responsible person is more likely to miss opportunities or neglect responsibilities during the risk life cycle.
- Risk owners who are not equipped with the appropriate level of authority will need the support of their leadership to respond to threats, potentially increasing response time and likelihood or increased impact during an incident.

9.4.6 Technology Controls

- Risk management software tools.
- Risk register for actively documenting ongoing risk mitigation and threat-shifting activities.

9.4.7 Process Controls

- Enterprise Risk Management (ERM) strategy.
- An approach to developing an organizational positive risk culture.
- A risk treatment plan with identified risk owners for the critical risks.

9.5 Computer Forensics: SOC, SIEM

1. Business Analysis Practitioner (BA) Focal Points
2. Key Terms and Definitions
3. Use Cases
4. Related Risks
5. Technology Controls
6. Process Controls

9.5.1 Business Analysis Practitioner (BA) Focal Points

- Identify data that will be imported into the SIEM tool and how that data will be secured and utilized.
- Identify the organization-specific threats and develop the appropriate procedures and responses for action on event detection.
- Define the service catalog, the full scope of services to be deployed within the SOC and their interrelation.
- Define the organizational change including staffing levels and training required to support the SOC processes and services.

9.5.2 Key Terms and Definitions

- **Security Operations Center (SOC):** A combination of people, processes and technology protecting the information systems of an organization through: proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state, and minimizing damage from unwanted effects.¹
- **Security Information and Event Management (SIEM):** Supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting).²
- **Governance, Risk, and Compliance (GRC):** A strategy for managing an organization's overall governance, enterprise risk management, and compliance with regulations. A GRC software solution allows organizations to create and coordinate policies and controls and map them to regulatory and internal compliance frameworks.
- **Managed Service Provider (MSP):** Delivers services, such as network, application, infrastructure and security, via ongoing and regular support and active administration on customers' premises, in their MSP's data center (hosting), or in a third-party data center.³

1.Crowley, Christopher and John Pescatore. *The Definition of SOC-cess?; SANS 2018 Security Operations Center Survey*. SANS Institute. August 2018. <https://www.cyberbit.com/wp-content/uploads/2018/08/SANS-SOC-Survey-2018.pdf>.

2.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

3.Gartner. *Gartner Information Technology Glossary: Managed Service Provider (msp)*. <https://www.gartner.com/en/information-technology/glossary/msp-management-service-provider>.

- **Cloud Access Security Broker (CASB):** On-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement.¹
- **Identity Access Management (IAM):** Encapsulates people, processes and products to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources. The goal of IAM is to provide appropriate access to enterprise resources.²
- **User and Entity Behavior Analytics (UEBA):** A type of cyber security process that takes note of the normal conduct of users. In turn, they detect any anomalous behavior or instances when there are deviations from these "normal" patterns.³

9.5.3 Use Cases

- The following attributes are important to have in a Security Operations Center (SOC):
 - The technical solution's capabilities should be powerful enough to effectively perform within the environment's security posture
 - Business and change management processes should be well defined, clearly documented, consistently enforced, efficiently maintained.
 - Business processes should be evaluated frequently for improvement opportunities, and to ensure they are aligned with technical advancements made within the solution.
- To survive attacks, organizations must be aware of potential threats (IDS), detect incidents early and react quickly (IPS). It is important to align the objectives of the SIEM with the strategic goals of the organization.
- If access control is not managed adequately when users change roles or leave the organization, they may still retain unnecessary access to applications; a SIEM can scan the global environment and identify unused credentials.

1.Gartner. *Gartner Information Technology Glossary: Cloud Access Security Brokers (CASBs)*. <https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs>.

2.ISACA. *Cybersecurity Fundamentals Glossary*. ISACA. 2016. <https://www.isaca.org/Pages/Glossary.aspx>.

3.Brook, Chris. *What is User and Entity Behavior Analytics?*. DATAINSIDER. December 2018. <https://digitalguardian.com/blog/what-user-and-entity-behavior-analytics-definition-ueba-benefits-how-it-works-and-more>.

9.5.4 Related Risks

- If the technical solution is limited in its capabilities, it may perform effectively within the environment, missing event correlations and result in an incident.
- It takes an organization that does not have a SOC an average of 206 days before a breach is detected. During that time, the organization is at risk for financial, data, and reputational losses.
- Due to the large amount of data stored in SIEM tools, they are also attractive targets for would be attackers. Security of the SIEM tool and data stored within it are of critical importance, as the central nature of the tool itself leads to it being a one stop location for critical information.

9.5.5 Technology Controls

- Anti-Virus/Anti-Malware (AV/AM) software to prevent against infection of systems
- Cloud Access Security Broker (CASB)
- Identity Access Management (IAM)
- Intrusion Detection System/Intrusion Prevention System (IDS/IPS)
- Next Gen Firewalls combine a traditional firewall with additional network device filtering utilities making them more fortified.
- Network Segregation creates zones of trust within the network, to separate network traffic from untrusted sources

9.5.6 Process Controls

- Security Awareness Training is performed to ensure the organization is familiar with common threats and vulnerabilities such as phishing and social engineering. It ensures the organization takes steps to protect itself from these threats.
- A Threat Risk Assessment, commonly known as a TRA is a risk analysis tool for identifying potential threats to a software solution; it includes identification of vulnerabilities within, and assesses the security risk that would result should a threat be realized.
- Principle of Least Privilege provides the minimum privileges for a user to perform their work.
- Internal and External Security Audits check and enforce that security controls are effective.

9.6 Future Proofing your Security Posture

1. Summary of Key Topics
2. Business Analysis Practitioner (BA) Focal Points
3. Changes that impact Security
4. Infrastructure and Technical Topics
5. Access Controls and Data Level Topics
6. Solution Delivery Topics
7. Operations Security Considerations
8. The Future of Cybersecurity
9. Concluding Considerations
10. Summary

9.6.1 Summary of Key Topics

- Cybersecurity Imperative
 - The expansion of technology in our business and in our lives has made cybersecurity a top of mind concern for enterprises, government, and individuals.
- IIBA Perspectives
 - Enterprise Governance and Risk
 - Infrastructure, and Networking
 - Applications and Information integrity
- Business Analysis Focal Points
 - Analysis is the basis of planning and preparation for a secure cyber environment.
 - Business Analysis is about understanding the requirements, the value, and in cybersecurity context it is about building in not bolting on security into everything we work on.

9.6.2 Business Analysis Practitioner (BA) Focal Points

- Enterprise Cybersecurity
 - Understanding the enterprise environment is a critical understanding, and is required to support governance and policy. Enterprise governance needs to consider the edges of the network.
 - Senior, seasoned business analysts work with the business, architects and security specialists in establishing the security framework and governance processes

- Infrastructure and Networking IT Cyber initiatives
 - BAs act with strong technical acumen as the liaison between the business and the technical team to assure business needs are effectively part of the requirements and plan and collaborate on key cyber initiatives. BAs work closely with and give support to operations.
- Applications and Information integrity
 - BAs play a critical role in assuring requirements are met for security, data integrity, user interface, system integration components, and additional functional and non-functional.
 - This role includes methodologies such as: Agile, DevOps, and other SDLC methods.
 - It applies to making sure the application or solution requirements are met while maintaining overall security controls in this layer. Most BA's work at this level.

9.6.3 Changes that impact Security

- Changing users: many businesses have more 'field' workers that use mobile laptops and smart phone mobile devices. They work from home, from the local café, and client locations.
- Changing scope: with changes like IoT (internet of things) we see more devices in the network that provide access to the network and to shared resources. Everything from point of sale devices, to HVAC systems are smart devices on the network, and create new security scenarios. The landscape is constantly changing and presenting new cyber threats.

9.6.4 Infrastructure and Technical Topics

- Technical and Infrastructure are also changing: Traditional data centers and network hubs had a central hub and spoke model. Protect the core and security was good. This is no longer the case for many. It is more a mixed data center, network center, and cloud-based set of components.
- In addition to the hub and spoke, there is more of an architecture to move to 'direct to internet'. This has SaaS, PaaS, and services like AWS, Azure, and Salesforce which are integrated with traditional architecture.

9.6.5 Access Controls and Data Level Topics

- Applications are more likely to exist outside the traditional data center and are on the Cloud based services.
- Sensitive data tends to move across data centers and cloud based environments, and creates a different need for security controls.
- Mobile 'apps' as well as traditional access create new control points.
- More smart devices in IoT move security to the edge of the network with more penetration points and more need to non-human access to the network and to applications.

- The long-term trend is that this will grow significantly and create a need to have more ability to control the cloud security using newer technology approaches.

9.6.6 Solution Delivery Topics

- Operational changes and technical approach to cybersecurity is evolving.
- More attention is needed to the pattern of change and the pace of change within each organization and enterprise.
- Cybersecurity as a Service firms are emerging which can support the evolving technology and infrastructure.
- Technology such as AI is becoming embedded in the threat detection landscape.
- The trends to 'mobile first' also add new challenges to monitor the cyber environment, as many firms continue to have global support issues for their globe trotting sales, service and executive teams.

9.6.7 Operations Security Considerations

- Incident Alerts, Escalation Process, Roles for response teams
- Incident Response, Recovery and Remediation
- Risk Log and Mitigation Tracking
- Operational Risk Management & Ownership
- Security Operations Center Concepts & SIEM – Security Information and Event Management
- Forensics and continuous improvement
- Future-Proofing your security Investment

9.6.8 The Future of Cybersecurity

- Artificial Intelligence (AI) will influence and empower us.
 - New data can be checked against data classification rules or generate notifications and workflow
- Security awareness and education needs to be central to securing organizations; it will become second nature.
- The principle of least privilege is a critical policy to apply throughout the organization.
- The right level of security should be applied:
 - Passwords for low-value accounts
 - Two and Three factor for escalating security
 - Biometrics for most valuable accounts
- Outsourced and cloud technology to manage Everything as a Service (XaaS) and Managed Security Services (MSS). Evolution of Azure, Amazon and Google security services. Tools like Zscaler to force users to go through secure layers to get to the Web.

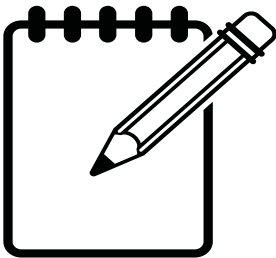
9.6.9 Concluding Considerations

- The black hats don't sleep; therefore, as we do our best to be proactive and to secure our solutions and our organizations, the landscape is continually evolving. What is secure today will likely not be secure tomorrow.
- Designing an organization with strong governance, policy and awareness will help to maintain a consistent approach to security across the organization.
- Considerations of cyber security while managing and developing infrastructure and delivery of solutions will help to ensure we are prepared to identify and respond to threats. As we balance security with ease of use, the role of the business analysis practitioner will be needed to address this evolving landscape.

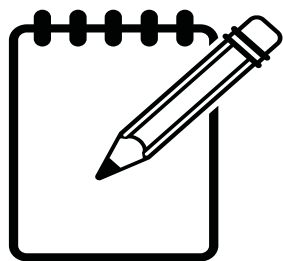
9.6.10 Summary

- Cybersecurity remains a critical concern for all enterprises and is an essential knowledge area for the business and for all BAs and many other professionals. No longer just a tech skill.
- Business analysis practitioners have an obligation to develop basic knowledge and competency in the effective use of cybersecurity tools and approaches to information and process management.
- IIBA and IEEE have partnered to provide a robust perspective on what the business and the business analyst need to know to be prepared for today's challenges. The training and the certification give everyone the opportunity to learn key concepts needed to perform, and the credibility of a joint certification to demonstrate core competency.
- The information provided is a broad-based set of the basics of cybersecurity designed around the kind of analysis needed to assist in the overall cybersecurity solution, but leverages the collaboration of the business, the analyst, the architects and the technology experts to create a safe and secure cyber environment.

NOTES



A series of horizontal dashed lines for taking notes.



NOTES

A series of horizontal dashed lines for taking notes.

Unfilled cybersecurity jobs worldwide will reach 3.5 million by 2021.

More than 300,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74% over the past five years.

<https://thehill.com/opinion/cybersecurity/365802-cyber-jobs-are-available-but-americans-dont-realize-they-are-qualified>

About International Institute of Business Analysis

International Institute of Business Analysis™ (IIBA®) is a professional association dedicated to supporting lifetime learning opportunities for business and professional success. Through a global network, IIBA connects with over 29,000 Members and more than 300 Corporate Members and 120 Chapters. As the recognized voice of the business analysis community, IIBA supports the recognition of the profession and discipline and works to maintain the global standard for the practice and certifications. For more information visit iiba.org.

About The IEEE Computer Society

The IEEE Computer Society is the premier source for information, inspiration, and collaboration in computer science and engineering. Connecting members worldwide, the Computer Society empowers the people who advance technology by delivering tools for individuals at all stages of their professional careers. Our trusted resources include international conferences, peer-reviewed publications, a robust digital library, globally recognized standards, and continuous learning opportunities.

Learn more about the Computer Society at computer.org.

Contributors:

Holly VanHelden (Lead SME), Principal IT Consultant, Iron Key Business Analytic Consulting

Allan Parrish, Associate Vice President for Research and Professor of Computer Science and Engineering, Mississippi State University

Bindu Channaveerappa, Business Analysis Consultant and Director of IIBA UK London Communities

Dylan Boudreau, Principal Consultant, Transom Consulting Group

Kevin Haines, Program Director, Sr BSA, Principal Consultant at Online Business Systems

Rich Hilliard, Software Systems Architect and Chair Engineering Disciplines, IEEE Computer Society

Terry Baresh, Principal Business Analyst, Securian Financial Group

Ken Fulmer, Former President & CEO, IIBA

