Enterprise Architecture Reference Guide

cloud security alliance®

The permanent and official location for the Cloud Security Alliance Enterprise Architecture research is: https://cloudsecurityalliance.org/research/working-groups/enterprise-architecture/

Acknowledgments

Version 2

Lead Authors:

Jon-Michael C. Brook
Michael Roza

Contributors:

Shawn Harris
Sunil Shanthi
Michael Theriault
Rolando Marcelo Vallejos
Ashish Vashishtha
Suri Venkat
Henry Werchan

CSA Team:

Sean Heide
Stephen Lumpe (Cover)
Jim Reavis
AnnMarie Ulskey (Layout)
John Yeoh

Version 1

Chief Architect:

Jairo Orea

Lead Architects:

Dan Logan

Contributors:

Richard Austin
Ryan Bagnulo
Charleton Barreto
Jon-Michael Brook
Phil Cox
Earle Humphreys
Tuhin Kumar
Subra Kumaraswamy
Yaron Levi
Yale Li
Dan Logan
Scott Matsumoto
Rajiv Mishra
Anish Mohammed
Price Oden
Jairo Orea
David Sherr
Ken Trant
Ravila White
Vern Williams
Rob Wilson

CSA Team:

Jim Reavis
J.R. Santos
Kendall Cline Scoboria
Evan Scoboria
John Yeoh

Table of Contents

Foreword

The Cloud Security Alliance's Enterprise Architecture Working Group release of the "Enterprise Architecture Reference Guide" version 2. With this release, users receive a needed compilation of every domain and container within the CSA Enterprise Architecture 2.3.

The CSA Enterprise Architecture is a comprehensive approach for the architecture of a secure, identity-aware cloud infrastructure. EAWG leverages four industry standard architecture models: TOGAF, ITIL, SABSA, and Jericho. This approach combines the best of breed architecture paradigms into a comprehensive approach to cloud security. By combining business drivers with security infrastructure, EAWG increases the value proposition of cloud services within an enterprise business model. The CSA Enterprise Architecture was adopted by the National Institute of Standards and Technologies in NIST SP 500-299 and NIST SP 500-292.

While this document simply compiles the existing architecture definitions, it is needed for upcoming EAWG releases, including a CSA Cloud Controls Matrix (CCM 3.0.1) to EA mapping and a refresh to the Enterprise Architecture itself.

Best Regards,

The Enterprise Architecture Team Leads

Jon-Michael C. Brook John Yeoh Michael Roza Jim Reavis

Overview of the Enterprise Architecture

Out of common needs come common solutions. The Enterprise Architecture is both a methodology and a set of tools that enable security architects, enterprise architects, and risk management professionals to leverage a common set of solutions and controls. These solutions and controls fulfill a set of common requirements that risk managers must assess regarding the operational status of internal IT security and cloud provider controls. These controls are expressed in terms of security capabilities and designed to create a common roadmap to meet the security needs of their business.

Business requirements must guide architecture. In the case of the Enterprise Architecture, these requirements come from a controls matrix partly driven by regulations such as Sarbanes-Oxley and Gramm-Leach-Bliley, standards frameworks such as ISO-27002, the Payment Card Industry Data Security Standards, and the IT Audit Frameworks, such as COBIT, all in the context of cloud service delivery models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

From these requirements, a set of security capabilities have been defined and organized according to best practice architecture frameworks. The Sherwood Business Security Architecture (SABSA) defines a security model from a business perspective. The Information Technology Infrastructure Library (ITIL) specifies the schema needed to manage the company's IT services, and thus, the security guidelines to manage those services securely. The Jericho Forum designates technical security specifications that arise from the reality of the traditional in-the-datacenter technology environments shifting to one where solutions span the internet across multiple datacenters, some owned by the business and some purely used as an outsourced service. Lastly, The Open Group Architecture Framework (TOGAF) provides an enterprise architecture framework and methodology for planning, designing, and governing information architectures, concluding in a common framework to integrate the work of the security architect with the enterprise architecture of an organization.

How to Use the Enterprise Architecture

The Enterprise Architecture can be used to assess opportunities for improvement, create road maps for technology adoption, identify reusable security patterns and assess various cloud providers and security technology vendors against a common set of capabilities.

Assessing Opportunity

Because the Cloud Security Alliance Controls Matrix is mapped back to existing security controls requirements from various legal and regulatory frameworks, and because that same matrix is mapped to the security capabilities of the architecture, it is easy for a company to assess which capabilities it has in place for compliance with applicable regulations and best practice frameworks.

Create Road Map

After assessing the current capabilities of the organization, the reference architecture can be used to guide those capabilities which need investment based on the business needs of the company as either a cloud consumer or a cloud provider. For instance, in a cloud-based solution, the physical security controls and capabilities are less critical to the cloud consumer and more critical to the cloud provider. Furthermore, the capabilities of the architecture can be used to organize the technology standards portfolio of an organization to identify areas where multiple technologies exist for the same capability, demonstrating that those technology functions can be consolidated. Conversely, it can show capabilities for which a company does not yet have a standard technology in place.

Identify Reusable Security Patterns

As security patterns and best practices are built around the reference architecture, sharing of these patterns within and between companies will be enhanced due to the common capabilities models that tie them together. Vendors can certify their solutions against the set of capabilities and controls in the architecture, thus giving consumers of their solutions more assurance in, and understanding of, the vendors' solutions.

Assess Cloud Service Providers and Security Technology Vendors

The defined controls are written in clear and concise contract-ready requirements verbiage and can be used with little to no modification as the basis of service contracts and requests for proposal (RFPs).

Table Definition Usage

Each of the below area tables (BOSS, ITOS, TSS, SRM) break out all the domains, component groups, sub-groups and containers. The hyphens at the beginning of each element in the Area Component column designate the hierarchy of the Enterprise Architecture naturally understood in the diagrams and drill downs.

Area Components	Definition
1 Domains	Top tier item, segmenting the areas, such as Governance Risk & Compliance in SRM or Compliance in BOSS
2 Component Groups	Second tier item, segmenting the domains into subtopics, such as Audit Planning in BOSS--> Compliance or Compliance Management under SRM--> Governance Risk & Compliance.
3 Component Sub-Groups	Third tier item (depending on components, containers may be at this level)
4 Containers	Lowest level elements within the architectural diagrams

CSA Enterprise Architecture

This EA Reference Guide v2 document corresponds with two representations of the CSA Enterprise Architecture. The interactive representation resides on the Cloud Security Alliance's website, and allows drill down into each of the various areas, domains and containers.

Figure 1: Interactive CSA Enterprise Architecture Diagram[1]

The other, and original, representation consists of a Visio diagram useful for offline or reference situations.

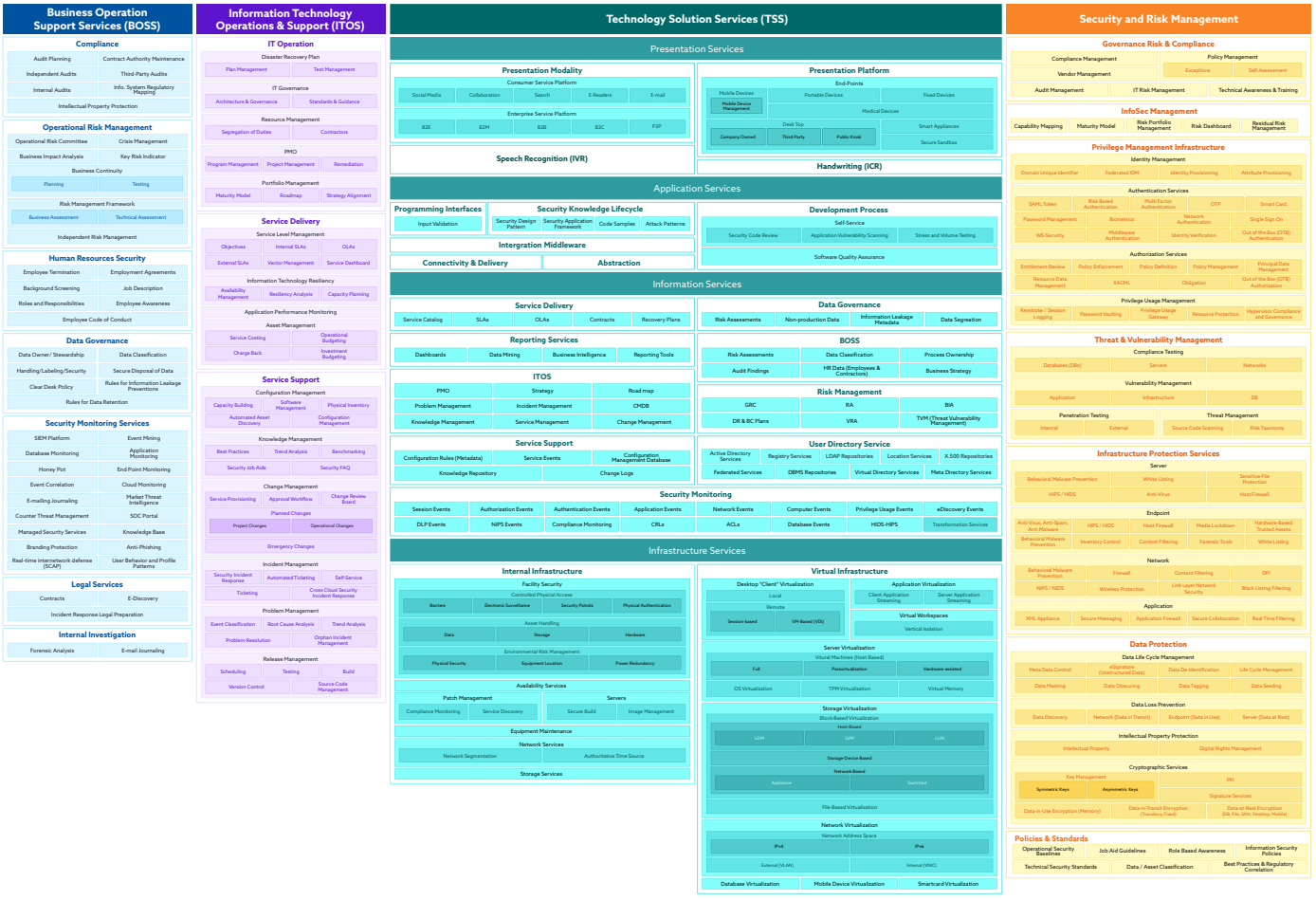

Figure 2: Enterprise Cloud Architecture Visio Diagram[2]

[1] https://ea.cloudsecurityalliance.org/index.php/explore/

[2] https://ea.cloudsecurityalliance.org/index.php/resources/

Business Operation Support Services (BOSS)

Partners with the business

Description

The BOSS domain is all the corporate support functions such as Human Resources, Compliance, and Legal that are critical to a security program. It is also the place where the company's operations and its systems are monitored for any signs of abuse or fraud.

BOSS was designed based on best practices and reference frameworks with the proven success of aligning the business and transforming the information security practice across organizations into a business enabler.

Most of the security architectures focus only on technical capabilities, missing the opportunity to create a dynamic synergy with the business, transforming reactive practices into proactive areas, that eventually can enable business command centers that provide relevant information about the health around information assets and business processes.

A common concern when organizations decide to integrate services with cloud providers is the level of security the provider will offer, and the amount of exposure when data is hosted on a multi-tenant model. This domain outlines aspects that must be considered besides the technological solutions, such as legal guidance, compliance and auditing activities, human resources, and monitoring capabilities with a focus on fraud prevention.

BOSS Components	Definition
1 Compliance	The goal that organizations aspire to achieve in their efforts to ensure that they are aware of and take steps to comply with relevant laws, policies, and regulations.
2 Audit Planning	Audit planning ensures the audits are scheduled and take place, are adequately staffed, and are considered part of the overall business delivery aspects.
2 Contact / Authority Maintenance	Ensures that contact information for relevant authorities and critical business partners is kept up-to-date, so it is correct when you need it and it also enforces a risk limit for the corporate role level.
2 Independent Audits	Independent audits effectively prevent you from 'fooling yourself.' It ensures an unbiased review of the current business state of affairs related to security and compliance.

2 Third Party Audits	Ensures that the services you rely upon are consistent with your security requirements.
2 Internal Audits	Provides a cross-checking mechanism within the organization. In larger organizations, there is likely to be some level of independence as well.
2 Information System Regulatory Mapping	The main focus here is to ensure that all regulatory requirements are identified and that the business's compliance effort takes them into account.
2 Intellectual Property Protection	The main focus here is to ensure that the protection of the intellectual property is identified as a key business driver and that the compliance effort of the business takes this into account.
1 Operational Risk Management	Operational Risk Management provides a holistic perspective for risk evaluation from the business perspective, using the risk management framework will help to have insight into risks and threats to the organization, as well the framework will provide means to assess, manage, and control the different risks across the organization. The use of an Operational Risk Committee (ORC) should be in place to periodically discuss the threat and compliance landscape that the organization has throughout time. Usually, the participants for this committee are conformed by the business (i.e., CEO, COO, CIO, CFO), compliance (CRO, Compliance Officers), and Control personnel (Audit, Security, and Risk Management). The use of Business Impact Assessment methodologies will help the organization identify which processes are critical for the organization and plan accordingly to protect them, ensure proper continuity plans and measure the associated risk using Key Risk Indicators. Key Risk Indicators can be monitored periodically through a Risk Scorecard, integrating information from Security Monitoring Services or information consolidated on the Information Services Domain.
2 Operational Risk Committee	Ensures that operational considerations are given to all identified business risks. It is not possible to adequately prioritize risk unless true operational considerations are considered.
2 Crisis Management	The overall coordination of an organization's response to a crisis effectively with the overall goal of avoiding or minimizing damage to the organization's profitability, reputation, or ability to operate.
2 Business Impact Analysis	Ensures that the business impact, and not only the technical aspects of risk, are considered in the risk management process.

2 Key Risk Indicators	Identifies what the key risks are from a management or executive level. These are the key risk factors that can affect a specific business.
2 Business Continuity	Ensures that business continuity is considered in the risk management process. This should not only address business continuity but business resumption as well.
3 Planning	Preparing a business continuity plan and all the steps required to put it into action should it be required.
3 Testing	Testing a business continuity plan to ensure that it is effective.
2 Risk Management Framework	Ensures that a repeatable process is defined and documented that is workable within the business. The risk management framework must be used within the business context for which it is defined.
3 Business Assessment	Ensure that the business risks are identified, documented, and appropriate treatments are identified.
3 Technical Assessment	Ensure that the technical risks identified, documented, and appropriate treatments are identified.
2 Independent Risk Management	Risk Assessments performed by a third-party to assess the maturity of the organization's controls from a reference framework perspective (i.e., COBIT, ISO27001), regulatory perspective (i.e., SOX, PCI), this type of assessment could also include Security Testing (Black-Box, White-Box, Pen-Testing).
1 Human Resources Security	This section focuses on the security and risk management perspective for those processes and best practices associated with the interaction that persons (employees, contractors, or any other third-party) have with the organization's human resources function.
2 Employee Termination	The process for ensuring that an employee exit procedure minimizes the risk of an ex-employee misusing information assets after their term of employment. The process includes access removal to electronic accounts typically, turn off VPN or external email services, etc.
2 Employment Agreements	All contractual agreements entered between the organization and the employees, contractors, third party users, and customers, which specify the terms and conditions of their employment or service contract before granting access to data and services, which must explicitly include the parties responsible for information security. Examples include a privacy policy, intellectual property agreements, acceptable use, website terms, and conditions.

2 Background Screening	Background verification for personnel, contractors, and third-parties must be in place and should be proportional to the data classification to be accessed under local laws, regulations, and ethics.
2 Job Descriptions	Clear definitions of the responsibilities of a job help to identify the data access requirements of people with that job to ensure that they only have the minimum required access.
2 Roles and Responsibilities	Dividing the work among multiple positions with different roles and responsibilities allows for the segregation of duties to ensure appropriate integrity within an organization's processes.
2 Employee Awareness	This capability will focus on the management of materials and tools associated with the process of providing awareness to ensure compliance with regulatory requirements, security policies, and risk management best practices that will ensure that the organization will have a secure, compliant, and safe working environment. Examples of this include Clean-Desk Policy, Disaster Recovery, On-Line training, PII/PHI information protection, among others.
2 Employee Code of Conduct	This capability is intended to manage the lifecycle for a formal agreement between the personnel that interacts with the organization's data, assets, and services. The code of conduct must include expected behavior relevant to the organization from the Regulatory perspective, Information Security Policies and Risk Management best practices.
1 Data Governance	As the organization manages data between Applications, Services, and Enterprise Information Integration activities, the need to have a well define governance model that outlines and looks for compliance on how data is massaged, transformed, and stored throughout the IT infrastructure including internal and external services (i.e., SaaS, PaaS, IaaS, ASP, or others). Processes included in data governance include data ownership, how data should be classified, and responsibilities that data/ asset owners have for their applications and services, and the necessary controls for data throughout the lifecycle.
2 Data Ownership / Stewardship	This capability manages the communications, responsibilities, and associated processes for personnel that interacts with data throughout its lifecycle. Roles associated with the data interaction include Data Owners, Asset Custodians, Data Users, Supporting Services, and Delegates.

2 Data Classification	The process of assessing the value of information to the business and assigning it to different levels such as (protected, public, top-secret) based on the business's impact should the data be obtained by unauthorized individuals.
2 Handling / Labeling / Security Policy	This capability manages policies, procedures, and communication associated with labeling, handling, and security of data and objects which contain data.
2 Secure Disposal of Data	Ensure that data is destroyed appropriately to preclude its recovery (e.g., through digital forensic techniques).Documentation of such destruction should be in place and should be included in information lifecycle management processes.
2 Clear Desk Policy	A corporate policy that ensures sensitive information is not left out in the open for viewing or theft by unauthorized users.
2 Rules for Information Leakage Prevention	This capability manages policies, procedures, and business requirements associated with data loss prevention and controls related to data privacy and protection throughout the organization. Examples of this include Content Management, Share File Repositories, and Data usage from the Endpoint perspective.
2 Rules for Data Retention	This capability manages the policies, procedures, or requirements associated with keeping data (transactions information, email, document images, card swipes, online browsing history) as long as required to do so from the business and regulatory perspective, then secured disposal.
1 Security Monitoring Services	All capabilities associated with proactive security and risk management situational awareness across the organization with a business focus to prevent internal or external attacks, misuse of privilege, and data loss, while maintaining proper monitoring for the organization's data and access regardless where these services are allocated or managed (Cloud, Internal, Hosted, etc.)
2 SIEM Platform	The Security Information and Event Management Platform collects, correlates, reports, on multiple security information sources to maintain situational awareness.
2 Event Mining	Statistical analysis of historical events to determine patterns of normal and abnormal behavior.
2 Database Monitoring	This capability is a collection of database management system related events, including logins, queries, transactions, and administrative activity.

2 Application Monitoring	This capability is a collection of application-related events, including logins, access to sensitive data, transactions, administrative activity.
2 Honey Pot	A real or virtual system configured to attract and detect an intruder by mirroring a real production system.
2 Endpoint Monitoring	Collection of events associated with end user usage of devices.
2 Event Correlation	Process of analyzing and associating an event from one source with events from the same or other sources to derive additional information or detect activity patterns.
2 Cloud Monitoring	Collection of events associated with the usage of the services provided by cloud solutions at all layers of the application stack.
2 Email Journaling	Monitoring the contents of email to detect data loss, malware spread, or other email-based threats.
2 SOC Portal	A dashboard application maintained by the Security Operations Center to give overall visibility of the organization's security status.
2 Counter Threat Management	The overall process of managing threats and countermeasures.
2 Market Threat Intelligence	Cyber Intelligence information collected by distributed IDS sensors and analyzed by security firms. Also, this capability can consolidate Threat Intelligence from industry peers (i.e., HITRUST, Commercial branches from NSA, etc.)
2 Managed Security Services	An outsourced arrangement to provide some or all part of the security operations capabilities for an organization.
2 Knowledge Base	A repository of knowledge about the organization's infrastructure and operations to enable the Security Operations Center to respond to events efficiently.
2 Branding Protection	The monitoring of external entities and activity that poses risk to the organization's brand, such as imposter web sites, typo-squatting, etc.
2 Anti-Phishing	The ability to detect phishing attacks targeted at an organization's users such as inbound phishing emails.
2 Real-Time Internet Work Defense (SCAP)	Security Content Automation Protocol is a continuous assurance process that verifies compliance with security policies and procedures in real time.

2 User Behavior & Profile Patterns	Collection of events and information about users that profiles and identifies normal and abnormal behavior patterns such as application usage by specific users or roles.
1 Internal Investigations	Internal investigations are concerned with determining the factual truth and implications of a policy or criminal investigation. This process includes fraud detection, prevention, and forensic investigation.
2 Forensic Analysis	Forensic analysis is concerned with preserving, identifying, extracting, and analyzing potential evidentiary value items relevant to questions of fact regarding a policy or criminal violation.
2 Email Journaling	The processes and procedures that ensure all EMAIL traffic is recorded and preserved as required for regulatory compliance or support litigation.
1 Legal Services	As security incidents occur, the need for legal counsel is critical for organizations. There are several capabilities included that may help legal counsels lead compliance activities, deal with lawsuits, and track preventive awareness across the organization.
2 Contracts	An agreement between two or more parties with the serious intent of creating a legal obligation or obligations.
2 eDiscovery	e-discovery is concerned with how data responsive to a planned or ongoing litigation is identified, preserved, and produced.
2 Incident Response Legal Preparation	Processes and procedures to ensure that relevant information is identified, collected and preserved to support future litigation regarding the incident.

Example

The security monitoring tool alerts an analyst that a customer withdrawal transaction was initiated from a workstation in the IT department instead of the customer contact center. A special investigation is held with the help of HR and Legal to determine that a disgruntled system administrator has been stealing from the company.

Services Provided

Compliance: The main focus of Compliance capabilities is to track internal, external, third parties (such as customers), audit activities, and related findings. For Compliance, it is necessary to have a common repository that allows the organization to track and remediate the technical or operational gaps outlined by these findings.

Audit activities should include developing an annual plan that can simplify the audit process throughout the year, preventing redundant tasks.

A regulatory mapping process will help the organization coordinate and simplify control evidence that each capability or process generates and store it on the risk registry (Information Services Domain).

Associated Components:

- 2 Audit Planning
- 2 Contact / Authority Maintenance
- 2 Independent Audits
- 2 Third Party Audits
- 2 Internal Audits
- 2 Information System Regulatory Mapping
- 2 Intellectual Property Protection

Data Governance: As the organization manages data between Applications, Services, and Enterprise Information Integration activities, there is a need to have a well-defined governance model that outlines and looks for compliance on how data is massaged, transformed, and stored throughout the IT infrastructure, including internal and external services (i.e., SaaS, PaaS, IaaS, ASP, or others). Processes included as part of Data Governance include data ownership, data classification, and responsibilities that data/asset owners have for their applications and services, as well as the necessary controls for data throughout the lifecycle.

Associated Components:

- 2 Data Ownership / Stewardship
- 2 Data Classification
- 2 Handling / Labeling / Security Policy
- 2 Secure Disposal of Data
- 2 Clear Desk Policy
- 2 Rules for Information Leakage Prevention
- 2 Rules for Data Retention

Operational Risk Management: Operational Risk Management provides a holistic perspective on risk evaluation from a business perspective. Using the Risk Management framework will give insight into risks and threats to the organization. framework will provide a means to assess, manage, and control the different risks across the organization.

The use of an Operational Risk Committee (ORC) should be in place to periodically discuss the threat and compliance landscape that the organization has throughout time. Usually, the participants for this committee are grouped by the business (i.e., CEO, COO, CIO, CFO), compliance (CRO, Compliance Officers) and control personnel (Audit, Security, and Risk Management).

The use of business impact assessment methodologies will help the organization identify which processes are critical for the organization and plan accordingly to protect them, ensure proper continuity plans, and measure the associated risk using Key Risk Indicators.

Key Risk Indicators can be monitored periodically through a risk scorecard, integrating information from security monitoring services or information consolidated on the Information Services Domain.

Associated Components:

- 2 Operational Risk Committee
- 2 Crisis Management
- 2 Business Impact Analysis
- 2 Key Risk Indicators
- 2 Business Continuity
- 3 Planning
- 3 Testing
- 2 Risk Management Framework
- 3 Business Assessment
- 3 Technical Assessment
- 2 Independent Risk Management

Human Resources Security: Security incidents and breaches often happen to organizations because there are no formal controls, awareness, and guidelines for the most critical asset that organizations will have: people.

This section was created to ensure that formal procedures, codes of conduct, personnel screening, and other best practices are in place for the organization, especially for third parties that will support the cloud services that an organization may have.

Associated Components:

- 2 Employee Termination
- 2 Employment Agreements
- 2 Background Screening
- 2 Job Descriptions
- 2 Roles and Responsibilities
- 2 Employee Awareness
- 2 Employee Code of Conduct

Security Monitoring Services: The security and availability monitoring services were positioned in the Business Operations and Support Services Domain to ensure that the business is the focus, not the events or hardware. It is a common mistake not to focus the security function on the business operations, the processes, and the human behavior behind those processes. Transforming typical infrastructure monitoring into a business operations center, focused on fraud prevention, alignment with the business strategy, business impacts, and operational needs are the goal of a successful security monitoring service.

Organizations usually concentrate their monitoring activities only on reactive mode, losing the opportunity to become a business partner. By using monitoring services, businesses can identify new opportunities for process improvement as knowledge about employees' behavior is collected. Some employees have more access to many institutions than others to the most critical information, such as customer data, credit cards, etc. If the Security Monitoring Services focus on those users and their behavior, potential fraudulent activities can be prevented.

As the monitoring services start to be less reactive, and more proactive, the focus of Security Monitoring Services will shift from internal to external threats. This architecture outlines several capabilities oriented on cyber intelligence, looking to prevent threats before they become security incidents.

Associated Components:

- 2 SIEM Platform
- 2 Event Mining
- 2 Database Monitoring
- 2 Application Monitoring
- 2 Honey Pot
- 2 Endpoint Monitoring
- 2 Event Correlation
- 2 Cloud Monitoring
- 2 Email Journaling
- 2 SOC Portal
- 2 Counter Threat Management
- 2 Market Threat Intelligence
- 2 Managed Security Services
- 2 Knowledge Base
- 2 Branding Protection
- 2 Anti-Phishing
- 2 Real-Time Internet Work Defense (SCAP)
- 2 User Behavior & Profile Patterns

Legal Services: As security incidents occur, the need for legal counsel is critical for organizations. There are several capabilities included that may help legal counsels lead compliance activities, deal with lawsuits, and track preventive awareness across the organization.

Capabilities that can help increase, track, and manage regulatory compliance are also included and detailed.

Associated Components:

- 2 Contracts
- 2 eDiscovery
- 2 Incident Response Legal Preparation

Internal Investigation: The role of Internal Investigations varies across organizations; some companies have their information security teams performing forensic activities, and more mature companies may have a dedicated team focused on internal and/or external fraud activities.

To better assist investigators, capabilities are oriented to enable better Security Incident Response, Cyber Intelligence, Legal, Security Monitoring, HR, and Information Security teams.

Associated Components:

- 2 Forensic Analysis
- 2 Email Journaling

Relationships to other Domains

Business Operations Support Services defines the high-level policy requirements that IT Operation Support Services, Presentation Services, Application Services, Information Services, Infrastructure Services, and Security & Risk Management exist to support. BOSS embodies the direction of the business and objectives of the cloud consumer. BOSS is embodied in the Compliance objectives, Legal objectives, Human Resource requirements, Operational Risk tolerance, and Security Monitoring services that are required to satisfy a client's service-level objectives and jurisdictional legislative mandates.

The BOSS domain works to align the ITOS and the SRM domains with the business' desired strategy, capabilities, and risk portfolio.

Information Technology Operation & Support (ITOS)

Managing IT Processes

ITOS is the IT Department. It is the help desk that takes the call when a problem is found. It is the teams that coordinate changes and roll them out in the middle of the night. It is the planning and process that keep the systems going even in the event of a disaster.

Description

ITOS outlines all the necessary services an IT organization will have to support its business needs. This domain provides alignment of industry standards and best practices (PM BOK, CMMI, ISO/IEC 27002, COBIT, and ITIL v3), providing a reference from two main perspectives that enable the organization to support its business needs.

However, relationships between technology components are not intended to be a one-to-one match to the process touch points described in PM BOK, ISO/IEC 27002, CMMI, COBIT and ITIL v3.

Area Components	Definition
1 IT Operation	IT operation defines the organizational structure and skill requirements of an IT organization and a set of standard operational management procedures and practices to allow the organization to manage an IT operation and associated infrastructure. IT Operation capabilities are oriented to align the business and IT Strategies, management of the project and technological portfolios, and ensure architecture governance throughout IT.
2 DRP	The document defines the resources, actions, tasks, and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.
3 Plan Management	The overall process for assuring that the DRP is continuously updated to reflect changes in the business and its critical functions.
3 Test Management	The function that manages the overall process of periodic testing and subsequent review of the DRP.
2 IT Governance	This capability covers all processes and components oriented to establish decision rights and accountability framework to encourage desirable behavior in the life cycle for IT services.
3 Architecture Governance	Set of tools that can be used for developing a broad range of different architecture perspectives usually integrated as a common Architecture Framework. Elements that the governance process must cover are: • Describe a method for defining an information system in terms of a set of building blocks • Show how the building blocks fit together • Technical roadmap for the standards list • Contain a set of tools, and enforce a technology standards list • Provide a common vocabulary • Governance processes to ensure that existing solutions and new IT services are aligned with the framework.
3 Standards & Guidelines	This capability is a complement for the Architecture Governance, outlines all the technology standards, and guidelines regarding how they can be consumed across the organization. These standards should include alignment with the organization's strategy, industry standards, principles, patterns that can be reused across the organization, among other elements necessary to ensure consistent implementation and adoption.

2 Resource Management	Resource management deals with the accurate assignment of resources to IT service delivery functions. It is considered a sharable service, separate from project management since the same patterns can be applied to solve operational, production, and emergency resource allocations. Resource management includes technologies that assist in resource pooling, forecasting, and leveling. Other resource management functions are more strictly related to solutions for Human Resources management. This service does provide valuable input into the BOSS Domain for costing, forecasting, and planning activities.
3 Segregation of Duties	Separation of duties (SoD) is the concept of having more than one person required to complete a task to prevent fraud and error.
3 Contractors	All third-parties bound to a contract to provide a service for the organization are not considered employees but have access to various resources and data across the company. This capability is intended to manage these contractors and the associated processes to onboard and release them.
2 PMO	The Project Management Office (PMO) is the department or group that defines and maintains the standards of process, generally related to project management within the organization. The PMO strives to standardize and introduce economies of repetition in the execution of projects. The PMO is the source of documentation, guidance, and metrics on the practice of project management and execution. In some organizations, this is known as the Program Management Office.
3 Program Management	Program management deals with the incident after it has begun the cycle through the remediation process. Program management architecture interacts with the service desk. Program management offers advanced root cause analysis tools and technologies and interfaces with the information repositories to perform trending and prevention services within the environment.
3 Project Management	All processes, artifacts, and methodologies associated with the Project Management Office to track projects (best practices include PMI Body of Knowledge among others).
3 Remediation	This capability is focused on projects that are remediating existing gaps, or findings that affect the enterprise. A remediation dashboard is recommended to be used to track progress for senior management.
2 Portfolio Management	This container is focused on planning, tracking, prioritizing current and future projects and programs for the enterprise.

3 Maturity Model	Tracking the organization's capabilities against industry best practices, benchmarking, and maturity to show progress over time.
3 Roadmap	Strategic direction and plans for changes to capabilities and solutions within the technology portfolio (including the security roadmap) to accomplish a desired future state (e.g., continuous innovation, integration of capabilities, etc.). This process must be aligned with the business strategy).
3 Strategy Alignment	Process-oriented to understand the business needs and strategy and ensure that Information Technology and the Security and Risk Management strategies are aligned to support those objectives within the roadmap.
1 Service Delivery	Service Delivery deals with those technologies that are essential in maintaining uninterrupted technical services. Services in this category typically include those that are more appropriate to the technical staff, such as availability management, service level management, service continuity, and capacity management. However, although those categories alone are enough to satisfy ITIL service management guidelines, there are several other IT disciplines that are closely aligned with service support and delivery, such as project management and service provisioning. Service Delivery is primarily concerned with the proactive and forward-looking services that the business requires from Information Technology to provide adequate support to the business users. It is focused on the business as the customer of the IT services. The discipline consists of the following processes, explained in subsections below.
2 Service Level Management	The function responsible for assuring that the level of services provided is in agreement with contractual obligations on an ongoing basis.
3 Objectives	Measurable objectives for services and their delivery used in assessing performance versus a service level agreement
3 Internal SLAs	Service level agreements within an organization that codify the specific services to be delivered and the performance criteria governing that delivery.
3 OLAs	Operational Level Agreements must be defined to support a Service Level Agreement (SLA) between areas or organizations. This capability is oriented to track effective integration between processes associated with a specific SLA from the operational perspective.

3 External SLAs	Service Level Agreements with external entities that codify the specific services to be delivered and the performance criteria governing that delivery.
3 Vendor Management	This capability governs the process of managing vendor relationships, including selection, vetting, evaluation, security, and compliance. Usually, these processes also include risk evaluation and a rating against the type of data that the vendor can access, process, host or see (given their maturity on their risk profile, financial, among other areas), and type of connectivity.
3 Service Dashboard	All SLAs, OLAs, and contracts should have associated and defined Key Performance Indicators, Key Goal Indicators, and Key Risk Indicators that must be tracked periodically to manage these agreements. The service dashboard should present these metrics for decision making.
2 Information Technology Resiliency	The attributes of an information technology entity and its services to continue to provide adequate services when events occur (power interruption, loss of network links, etc.).
3 Availability Management	The overall process that manages the availability of services to their users (both internal and external).
3 Resiliency Analysis	The process that assesses the ability of an organization to continue to deliver services despite the occurrence of various events (e.g., loss of power, loss of network connectivity, etc.).
3 Capacity Planning	Capacity planning assures that resources and workloads are matched at both the present time and in the future.
2 Application Performance Monitoring	Provides alerting, incremental resource provisioning, etc., when application performance measurements (e.g., response time) exceed service level objectives
2 Asset Management	This container manages all the financial aspects of the Configuration Items and Services provided by the Information Technology organization.
3 Service Costing	The internal function that analyzes the overall costs accrued in delivering a particular service so that revenue (whether external or internal chargeback) is adequate to support the delivery of that service.
3 Operational Budgeting	The planning process used to determine day to day investments such as Maintenance of existing services and infrastructure, applications, among other associated elements that allow the organization to operate. Usually, the Chargeback process is used to distribute these costs across medium to large organizations.

3 Chargeback	This process manages the IT service consumption by an area or user across the organization, as well calculates the associated costs to those services including People, Technology and supporting materials. The process ensures that there is a clear understanding on the TCO and costs per service (i.e. Desktop support, Network services, Security Services, etc.).
3 Investment Budgeting	The planning process used to determine whether an organization's long term investments such as new infrastructure, replacement of existing services and infrastructure, new data centers, new products or services, research, application development, security, and project deployment are worth pursuing. Usually, a cost-benefit analysis is used as part of the investment budgeting process.
1 Service Support	Service Support is focused on the User of Information Technology services and is primarily concerned with ensuring that they have access to the appropriate services to support the business functions. To the business, customers, and users, this is the entry point for service requests. They get involved in service support by: • Asking for changes • Needing communication, updates • Having difficulties, queries. The service desk is the single contact point for the customers to record their problems. The service desk will try to resolve problems if there is a direct solution or will create an incident. Incidents initiate a chain of processes: Incident Management, Problem Management, Change Management, Release Management, and Configuration Management (see the following sections for details). This chain of processes is tracked using the Configuration Management Database (CMDB), which records each process, and creates output documents for traceability (Quality Management).

2 Configuration Management	Configuration management architecture could easily be thought of as the "backbone" of Service Delivery. The configuration management architecture provides base technology support for automated discovery of assets, license management, logical inventory, physical inventory, electronic software distribution, and software configuration. Configuration Management is heavily dependent upon an information architecture component known as the Configuration Management Database (CMDB), an ITIL term that is the point of truth for all configuration items. More important in terms of the CMDB than the repository for Configuration Items (CI's), is the notion of the technology relationship index, or technology metadata, that defines the relationships between each item. There are many to many logical relationships between CI's as diverse as physical contracts for support services to software applications.
3 Capacity Planning	The process for assuring that the capacity (CPU power, network bandwidth, etc.) to deliver a service is continuously in line with the demand for that service.
3 Software Management	The application of management activities-planning, coordinating, measuring, monitoring, controlling, and reporting-to ensure that the development and maintenance of software is systematic, disciplined, and quantified. This includes measurement at distinct points in time for the purpose of systematically controlling changes to the configuration and maintaining the integrity and traceability of the configuration throughout the system life cycle.
3 Physical Inventory	This process tracks all the physical components across the Information Technology organization. Also tracks the ownership and custody for these assets.
3 Automated Asset Discovery	This capability allows the Configuration Management process to identify new and changing assets across the infrastructure and maintains the existing inventory of Configuration Items. Usually a process must be in place to formalize ownership for these new assets.
3 Configuration Management	The process and procedures for managing the configuration of assets (servers, storage arrays, network equipment, etc.) to assure that their configuration as deployed matches that specified by policy, standards and guidelines.

2 Knowledge Management	Usually as incidents are resolved and the root cause analysis takes place, a significant amount of knowledge could be lost, causing delays as some of these incidents appear again throughout time. The Knowledge Management Process accumulates information regarding how incidents were resolved, or what are the fixes for root causes, once this knowledge is collected is transformed on Frequently Asked Questions or Self-Service Capabilities that the user and technical support communities can reuse to resolve issues with the IT services.
3 Best Practices	The process of developing and following a standard way of doing things that multiple organizations execute in an efficient manner, the process includes methods, techniques, or frameworks that consistently show results superior to those achieved with other means, and that is used as a benchmark. These practices can evolve to become better as improvements are discovered (using mechanisms such as lessons learned). This capability is intended to maintain quality as an alternative to mandatory legislated standards and can be based on self-assessment or benchmarking.
3 Trend Analysis	Analysis of requests for help regarding security in terms of consulting on projects, questions asked about policies, end-user training feedback, etc. to identify frequently asked questions and new areas of documentation required for the knowledge base.
3 Benchmarking	The process of identifying a leader in a given practice area and comparing the organization's practices against the leader and other organizations. This can help the organization to understand where they compare with other organizations in the industry with respect to knowledge, competency and capability.
3 Security Job Aids	As security standards and patterns are created across the organization, they should include guidelines and processes that can help employees comply with regulatory requirements or security standards in a consistent manner.
3 Security FAQ	One of the outcomes from the knowledge management process would be to establish a standard and consistent answer to questions that employees ask frequently. This process captures those questions associated with information security and compliance.

2 Change Management	Change is a major pattern that acts as an intermediary between request, release and configuration/provisioning. Change management allows for management of scope, impact analysis, as well as scheduling of change. Change management provides one of the primary inputs into configuration management from a data maintenance perspective to keep application data up to date.
3 Service Provisioning	The process of implementing a new configuration item or changes to an existing configuration item.
3 Approval Workflow	The process of reviewing requested changes to ensure their appropriateness and receive authorization to continue from the necessary reviewers.
3 Change Review Board	A cross-functional team charged with ensuring that all changes to the environment are carefully considered and reviewed to minimize impact to users and existing services.
3 Planned Changes	Planned changes are changes that are identified well in advance of their needed implementation. These changes are carefully thought through and fully documented.
4 Project Changes	A type of planned change resulting from a project. Project changes occur due to implementation or changes to business requirements.
4 Operational Changes	A type of planned change resulting from ongoing maintenance activities of existing services.
3 Emergency Changes	Changes generated to fix an issue on a production service or application.
2 Incident Management	Architectural patterns for incident management include services for trouble ticketing and incident classification. Incident Management interacts with other areas of the architecture either directly (as with the service desk), indirectly (through manipulation of common data) or asynchronously (as part of a business process for incident management). Incidents begin their lives either as a phone incident from a human, a detected error in the environment (usually as a result of event correlation from the Systems Management domain) or via incident messaging from another application.
3 Security Incident Response	The process and procedures for responding to a declared security incident.
3 Automated Ticketing	The capability of having system generated events automatically spawn incidents.
3 Self-Service	This capability allows anyone in the organization to report an incident and begin the incident management process.

3 Ticketing	The process of creating a record of incidents that can be tracked through their lifecycle. These incidents should be referenced by a unique identifier.
3 Cross Cloud Security Incident Response	Because of the ubiquitous nature of cloud computing, a security incident may be detected in or affect several cloud instances. The incident response plan must include processes and procedures for handling trans-cloud security incidents.
2 Problem Management	The objective of problem management is to minimize the impact of problems on the organization by analyzing them to prevent their recurrence.
3 Event Classification	An event may or may not indicate that an incident has occurred or is in progress. Event classification provides processes for analysis and event correlation to provide an assessment and confidence estimate for the occurrence of an incident.
3 Root Cause Analysis	An important component of incident response that looks beyond the face details of an incident to determine the root cause of the incident (e.g., a missing patch might enable a successful intrusion but root cause analysis might reveal that the vulnerable service should never have been running anyway).
3 Trend Analysis	As part of the Root Cause Analysis, this capability will allow the organization to identify the effects and tendencies that certain incidents or root causes will have across the Information Technology Services. All of these trends should be tracked throughout time. Also can be an ongoing process for assessing the overall trend of usage of a resource, occurrences of an event, etc.
3 Problem Resolution	The process of identifying the appropriate changes to configuration items and/or processes necessary to address the root cause of a problem to minimize the likelihood of recurrence.
3 Orphan Incident Management	Identification of incidents that do not have a current owner, so that appropriate resources can be engaged to resolve the problems.

2 Release Management	The release management architecture is the set of conceptual patterns that support the movement of pre-production technical resources into production. Pre-production includes all the activities that are necessary to prove that a particular resource is appropriate for the technical, business, and operational environment and does not exceed a risk profile for a particular task. Significant release management patterns include those for release scheduling, release acceptance, and audit. Release management plays a vital role both as a process and as a set of technologies and it provides a vital control point for request, change, and configuration management processes and architectures.
3 Scheduling	As part of release management, a detailed schedule of releases and their features should be developed to bundle many change requests into a single change calendar.
3 Testing	The process of testing all changes associated with a release to ensure they meet the requirements and will not disrupt existing services. This is a Quality Assurance function coordinated through Release Management.
3 Build	The process of compiling source code and configurations into one or more deployable units to be handed off to the change management process.
3 Version Control	The process of tracking all changes to source code, configuration items, and documentation and assigning these changes a version identifier.
3 Source Code Management	A form of version control for source code that allows for versioning of software, branching software into different releases, and controlling access to software.

Example

An employee receives a suspicious email, which she thinks may contain a malware program. She notifies the help desk. The help desk opens a security incident, and a response team works to block the sender, identify other affected users, and restore any damage that may have been done.

Services Provided

IT Operation: IT Operation defines the organizational structure, skill requirements of an IT organization, and standard operational management procedures and practices to allow the organization to manage an IT operation and associated infrastructure.

IT Operation capabilities are oriented to align the business and IT strategies. The management of the project and technological portfolios ensure architecture governance throughout IT.

Associated Components:

- 2 DRP
- 3 Plan Management
- 3 Test Management
- 2 IT Governance
- 3 Architecture Governance
- 3 Standards & Guidelines
- 2 Resource Management
- 3 Segregation of Duties
- 3 Contractors
- 2 PMO
- 3 Program Management
- 3 Project Management
- 3 Remediation
- 2 Portfolio Management
- 3 Maturity Model
- 3 Roadmap
- 3 Strategy Alignment

Service Delivery: Service Delivery deals with technologies essential in maintaining uninterrupted technical services. Services in this category typically include those that are more appropriate to the technical staff, such as availability management, service level management, service continuity, and capacity management.

Although those categories alone are enough to satisfy ITIL service management guidelines, several other IT disciplines are closely aligned with service support and delivery, such as project management, service provisioning, and portfolio management.

Service Delivery is primarily concerned with the proactive and forward-looking services that the business requires from Information Technology to provide adequate support to the business users. It is focused on the business as the customer of the IT services.

Associated Components:

- 2 Service Level Management
- 3 Objectives
- 3 Internal SLAs
- 3 OLAs
- 3 External SLAs
- 3 Vendor Management
- 3 Service Dashboard
- 2 Information Technology Resiliency

- 3 Availability Management
- 3 Resiliency Analysis
- 3 Capacity Planning
- 2 Application Performance Monitoring
- 2 Asset Management
- 3 Service Costing
- 3 Operational Budgeting
- 3 Chargeback
- 3 Investment Budgeting

Service Support: Service Support is focused on the users and is primarily concerned with ensuring they have access to the appropriate services to support the business functions.

To the business customers and users, Service Support is the entry point for service requests. Users become involved in service support by:

- Asking for changes
- Needing communication, updates
- Having difficulties, queries

The service desk is the single contact point for customers to record their problems. The service desk will try to resolve issues if there is a direct solution or create an incident. Incidents initiate a chain of processes: Incident Management, Problem Management, Change Management, Release Management, and Configuration Management (see the following sections for details). This chain of processes is tracked using the Configuration Management Database (CMDB), which records each process and creates output documents for traceability (Quality Management).

Associated Components:

- 2 Configuration Management
- 3 Capacity Planning
- 3 Software Management
- 3 Physical Inventory
- 3 Automated Asset Discovery
- 3 Configuration Management

Incident Management: Architectural patterns for incident management include services for trouble ticketing and incident classification. Incident Management interacts with other areas of the architecture either directly (as with the service desk), indirectly (through manipulation of common data), or asynchronously (as part of a business process for incident management). Incidents begin their lives either as a phone-in incident from a human, a detected error in the environment (usually due to event correlation from the Systems Management domain) or via incident messaging from another application.

Associated Components:

- 3 Security Incident Response
- 3 Automated Ticketing
- 3 Self-Service
- 3 Ticketing
- 3 Cross Cloud Security Incident Response

Problem Management: Problem Management deals with the incident after it has started to cycle through the remediation process. Problem Management architecture interacts with the service desk. Problem Management offers advanced root cause analysis tools and technologies, and interfaces with the information repositories to perform trending and prevention services within the environment.

Associated Components:

- 3 Event Classification
- 3 Root Cause Analysis
- 3 Trend Analysis
- 3 Problem Resolution
- 3 Orphan Incident Management

Knowledge Management: Usually, as incidents are resolved, and the root cause analysis occurs, a significant amount of knowledge could be lost, causing delays as some of these incidents appear again throughout time.

The Knowledge Management Process accumulates root cause solutions or information regarding how incidents were resolved. Once this knowledge is collected, it is transformed into frequently Asked Questions or Self-Service Capabilities that the user and technical support communities can reuse to resolve IT services issues.

Associated Components:

- 3 Best Practices
- 3 Trend Analysis
- 3 Benchmarking
- 3 Security Job Aids
- 3 Security FAQ

Change Management: Change Management is a significant pattern that acts as an intermediary between request, release, and configuration/provisioning. It allows for management of scope, impact analysis, as well as scheduling of change. Change Management provides one of the primary inputs into configuration management from a data maintenance perspective to keep application data up-to-date.

Associated Components:

- 3 Service Provisioning
- 3 Approval Workflow
- 3 Change Review Board
- 3 Planned Changes
- 4 Project Changes
- 4 Operational Changes
- 3 Emergency Changes

Release Management: The Release Management architecture is the set of conceptual patterns that support the movement of pre-production technical resources into production. Pre-production includes all the activities that are necessary to prove that a particular resource is appropriate for the technical, business, and operational environment and does not exceed a risk profile for a particular task. Significant Release Management patterns include those for release scheduling, release acceptance, and audit. Release Management plays a vital role both as a process and as a set of technologies, and it provides a vital control point for request, change, and configuration management processes and architectures.

Associated Components:

- 3 Scheduling
- 3 Testing
- 3 Build
- 3 Version Control
- 3 Source Code Management

Relationships to other Domains

The use of the ITOS analytic services such as data warehousing, data marts, and common operational data stores are key to enable an effective business operation service.

- ITOS supports the Business Operation Support Service, to maintain tactical and strategic alignment between the business and IT.
- ITOS implements Presentation, Application, Information, and Infrastructure services.

Technology Solution Services (TSS)

Description

IT solutions can be thought of as a technology stack: at the top level are the actual interactions that the users have with the stack, with applications that accept the interactions and push data down where it may be manipulated, followed by the data that runs on them, with the computers and networks at the bottom layer. The four technology solution domains (Presentation Services, Application Services, Information Services, and Infrastructure Services) are based on the standard multi-tier architecture used to build these solutions.

Presentation Services

Interaction with the user

Presentation is the website you see when you go to an online bank. It is the voice on the phone when you call the airline reservation system or the mobile platform when you order remotely.

Description

The Presentation Services domain is where the end-user interacts with an IT solution. The security requirements for the Presentation Domain will vary on the type of user and the type of service being provided. For instance, a Business-to-Consumer (B2C) website will have different security concerns than a social media website. The security requirements will also vary based on the types of endpoints being used by the end-user.

Presentation Services Components	Definition
1 Presentation Modality	The Presentation Modality Services focus on the security concerns that differ based on user and service type. The two major types are Consumer Service Platforms like Social Media, Collaboration, Search, Email and e-Readers, and Enterprise Service Platforms like Business-to-Consumer (B2C), Business-to-Employee(B2E), Business-to-Business (B2B), etc.
2 Consumer Service Platform	This container holds the various types of presentation modalities that are consumer-oriented as opposed to enterprise-oriented.
3 Social Media	A presentation modality links users together to exchange messages, photos, etc. to network and communicate one-on-one or in groups.
3 Collaboration	A presentation modality geared towards joint efforts on a combined effort such as a project or a document. Collaboration applications share files, allow multiple editors of documents, and often provide calendars, task tracking, and messaging for its participants.
3 Search	A presentation modality that allows users to query a single site or multiple sites for content related to the terms in the query. This modality is often used as an initial form of navigation across the internet or within the site.
3 E-Readers	A presentation modality that simulates the reading of a book or other printed material.

3 E-mail	A presentation modality that presents an in-box of messages and allows users to send new messages or organize old messages into folders. Often email is combined with calendar functions and contact management functions.
2 Enterprise Service Platform	This container holds the various types of presentation modalities oriented to enterprise users in the workplace, or towards customers and partners of an enterprise.
3 B2E	Business-to-Employee (B2E) applications allow employees of an enterprise to transact the business of the company.
3 B2M	Business-to-Mobile (B2M) applications utilize a mobile device such as a smartphone to enable customers or employees to interact with a business's systems from anywhere at any time.
3 B2B	Business-to-Business (B2B) applications allow enterprises to exchange common transactions in bulk, for example purchase orders, invoices, etc.
3 B2C	Business-to-Consumer (B2C) applications are the online presence of an enterprise that allow it's customers to conduct business with the enterprise over the internet.
3 P2P	Peer-to-Peer (P2P) applications allow users within an enterprise to connect directly to each other to exchange instant messages or files.
1 Presentation Platform	The Presentation Platform Services focus on the different types of Endpoints that end-users utilize to interact with a solution such as Desktops, Mobile Devices (smartphones, tablets), Portable Devices (laptops), or special purposes devices such as medical devices or smart appliances. The presentation platform also includes different interaction technologies such as Speech Recognition or Handwriting Recognition that could be used to interact with a solution.
2 Endpoints	Endpoints are the devices that users interact with when using an IT solution. They are called Endpoints because they are at the edge of the solution where technology meets humans.
3 Mobile Devices	Mobile devices include smartphones, PDAs and tablets.
4 Mobile Device Management	Mobile device management enables an enterprise to manage mobile endpoints' security similar to the way that desktops are managed. The security features include locking or wiping the device if compromised, pushing software updates to the device, and requiring certain security features to be enabled before allowing a device to connect to the corporate network.

3 Portable Devices	Class of devices such as laptops full-featured or nearly full-featured computers with the same operating systems that desktop (fixed) devices have.
3 Fixed Devices	devices that are not easily movable and are designed to be used from only one location.
3 Medical Devices	Medical devices in the context of this architecture mean devices with connectivity to networks or the ability to download data so that information can be exchanged with the device, such as a monitoring device, worn by a patient.
3 Desktops	Desktops are the classic computer that typically sits on or under a desktop and includes a CPU, monitor, keyboard, mouse, and other peripheral devices.
4 Company Owned	Devices purchased, owned, and managed by the enterprise and given out to employees or perhaps rented by customers.
4 Third-Party	Third-party devices are owned by one business and provided for use by another business.
4 Public Kiosk	Public Kiosks are devices, often PCs, that are used by multiple people in a shared space.
3 Smart Appliances	Devices whose primary purpose is not computation, but include connectivity to a network to provide real-time updates on their status or to be controlled remotely.
3 Secure Sandbox	An isolated environment that provides abstraction of trust concerns between custom or third party code and the underlying system. Allows applications to run in a context that does not affect each other or the host operating system and allows the enterprise to have an area with managed security controls for applications with sensitive data.
1 Speech Recognition (IVR)	Speech recognition can translate the spoken word into computer input. Interactive Voice Response (IVR) systems provide a menu of choices that a person can respond to to interact with a system.
1 Handwriting (ICR)	Handwriting, or interactive character recognition (ICR) can translate handwritten text into computer input.

Example

A mobile device provides the risk of locally-stored data being lost with the device, and a shared public kiosk provides the risk of subsequent end-users having access to prior users' data.

Services Provided

Presentation Modality: The Presentation Modality Services focus on the security concerns that differ based on user and type of service. The two major types are consumer service platforms like Social Media, Collaboration, Search, Email, e-Readers, and Enterprise Service Platforms like Business-to-Consumer (B2C), Business-to-Employee (B2E), Business-to-Business (B2B), and more.

Associated Components:

- 2 Consumer Service Platform
- 3 Social Media
- 3 Collaboration
- 3 Search
- 3 E-Readers
- 3 E-mail
- 2 Enterprise Service Platform
- 3 B2E
- 3 B2M
- 3 B2B
- 3 B2C
- 3 P2P

Presentation Platform: The Presentation Platform Services focus on the different types of Endpoints that end-users utilize to interact with a solution such as desktops, mobile devices (smartphones, tablets), portable devices (laptops), or special purposes devices such as medical devices or smart appliances. The presentation platform also includes different interaction technologies such as Speech Recognition or Handwriting Recognition that could be used to interact with a solution.

Associated Components:

- 2 Endpoints
- 3 Mobile Devices
- 4 Mobile Device Management
- 3 Portable Devices
- 3 Fixed Devices
- 3 Medical Devices
- 3 Desktops
- 4 Company Owned
- 4 Third-Party
- 4 Public Kiosk
- 3 Smart Appliances
- 3 Secure Sandbox
- 1 Speech Recognition (IVR)
- 1 Handwriting (ICR)

Relationships to other Domains

Presentation Services utilizes the Security and Risk Management domain to authenticate and authorize the end-user, to protect the data on the Endpoint device and in-transit to the Application Services domain, and to protect the Endpoint device itself from tampering, theft, and malware. The Information Technology Operation and Support domain supplies services to deploy and make changes to the endpoints and to manage problems and incidents that the end users experience. The Business Operation Support Services provides security monitoring of the Endpoints, Human Resources (HR), and Compliance policies for end-user usage of IT solutions.

Application Services

Development and implementation of business logic

Think of application services as the processes that developers use to write code, as well as the code itself.

Description

Application services are the rules and processes behind the user interface that manipulate the data and perform transactions for the user. In an online bank, this might be a bill payment transaction that deducts the payment amount from the user's account and sends a check to the payee. In addition to the application services of an IT solution, the Application Services domain also represents the development processes that programmers go through when creating applications.

Application Services Components	Definition
1 Programming Interfaces	[Application] Programming Interfaces (APIs) allow applications or services to talk to another or allow pieces of an application to talk to each other. Input validation is important for these interfaces to make sure that only the expected input is being provided. Lack of this validation can create vulnerabilities by allowing attackers to inject malicious code into the application or retrieve more data than they are supposed to access.
2 Input Validation	Input validation examines the user's input and determines what input is acceptable input to the system. This process helps with data quality as well as allows malicious input from being injected into the system.
1 Security Knowledge Life Cycle	To build secure applications, a development team must keep up to date with the latest threats and appropriate countermeasures in their development process. A security framework is often used to provide reusable components when a development team is building multiple applications.

2 Security Design Patterns	Design Patterns are blueprints and instructions for solving commonly occurring technical challenges. Security Design Patterns focus on designs of security capabilities such as authentication, authorization, log monitoring, single sign-on, etc.
2 Security Application Framework	Application frameworks provide a set of components that act as the fundamental starting point of an application. Frameworks enable application developers to reuse standard components across multiple applications and focus their efforts on the specific business needs of the applications. Security Application Frameworks provide security components that extend a specific application framework. For example, the ACEGI security framework became an official part of the Spring Framework for building web applications with Java.
2 Code Samples	Code samples provide snippets of code that demonstrate to programmers how to code a specific algorithm. For secure coding purposes, examples could include writing a database query that is not susceptible to SQL injection.
2 Attack Patterns	Attack Patterns are descriptions of common attacks used by malicious parties that programmers must be aware of to defend against. For instance, the Open Web Application Security Project (OWASP) Top 10 Security Risks describes the top 10 attack patterns used to exploit web applications.
1 Integration Middleware	Integration Middleware is a set of tools like service buses and message queues that allow applications to exchange information without talking directly. Security concerns for these services include making sure the messages being exchanged are not read or tampered with during delivery, and reliable sources are only sending them.
1 Development Process	The Development Process must address security concerns while the solution is being built using tools like source code scanners that can locate common security flaws in the code and web application vulnerability scanners that can test if a web application can be manipulated with common techniques used by hackers.
2 Self-Service	Self-Service capabilities are available for development teams to leverage independently without handing off work to another team
3 Security Code Review	Security code review capabilities from a self-service point of view refers to the ability to use a source code analyzer tool to read the source code of a program and identify areas of the code vulnerable to well-known attack patterns.

3 Application Vulnerability Scanning	Application vulnerability scanning is an automated capability that will examine the running application and identify areas where weaknesses exist that can be exploited.
3 Stress & Volume Testing	Performance and capacity tests seek to determine the workload level at which a service level objective is violated or the maximum workload that can be supported without violating a service level objective, respectively.
2 Software Quality Assurance	Software Quality Assurance is the process of testing software and tracking the defects found. Applications should be tested for security vulnerabilities as part of the software quality assurance process.
1 Connectivity & Delivery	Connectivity & Delivery services are the underlying mechanisms that Integration Middleware uses to move the messages between applications. These services must also protect the messages being delivered, including encrypting the messages to hide their contents.
1 Abstraction	When multiple applications do the same thing, they often use the concept of abstraction so that they have a common language that others will understand. While airlines may manage their flights differently than others, they both may use the same abstraction so that online travel services can find the flights across multiple airlines. These abstractions must include the proper security mechanisms to ensure that only authorized users are accessing them and that one user cannot access the information of another without permission.

Example

A developer is writing an Application Program Interface (API) that allows a banking system to exchange transactions with other banks. He scans the code with a source code analyzer that identifies a section of code that was not protected against invalid input that could corrupt the system. The change is made immediately, and the new API is now safe to use.

Services Provided

Development Process: The Development Process must address security concerns while the solution is being built using tools like source code scanners that can locate common security flaws in the code and web application vulnerability scanners that can test if a web application can be manipulated with common techniques used by hackers.

Associated Components:

- 2 Self-Service
- 3 Security Code Review
- 3 Application Vulnerability Scanning
- 3 Stress & Volume Testing
- 2 Software Quality Assurance

Security Knowledge Lifecycle: To build secure applications, a development team must keep up-to-date with the latest threats and appropriate countermeasures to use in development processes. A security framework is often used to provide reusable components when a development team is building multiple applications.

Associated Components:

- 2 Security Design Patterns
- 2 Security Application Framework
- 2 Code Samples
- 2 Attack Patterns

Programming Interfaces: Programming Interfaces allow one application to talk to another or let pieces of an application to talk to each other. Input validation is vital for these interfaces to make sure that only the expected input is being provided. Lack of this validation can create vulnerabilities by allowing attackers to inject malicious code into the application or to retrieve more data than they are supposed to have access to.

Associated Components:

- 2 Input Validation

Integration Middleware: Integration Middleware is a tool like service buses and message queues that allow applications to exchange information without talking directly to each other. Security concerns for these services include making sure the messages being exchanged are not read or tampered with during delivery and that reliable sources are only sending them.

Connectivity & Delivery: Connectivity & Delivery services are the underlying mechanisms that Integration Middleware uses to move the messages between applications. These services must also protect the messages being delivered, including encrypting the messages to hide their content.

Abstraction: When multiple applications do the same thing, they often use the concept of abstraction so that they have a common language others will understand. While airlines may manage their flights differently from each other, they all may use the same abstraction so that online travel services can find the flights across multiple airlines. These abstractions must include the proper security mechanisms to ensure that only authorized users are accessing them and that one user cannot access the information of another without permission.

Relationships to other Domains

Application Services rely on the Security and Risk Management domain to encrypt messages sent between applications and to authenticate and authorize applications to talk to each other. The development process of the Application Services domain relies on the threat and vulnerability management services of SRM to assess the security of the solution being developed. Application Services typically receives input from the Presentation Services domain and manipulates data in the Information Services domain. Application Services also require servers and network services from the Infrastructure Services domain. The Information Technology Operations and Support domain is used to manage changes to the Application Services. The Business Operations Support Services domain provides security monitoring services enabling administrators to monitor application activities for any statistically unusual behavior.

Information Services

Managing Data

Information Services refers to the storage of data, usually in databases, but sometimes just in files.

Description

One of the most common pain points across organizations is the amount of data generated across the company, sometimes including redundant data (different perspectives for the same threat or gap). All this data needs to be transformed into useful information that business asset owners can use to prioritize, strategize, and manage the risk portfolio they own.

This section manages the extraction, transformation, cleansing, and loading of information into a common data model either for analytical or operational goals.

Typical Extract, Transform, and Load (ETL) data normalization, data mining, balance scorecard, among other capabilities, will reside here.

This domain simplifies all these sources of data by having a data management approach. All data containers are allocated on this domain, where eventually they can be extracted, transformed, and loaded into the following:

- **Operational data store:** All day-to-day and transactional information will be allocated here, using a 360 degrees perspective around information assets (i.e., application and infrastructure vulnerabilities, patching gaps, penetration test results, audit findings, and controls per asset).
- **Data Warehouse:** All historical transactions will be used to develop a data warehouse or data mart that can measure the success obtained with the risk management program. Also, this model can be used to identify behavior patterns, trends, tendencies, and systemic gaps across the organization.

Information Services Components	Definition
1 Service Delivery	The Service Delivery discipline concentrates on the Information and Communication Technology (ICT) proactive services to provide adequate support to business users. It focuses on the business as the customer of the ICT services.
2 Service Catalog	Service Catalog is a list of services that an organization provides, often to its employees or customers. Each service within the catalog typically includes: Service Description, Timeframes or service level agreement for fulfilling the service, Who is entitled to request/view the service, Service Costs (if any) and how to fulfill the service.
2 SLAs	A Service-Level Agreement (SLA) is a negotiated agreement between two parties, where one is the customer (or end-user), and the other is the service provider. This can be a legally binding formal or an informal 'contract' (for example, internal department relationships). The SLA records a common understanding about services, priorities, responsibilities, guarantees, and warranties. The SLA may specify the levels of availability, serviceability, performance, operation, or other attributes of the service, such as billing. The 'level of service' can also be specified as 'target' and 'minimum,' which allows customers to be informed what to expect (the minimum) while providing a measurable (average) target value that shows the level of organization performance. In some contracts, penalties may be agreed upon in the case of non-compliance with the SLA (but see 'internal' customers below). It is important to note that the 'agreement' relates to the services the customer receives, and not how the service provider delivers that service. SLAs commonly include segments to address: a definition of services, performance measurement, problem management, customer duties, warranties, disaster recovery and termination of the agreement.
2 OLAs	An operational-level agreement (OLA) defines the interdependent relationships among the internal support groups of an organization working to support a service-level agreement (SLA). The agreement describes each internal support group's responsibilities toward other support groups, including the process and timeframe for delivery of their services. The OLA's objective is to present a clear, concise, and measurable description of the service provider's internal support relationships.

2 Contracts	Contracts between an enterprise and its service providers designate the responsibilities of each party and the penalties associated when service level agreements are not met.
2 Recovery Plans	Recovery plans describe the processes and procedures required to restore service delivery after interruption or disaster. The plans will often include steps to gradually restore the service while monitoring the performance and system health of every reached milestone.
1 Reporting Services	Reporting services provide the ability to present data in various ways going from a top-level aggregated dashboard, drilling down to raw data. Reporting services also offer the ability to mine and analyze data and provide business intelligence to decision-makers
2 Dashboard	The dashboard provides a top-level view of various aspects of the information services. The dashboard usually includes aggregated Key Performance Indicators (KPIs) and Key Quality Indicators (KQIs).
2 Data Mining	Data mining is the ability to drill-down on KPIs and KQIs in order to find the underlying root cause for the indicators' results. The actual data mining task can be an automatic or semi-automatic analysis of large quantities of data to extract previously unknown interesting patterns such as groups of data records (cluster analysis), unusual records (anomaly detection), and dependencies (association rule mining). These patterns can then be seen as a kind of summary of the input data and used in further analysis or, for example, in machine learning and predictive analytics. For example, the data mining step might identify multiple groups in the data, which can then be used to obtain more accurate prediction results by a decision support system.
2 Business Intelligence	Business intelligence refers to techniques used in identifying, extracting and analyzing business data. BI technologies provide historical, current and predictive views of business operations.
2 Reporting Tools	Reporting tools provide end-users with the ability to generate reports, share reports with other users, and analyze the information domain's data.
1 ITOS	Information Technology Operations & Support (ITOS)
2 PMO	The Project Management Office (PMO) is the department or group that defines and maintains the process's standards, generally related to project management within the organization. The PMO strives to standardize and introduce economies of repetition in the execution of projects. The PMO is the source of documentation, guidance, and metrics on the practice of project management and execution.

2 Strategy	The strategy information within ITOS represents the business and technology trends affecting the enterprise, gap analysis of current capabilities against desired capabilities, and the investments required to fill the gaps.
2 Roadmap	The roadmap information within ITOS represents the planned changes to the capabilities of the organization over time.
2 Problem Management	Process of managing recurring incidents as problems to find and fix root causes to prevent future events from recurring.
2 Incident Management	Process for managing an incident from detection through review and resolution.
2 CMDB	A configuration management database (CMDB) is a repository of information related to an information system's components. It contains the details of the configuration items (CI) in the IT infrastructure. A CMDB helps an organization understand the relationships between these components and track their configuration. The CMDB records CIs and details about the important attributes and relationships between CIs. Configuration managers usually describe CIs using three configurable attributes: Technical, Ownership, Relationship
2 Knowledge Management	The process of organizing information and providing search capabilities such that problems and incidents can be handled quickly by referring to experience. In the Information domain, this represents the actual knowledge stored in the knowledge base regarding security FAQs, best practices, and job aids.
2 Service Management	Service management is a discipline for managing information technology (IT) systems, philosophically centered on the customer's perspective of IT's contribution to the business.
2 Change Management	The process of managing the life cycle of changes in the IT environment.
1 Service Support	This container groups together the information sources coming from Information Technology Operation & Support - Service Support capabilities.
2 Configuration Rules (Metadata)	This metadata contains the configuration rules for how to deploy configuration changes to specific configuration items.
2 Service Events	Information regarding services provided in support of IT operations could include deployments, changes, and maintenance events. Events can be based on key performance indicators crossing a threshold, network alarms, device metrics.

2 Configuration Management Database (CMDB)	A configuration management database (CMDB) is a repository of information related to all the components of an information system. It contains the details of the configuration items (CI) in the IT infrastructure. A CMDB helps an organization understand the relationships between these components and track their configuration. The CMDB records CIs and details about the important attributes and relationships between CIs. Configuration managers usually describe CIs using three configurable attributes: Technical, Ownership, Relationship
2 Knowledge Repository	The Knowledge Repository contains information about known patterns, processes, and procedures
2 Change Logs	From a security standpoint, monitoring the change logs and comparing it to configuration management changes could detect an unauthorized change in the environment.
1 Data Governance	Data governance embodies a convergence of data quality, data management, data policies, business process management, and risk management surrounding data handling in an organization.
2 Risk Assessments	Risk Assessments measure the maturity of the organization's controls from a reference framework perspective (i.e., COBIT, ISO27001), regulatory perspective (i.e., SOX, PCI).
2 Non-Production Data	For testing and development purposes in non-production environments, test data should be generated to not host live data in environments with fewer controls. When live data must be used, it should be masked or tokenized to de-identify the personal information it contains.
2 Information Leakage Metadata	Metadata that is attached to critical pieces of information to mark it for detection by data leakage prevention tools.
2 Data Segregation	Data segregation is the process and controls that ensure data is segregated in a multi-tenant environment, so each tenant has access to his and only his data
1 BOSS	Business Operation Support Services (BOSS).
2 Risk Assessments	Risk Assessments measure the maturity of the organization's controls from a reference framework perspective (i.e., COBIT, ISO27001), regulatory perspective (i.e., SOX, PCI).
2 Data Classification	The process to describe data's business value to separate it into categories such as public, private, secret, to guide data handling procedures.

2 Process Ownership	Documentation regarding the business processes and the responsible parties for oversight and operations of those processes.
2 Audit Findings	Documentation regarding the specific gaps in an organization's controls discovered through an audit process.
2 HR Data (Employees & Contractors)	Information regarding the employees and contractors of an organization that can be used for various processes including access control, business continuity planning, data governance, and background checks.
2 Business Strategy	Documentation of the business goals and objectives that can be used to determine the information technology and security strategies in support of the business.
1 Risk Management	Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events.

2 GRC	Governance, Risk and Compliance (GRC) describes the overall management approach through which senior executives direct and control the entire organization, using management information and hierarchical management control structures. Governance activities ensure that critical information reaching the executive team is sufficiently complete, accurate, and timely to enable appropriate management decision making and provide the control mechanisms to ensure that strategies, directions, and instructions from management are carried out systematically and effectively. Risk management is the set of processes through which management identifies, analyzes, and, where necessary, responds appropriately to risks that might adversely affect realization of the organization's business objectives. The response to risks typically depends on their perceived gravity, and involves controlling, avoiding, accepting or transferring them to a third party. Whereas organizations routinely manage a wide range of risks (e.g. technological risks, commercial/financial risks, information security risks etc.), external legal and regulatory compliance risks are arguably the key issue in GRC. Compliance means conforming with stated requirements. At an organizational level, it is achieved through management processes which identify the applicable requirements (defined for example in laws, regulations, contracts, strategies and policies), assess the state of compliance, assess the risks and potential costs of non-compliance against the projected expenses to achieve compliance, and hence prioritize, fund and initiate any corrective actions deemed necessary.
2 RA	Documentation of the scope and results of Risk Assessments (RA).
2 BIA	Business Impact Assessment (BIA) information regarding the consequences to the organization if a business process and/or its data was unavailable, lost, or stolen.
2 DR & BC Plans	Documentation of Disaster Recover (DR) Plans to restore IT operations and Business Continuity (BC) Plans to ensure continuous service by the enterprise during planned or unplanned outages.
2 VRA	Documentation regarding risk assessments of 3rd party vendors used by the organization.
2 TVM (Threat Vulnerability Management)	Information regarding threats, vulnerability management testing, penetration testing, and compliance testing.

1 User Directory Services	User directory service is the system that stores, organizes, and provides access to information about users in a directory. The directory allows the lookup of values given a user ID where the ID may be associated with multiple, different types of data.
2 Active Directory Services	Active Directory Service serves as a central location for network administration and security. The AD is responsible for authenticating and authorizing all users and computers within a Windows domain network, assigning and enforcing security policies within all computers in a network, and installing or updating software on network computers.
2 Registry Services	Registry services catalog services available within the IT infrastructure and the metadata around how they should be accessed.
2 LDAP Repositories	Lightweight Directory Access Protocol (LDAP) Repositories organize users and groups of users into a hierarchical organizational structure.
2 Location Services	Geolocation information regarding the physical location of assets, resources, facilities, people.
2 X.500 Repositories	X.500 Repositories store hierarchical organization of entries according to the X.500 series of computer networking standards for electronic directory services.
2 Federated Services	Information regarding the trust between an organization's directories and 3rd party directories.
2 DBMS Repositories	Database Management Systems used to store user accounts and their data as tables within a database.
2 Virtual Directory Services	Virtual Directory Services aggregate multiple directories into a consolidated view which looks to the consumer application as a single directory.
2 Meta Directory Services	Provides for the flow of one or more directory services and databases to import or maintain synchronization of those data sources.
1 Security Monitoring	This container groups together the information sources coming from the BOSS - Security Monitoring Services.
2 Session Events	Events indicating the beginning and ending of a user interaction with a computing resource.
2 Authorization Events	Events indicating policy decision outcomes about a given subject access to a given object.

2 Authentication Events	Events indicating a successful or unsuccessful attempt to verify the identity of a user.
2 Application Events	Specific events within an application may be deemed useful for security monitoring, such as access to protected data or execution of transactions subject to fraud.
2 Network Events	Events generated by various network elements within the infrastructure including network health, KPIs, and threshold alarms.
2 Computer Events	Events generated by servers, desktops and other Endpoint devices including start ups, shutdowns, configuration changes, and system errors.
2 Privilege Usage Events	Events indicating administrative changes made to the system which could impact confidentiality, availability, or integrity of the system.
2 eDiscovery Events	Electronic Discovery (eDiscovery) Events regarding retention of data for legal hold and investigation purposes.
2 DLP Events	Data Leakage Prevention (DLP) events are triggered whenever privileged data is intercepted on its way out of the organization.
2 NIPS Events	Network Intrusion Prevention Services (NIPS) events regarding the source and destination of the intrusion attempt.
2 Compliance Monitoring	Information comparing the current configuration against the expected baseline configuration.
2 CRLs	A certificate revocation list (CRL) is a list of certificates that have been revoked, and therefore should not be relied upon.
2 ACLs	Access Control Lists (ACLs) indicate the permissions that subjects are granted regarding accessing or changing the objects within a system.
2 Database Events	Events regarding activity within the database management systems including logins, transactions, and administrative changes.
2 HIDS-HIPS	Host Intrusion Detection Systems (HIDS) can detect actions that attempt to compromise the confidentiality, integrity, or availability of a resource. Host Intrusion Prevention Systems (HIPS) includes taking a preventive measure without direct human intervention.
3 Transformation Services	Translation and normalization services for the security monitoring events in order to do data mining and event correlation.

Example

When an administrator creates a user account, the ID and Password are stored in a user directory. When that user logs into the system, a log entry showing the date and time of that log-in is stored in the security-monitoring database.

Services Provided

User Directory Services: All authentication and authorization repositories will be allocated in this section, to simplify the technology footprint for user directories.

Associated Components:

- 2 Active Directory Services
- 2 Registry Services
- 2 LDAP Repositories
- 2 Location Services
- 2 X.500 Repositories
- 2 Federated Services
- 2 DBMS Repositories
- 2 Virtual Directory Services
- 2 Meta Directory Services

Security Monitoring Data Management: All data related to Security Monitoring will be allocated here, considering the following main groups:

External monitoring: brand protection, honey-pots, web crawling prevention, and cyber intelligence.

Internal monitoring: SIEM related data, trends, behavior patterns, and forensic information.

Executive reporting: balance scorecard, executive dashboard, and ODS (risk registry).

Threat and vulnerability management data — application compliance, patching, configuration health-checking, infrastructure, application, and vulnerabilities.

Associated Components:

- 2 Session Events
- 2 Authorization Events
- 2 Authentication Events
- 2 Application Events
- 2 Network Events
- 2 Computer Events
- 2 Privilege Usage Events

- 2 eDiscovery Events
- 2 DLP Events
- 2 NIPS Events
- 2 Compliance Monitoring
- 2 CRLs
- 2 ACLs
- 2 Database Events
- 2 HIDS-HIPS
- 3 Transformation Services

Service Delivery Data Management: Focuses on the structure or unstructured data related to the management of IT services across the company. This includes service level management, availability management, disaster recovery, and recipient of services. A cost-benefit analysis should be performed when considering associated costs to these services.

Associated Components:

- 2 Service Catalog
- 2 SLAs
- 2 OLAs
- 2 Contracts
- 2 Recovery Plans

Service Support Data Management: All data related to providing services to the business across the company will reside here. This includes information pertaining to the service desk, incident management, configuration management, problem management, and knowledge management.

Associated Components:

- 2 Configuration Rules (Metadata)
- 2 Service Events
- 2 Configuration Management Database (CMDB)
- 2 Knowledge Repository
- 2 Change Logs

Data Governance Data Management: As applications and IT services are rolled out and managed across the organization, this section will store evidence, and proper compliance data throughout the software development lifecycle.

Associated Components:

- 2 Risk Assessments
- 2 Non-Production Data
- 2 Information Leakage Metadata
- 2 Data Segregation

Risk Management Data Management: All information related to the information security technical capabilities will be stored here, including data governance, application security, and data loss prevention, among other information sources that help improve the risk profile gathered per information asset.

Associated Components:

- 2 GRC
- 2 RA
- 2 BIA
- 2 DR & BC Plans
- 2 VRA
- 2 TVM (Threat Vulnerability Management)

ITOS Data Management: This section will have data related to the strategy and typical operations for an IT organization, such as the quality management, PMO, enterprise architecture compliance, business and IT alignment, and how all these services are transformed into agreements as we support the business needs.

Associated Components:

- 2 PMO
- 2 Strategy
- 2 Roadmap
- 2 Problem Management
- 2 Incident Management
- 2 CMDB
- 2 Knowledge Management
- 2 Service Management
- 2 Change Management

BOSS Data Management: All sources of data related to the Business Operations Support Services domain will be allocated here.

Associated Components:

- 2 Risk Assessments
- 2 Data Classification
- 2 Process Ownership
- 2 Audit Findings
- 2 HR Data (Employees & Contractors)
- 2 Business Strategy

Reporting Services: All tools used to generate operational reports, decision making, balance scorecards, dashboards, and other capabilities that will transform the different data sources and data models into useful information for the business and proper support (operational and strategic) for the risk management strategy will reside here.

Associated Components:

- 2 Dashboard
- 2 Data Mining
- 2 Business Intelligence
- 2 Reporting Tools

Relationships to other Domains

The Information Services domain provides contextual support for Application and Presentation service domains. The Information Technology Operations and Support domain govern the Application Service change and deployment process that other domains are required to implement periodically. The Business Operations Support Services domain governs security monitoring for information service applications. The BOSS domain then monitors the activities being performed by applications for any unusual behavior.

Infrastructure Services

Not to be confused with Infrastructure as a Service, Infrastructure Services can be visualized as the foundational capabilities provided by the rows of computers, network cables, power supplies, cooling vents, and fire suppression pipes you will see inside any standard data center. These capabilities include virtualization, compute, storage and network; facilities and environmentals; and physical security and access restrictions. Infrastructure Services may also reference Facilities, Hardware, Network and Virtual Environments.

Description

Infrastructure Services are the layered basic core capabilities that support higher-level capabilities in other architecture areas. These levels include virtual machines, applications, databases, as well as networking and the physical hardware and facilities.

As they provide a foundation, Infrastructure Services are mostly invisible to end-users of the cloud service. For example, a customer will likely be required by due diligence to assure that cloud facilities provide physical security to match the risk characteristics of the uses they make of cloud services, but otherwise will ignore the operational details of how physical access controls are implemented.

Infrastructure Services Components	Definition
1 Internal Infrastructure	The internal infrastructure services are mainly concerned with the physical assets used by the cloud service provider to support the virtualized services actually seen by cloud users. In many ways, these services are the lowest-level and least visible to the end cloud user though they are the foundation that underlies reliable and secure operation of the cloud service. For instance, without good facility security, there is no need for an adversary to mount a network attack on a cloud service as it is easier to just walk into the facility and unplug a server or network connection.
2 Facility Security	Concerned with the security controls applied at the cloud computing facility that assure a safe and secure operational environment for the physical components of a cloud infrastructure. Examples include restrictions applied to physical access, environmental controls, etc.
3 Controlled Physical Access	The security controls that limit physical access to a facility and its contents.
4 Barriers	Deny or limit physical access to a facility or portions of it (e.g., bollards placed between a facility and roadways to prohibit vehicular approach).
4 Electronic Surveillance	Continuous observation of an area to detect intrusion, record access and monitor movement.
4 Security Patrols	Periodic rounds by human or animal guards to deter and detect illicit activity as well as verify the status of other security controls (e.g., verifying doors are locked).
4 Physical Authentication	The process of verifying an asserted identity by physical means (e.g., a security guard verifying the photograph on an ID as matching the person providing it).
3 Asset Handling	The processes and procedures involved with managing physical assets (e.g., inventory control, location management, etc.).
4 Data	The digital representation of anything in any form (SNIA Dictionary).
4 Storage	A function that records data and supports retrieval (SNIA Dictionary).
4 Hardware	Generally, physical items of equipment used in providing infrastructure services (e.g., a server, a router, etc.).

3 Environmental Risk Management	The general process of assessing and controlling risks arising from the environment surrounding an infrastructure (e.g., estimating the size of a backup generator plant to provide power continuity in case of utility power loss).
4 Physical Security	Concerned with mitigating physical threats to a facility and its employees (e.g., fire suppression equipment and regular fire drills).
4 Equipment Location	The processes and procedures involved in siting equipment in appropriate locations (e.g., locating critical network equipment is a secured room with redundant power, temperature controls, etc.).
4 Power Redundancy	Providing multiple sources of electrical power to assure continuous operation in spite of loss of external utility power.
Availability Services	Concerned with assuring the availability of infrastructure components to match the service level objectives. Controls at this level include mirroring of data between geographically dispersed sites, redundant components and the processes for switching between them.
2 Patch Management	Concerned with assuring that required software fixes are applied in a controlled and timely fashion within the infrastructure. This includes both inventorying the services (operating systems, applications, embedded software, etc.) actually present in the infrastructure to identify the applicability of a particular fix and monitoring the infrastructure to assure that required fixes are actually present and installed.
3 Compliance Monitoring	Processed and procedures for assuring that a service is being provided in compliance with applicable policies and regulatory frameworks. This can be implemented through either periodic audit or continuous monitoring.
3 Service Discovery	Processes and procedures for identifying the services actually present (as opposed to those documented as being present) in order to assume that appropriate patches are installed.
2 Servers	Concerned with the software images that are installed on the physical servers and the controls applied to assure secure builds of those software images and how those images are managed.
3 Secure Build	The standard software image that is assured to comply with security policies.
3 Image Management	Processes and procedures for managing the collection of software images within an infrastructure.

2 Equipment Maintenance	Concerned with assuring that physical infrastructure devices are appropriately maintained to assure their continuous operations. Examples include periodic inspection, cleaning and replacement of air filters, proactive replacement of components when degradation is detected, etc.
2 Network Services	Concerned with managing the security risks posed by the network environment. Controls at this level include proper network segmentation (for example, assets used by organization A are not visible to organization B) and provision of basic network services such as an accurate and traceable time standard.
3 Network Segmentation	The processes and procedures that assure that the network structure matches the risk domains established within the infrastructure (e.g., externally facing servers are on a separate segment than internal servers).
3 Authoritative Time Source	Assures a traceable, standard time source for use within an infrastructure (e.g., server clocks are synced to the time source to enable events occurring on one server to be correlated with those occurring on another during incident response).
2 Storage Services	Concerned with the provisioning, migration and sanitization of physical storage in the infrastructure. Controls at this level assure that storage is available when required, its redundancy/reliability requirements match the service requirements, etc.
1 Virtual Infrastructure	The virtual infrastructure inherits some of the same services as are present in the physical infrastructure. For example, software images must be securely built and managed for the virtual servers that are hosted on the virtualization platform provided on the physical server. However, there are also unique requirements for the virtualized infrastructure itself.
2 "Desktop 'Client' Virtualization"	Concerned with how virtual instances of the traditional desktop are created, presented and managed.
3 Local	A virtual machine or application sandbox that is installed and managed on the endpoint but isolated from the rest of the endpoint. Management can be centralized but the virtual machine runs locally on the endpoint device (tablet, pc, etc.).
3 Remote	A virtual machine that is delivered over the network as opposed to being installed locally on a device.
4 Session-Based	A remote desktop presentation of any device where the presentation is controlled from a remote endpoint.

4 VM-Based (VDI)	A virtual desktop integrated with a presentation server to control access and manage multiple users.
2 Application Virtualization	Removes the link between the application and the server(s) that host it. A consumer would access an application instance without regard to where or on what the application was hosted.
3 Client Application Streaming	The Endpoint component of an application streaming solution. Clients could be tablets, phones, smart devices.
Server Application Streaming	The server-side component of an application streaming solution responsible for delivering content to multiple clients.
2 Virtual Workspaces	The template of the virtualized infrastructure defined by the cloud provider which defines characteristics of the virtual infrastructure instances such as number of hosts, network segmentation, storage and security elements. For High-Availability workspaces can be replicated across instances or cloud providers to provide redundant capabilities for failover purposes.
3 Vertical Isolation	Vertical isolation separates all virtualized components of the workspace, such as usage details, communication, memory or data, may not be leaked between workspaces.
2 Server Virtualization	Concerned with creating, accessing and managing a virtual server. Controls at this level assure that a server is configured correctly, includes the proper software image, etc.
3 Virtual Machines (Host-Based)	A physical host may virtualize various of its components and capabilities to provide the illusion of multiple machines, applications, etc.
4 Full	A fully virtualized environment or fabric that includes processor, storage and network capabilities. Can be provided as part of a physical machine or across multiple physical machines.
4 Paravirtualization	A virtualized operating system where the source code for the guest operating system is modified to run specifically as a guest operating system instead of a binary equivalent of the original hardware-targeted operating system.
4 Hardware-Assisted	Support in a given processor architecture for hypervisor execution (usually through provision of specialized instructions that support switching between guest instances, etc).
3 OS Virtualization	The capability to have a virtual workspace where different operating systems can be installed based on customer needs.

3 TPM Virtualization	A Trusted Platform Module can store code signatures or keys that the software trusts to be unalterable by an attacker. This capability refers to a virtualized TPM instance. TPM is defined by Trusted Computing Group.
3 Virtual Memory	An operating system feature that uses a combination of physical memory and backing storage (usually disk) to create the illusion that much larger memory space is available. For good performance, it relies on the principle of locality that assumes that only a small part of a program's address space (the working set) is actually in use at any point in time.
2 Storage Virtualization	Concerned with how virtualized storage is created, allocated and managed. This includes both 'block-based' storage such as a SAN (Storage Area Network) and 'file-based' virtualization such as NAS (Network Attached Storage) whether provided by a file server or appliance. Controls at this level assure that the storage is adequate to requirements, properly segregated and secured and that its performance matches the profile specified in the service level agreement.
3 Block-Based Virtualization	Virtualization at the level of block level devices (e.g., the host is presented with a virtual disk device).
4 Host-Based	Virtualized file systems may be presented by a server (e.g., a file server that provides several file shares).
5 LDM	Logical Device Manager (LDM). A Microsoft Windows capability similar in function to LVM.
5 LVM	Logical Volume Management (LVM). Allows grouping of several physical disks into a single logical volume as viewed by the host
5 LUN	Acronym for the SCSI protocol's Logical Unit Number (LUN) and commonly used as a term for the block device presented to a host via a SAN.
4 Storage-Device Based	Storage device controllers may allow virtualization of disk volumes (e.g., a hardware RAID controller that groups multiple physical volumes or sections of columns into a single host-visible RAID-5 array).
4 Network-Based	Virtualization at the filesystem level (i.e., the host is presented with a virtual filesystem).
5 Appliance	Network based visualization provided by a dedicated hardware appliance (e.g., a NAS filer).

5 Switched	A more complex storage area network architecture that includes a switching network to connect hosts with LUNs. Switched SANs may either be based on fibre channel or fibre channel over Ethernet (FCoE) or iSCSI.
3 File-Based Virtualization	A higher-level view of files that make the file largely independent of how it is presented. For example, a consumer would access mybudget.global without regard to whether it was hosted in a NAS appliance, a SAN or on a physical server.
2 Network Virtualization	Concerned with providing appropriate virtual network services. Controls at this level assure that the virtual network implements proper isolation (see 'segmentation' above), required connectivity and proper access controls.
3 Network Address Space	The ability to define network addresses within a virtual workspace to create a virtual network segment separate from that of the physical host machine.
4 IPv4	Internet Protocol Version 4 is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet and other packet-switched networks. IPv4 was the first version deployed for production on SATNET in 1982 and on the ARPANET in January 1983. It still routes most Internet traffic today, despite the ongoing deployment of a successor protocol, IPv6.
4 IPv6	Internet Protocol Version 6 is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion.
3 External (VLAN)	a VLAN is a group of hosts (on premise, in the cloud, between clouds or hybrid) with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location.
3 Internal (VNIC)	A VNIC is a virtualized network interface that presents the same media access control (MAC) interface that an actual interface would provide.

2 Database Virtualization	Database virtualization is the decoupling of the database layer, which lies between the storage and application layers within the application stack. Virtualization at the database layer allows hardware resources to be extended to allow for better sharing resources between applications and users, masking of the physical location and configuration of a database from querying programs, as well as enable more scalable computing.
2 Mobile Device Virtualization	Mobile Device Virtualization allows the organization to test compatibility with new technologies for different mobile devices.
2 Smartcard Virtualization	Methods and systems that allow users to virtualize a local smart card so that they can remotely connect to a server and interact with the server as if the local smart card was physically connected to the server.

Example

Even the cloud needs to reside somewhere physical, i.e., at a data center. These data centers are physically secured with fences, cameras, security guards, man-traps, and badge activated doors. Availability of the infrastructure is ensured with lines to multiple Internet service providers, power generators in a power failure, and multiple computers to do the same job in case one fails.

Services Provided

Infrastructure Services

The Infrastructure services are mainly concerned with the physical assets used by the cloud service provider to support the virtualized services seen by cloud users. In many ways, these services are the lowest level and least visible to the end cloud user. However, they are the foundation that underlies the reliable and secure operation of the cloud service. For instance, without good facility security, there is no need for an adversary to mount a network attack on a cloud service. It is easier just to unplug a server or network connection.

Facility Security: It is concerned with the security controls applied at the cloud computing facility that assures a safe and secure operational environment for a cloud infrastructure's physical components. Examples include restrictions applied to physical access and environmental controls.

Associated Components:

- 3 Controlled Physical Access
- 4 Barriers
- 4 Electronic Surveillance
- 4 Security Patrols
- 4 Physical Authentication
- 3 Asset Handling

- 4 Data
- 4 Storage
- 4 Hardware
- 3 Environmental Risk Management
- 4 Physical Security
- 4 Equipment Location
- 4 Power Redundancy

Servers: It is concerned with the software images installed on the physical servers and the controls applied to assure secure builds of those software images and how those images are managed.

Associated Components:

- 3 Secure Build
- 3 Image Management

Storage Services: It is concerned with the provisioning, migration, and sanitization of physical storage in the infrastructure. Controls at this level assure that storage is available when required and that its redundancy/reliability requirements match the service requirements.

Network Services: It is concerned with managing the security risks posed by the network environment. Controls at this level include proper network segmentation (for example, assets used by organization A are not visible to organization B) and provision of essential network services, such as an accurate and traceable time standard.

Associated Components:

- 3 Network Segmentation
- 3 Authoritative Time Source

Availability Services: It is concerned with assuring the availability of infrastructure components to match the service level objectives. Controls at this level include mirroring data between geographically dispersed sites, redundant components, and switching between them.

Patch Management: Concerned with assuring that required software fixes are applied in a controlled and timely fashion within the infrastructure. This includes both inventorying the services (operating systems, applications, embedded software, etc.) actually present in the infrastructure to identify the applicability of a particular fix, and monitoring the infrastructure to assure that required fixes are present and installed.

Associated Components:

- 3 Compliance Monitoring
- 3 Service Discovery

Equipment Maintenance: It is concerned with assuring that physical infrastructure devices are appropriately maintained to ensure their continuous operations. Examples include periodic inspection, cleaning, and replacement of air filters, and proactive replacement of components when degradation is detected.

Virtual Infrastructure Services

The Virtual Infrastructure inherits some of the same services as are present in the physical infrastructure. For example, software images must be securely built and managed for the virtual servers hosted on the virtualization platform provided on the physical server. However, there are also unique requirements for the virtualized infrastructure itself.

Desktop "Client" Virtualization: Concerned with how virtual instances of the traditional desktop are created, presented, and managed.

Associated Components:

- 3 Local
- 3 Remote
- 4 Session-Based
- 4 VM-Based (VDI)

Storage Virtualization: It is concerned with how virtualized storage is created, allocated, and managed. This includes both "block-based" storage such as a SAN (Storage Area Network) and "file-based" virtualization such as NAS (Network Attached Storage), whether provided by a file server or appliance. Controls assure that the storage is adequate to requirements, adequately segregated and secured, and that its performance matches the profile specified in the service level agreement.

Associated Components:

- 3 Block-Based Virtualization
- 4 Host-Based
- 5 LDM
- 5 LVM
- 5 LUN
- 4 Storage-Device Based
- 4 Network-Based
- 5 Appliance
- 5 Switched
- 3 File-Based Virtualization

Server Virtualization: Concerned with creating, accessing, and managing a virtual server. Controls at this level assure that a server is configured correctly and includes the proper software image and hypervisor.

Associated Components:

- 3 Virtual Machines (Host-Based)
- 4 Full
- 4 Paravirtualization
- 4 Hardware-Assisted
- 3 OS Virtualization
- 3 TPM Virtualization
- 3 Virtual Memory

Network Virtualization: Concerned with providing appropriate virtual network services. Controls at this level assure that the virtual network implements proper isolation (see "segmentation" above), required connectivity, and proper access controls.

Associated Components:

- 3 Network Address Space
- 4 IPv4
- 4 IPv6
- 3 External (VLAN)
- 3 Internal (VNIC)

Relationships to other Domains

Infrastructure Services provides many of the core components and capabilities that support capabilities provided in other parts of the architecture. For example, the higher levels of governance provided in the Security and Risk Management domain is largely meaningless without good physical security at the base level of the infrastructure. Service Delivery and Support under the ITOS domain similarly depends on the performance and reliability assurances provided at the infrastructure level.

Security and Risk Management (SRM)

Protecting data and managing risk

Security and Risk Management is the passwords, firewalls, and encryption that protect computer systems and data. It is the processes that define policies and audit systems against those policies. It uses ethical hackers and tools to test for weak spots in the systems. These services are what most people think of when they think of cyber security.

Description

The Security and Risk Management domain provides the core components of an organization's Information Security Program to safeguard assets and detect, assess, and monitor risks inherent in operational activities. Capabilities include Identity and Access Management, GRC (Governance, Risk and Compliance), Policies and Standards, Threat and Vulnerability Management, and Infrastructure and Data Protection.

Infrastructure Services Components	Definition
1 Governance Risk & Compliance	The fundamental issues of governance and enterprise risk management in Cloud Computing concern the identification and implementation of the appropriate organizational structures, processes, and controls to maintain effective information security governance, risk management and compliance. GRC encompasses, integrates and aligns activities such as corporate governance, enterprise risk management, and corporate compliance with applicable laws and regulations. **Components include:** a. compliance management (which assures compliance with all internal information security policies and standards), b. vendor management (to ensure that service providers and outsourcers adhere to intended and contractual information security policies applying ownership and custody), c. audit management (to highlight areas for improvement), d. IT risk management (to ensure that risk of all types is identified, understood, communicated, and either accepted, remediated, transferred or avoided), e. policy management (to maintain an organizational structure and process that supports the creation, implementation, exception handling, and frameworks that support business requirements), and f. technical awareness and training (to increase the ability to select and implement effective technical security mechanisms, products, processes, and tools).
2 Compliance Management	It analyzes compliance with all specified internal information security policies, control standards and procedures.
2 Policy Management	Security policies are the primary objectives of the security program. Policy management strives to maintain an organization structure and process that supports the creation, implementation, exception handling, and frameworks that represent business requirements.
3 Exceptions	A deviation that includes granting an exception to a standing policy when it cannot be met or can only partially be met. In this way, the Information Security team is aware of a scenario that is out of compliance and can, therefore, understand the associated risk and monitor the exception. Sometimes the exception is time-bound and reviewing periodically to assess risk and allow a remediation plan to be met.

3 Self-Assessment	A tool and process that involves performing an analysis/ assessment of risk or compliance by the owner/user rather than by a third party.
2 Vendor Management	Ensure that service providers and outsourcers adhere to intended and contractual information security policies applying concepts of ownership and custody.
2 Audit Management	It must be possible for an independent auditor to verify that the system conforms to the security policy. To enable this, systems and processes must ensure that security related events are recorded in a tamper-resistant audit log.
2 IT Risk Management	Information risk management is the act of aligning exposure to risk and capability of managing it with the risk tolerance of the data owner. It is the primary means of decision support for information technology resources designed to protect the confidentiality, integrity, and availability of information assets. Ensures that risk of all types are identified, understood, communicated, and either accepted, remediated, transferred or avoided. IT Risk Management can look at the output of Compliance Management activities to assist the organization in evaluating the overall security posture and aligning with the defined risk objectives.
2 Technical Awareness & Training	To increase the ability to select and implement effective technical security mechanisms, products, process and tools.

1 InfoSec Management	The main objective of Information Security Management is to implement the appropriate measurements to minimize or eliminate the impact that security-related threats and vulnerabilities might have on an organization. Measurements include Capability Maturity Models (which identify stages of development of an organization from an immature state through several levels of maturity as the organization gains experience and knowledge), Capability Mapping Models (which describe what a business does to reach its objectives and promotes a strong relationship between the business model and the technical infrastructure that supports the business requirements resulting in a view that can be understood by both the business and IT), Roadmaps in the form of security architectures (which provide a guideline to be followed by individual projects serving individual business initiatives), and Risk Portfolios (where identified risks are registered, monitored, and reported). Dashboards for security management and risk management are used to measure and report the effectiveness of decisions and help the organization make new decisions that will maintain and improve that effectiveness. Analysis and plans for remediating residual risks are also part of the overall risk management framework.
2 Capability Mapping	The capabilities of an Information Security Program can be described by a Security Service Catalog that is part of a larger catalog that some IT organizations document and publish to the business. These capabilities can be mapped in a way that describes what a business does to reach its objectives and promotes a strong relationship between the business model and the technical security infrastructure that supports the business requirements resulting in a view that can be understood by both the business and IT.
2 Maturity Model	Identify the stages of development of an organization from an immature state through several maturity levels as the organization gains experience and knowledge. COBIT defines a Capability Maturity Model with six levels of maturity: non-existent, initial, repeatable, defined, managed, and optimized.
2 Risk Portfolio Management	An articulation of the Information Security Program's scope and charter includes, for example, such focus areas as reputation, corporate governance and regulation, corporate social responsibility, and information assurance. The portfolio can change as necessary to remain consistent with the business objectives and to remain relevant and responsive to a changing threat landscape and evolving laws and regulations.

2 Risk Dashboard	Graphically measure and report the level of potential, inherent, and residual risks and the effectiveness of controls to help the organization understand threats and vulnerabilities and make risk-based decisions to maintain or improve control effectiveness.
2 Residual Risk Management	Analysis and plans for remediating information security risk that remains after the theoretical or applied implementation of mitigating controls with the intent of increasing control effectiveness and ultimately reducing risk to an acceptable level.
1 Privilege Management Infrastructure	Privilege Management Infrastructure ensures users have access and privileges required to execute their duties and responsibilities with Identity and Access Management (IAM) functions such as identity management, authentication services, authorization services, and privilege usage management. This security discipline enables the right individuals to access the right resources at the right times for the right reasons. It addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments and meet increasingly rigorous compliance requirements. This security practice is a crucial undertaking for any enterprise. The technical controls of Privilege Management Infrastructure focus on identity provisioning, password, and multi-factor authentication, policy management, etc. It is also increasingly business-aligned, and it requires business skills, not just technical expertise.
2 Identity Management	Ensure that credible identities can be used for authentication, entitlement, and access management by oversight of the full lifecycle of an identity.
3 Domain Unique Identifier	A unique reference number used as an identifier in computer software (for example GUID, 32-character hexadecimal string, used for Microsoft's implementation of the Universally unique identifier standard.
3 Federated IDM	Refers to a new standard based approach to directory services that streamlines and secures user access to networked resources, with the ability to establish trust relationships between various security domains to enable the passing of authentication, authorization, and privacy assertions.
3 Identity Provisioning	The creation, maintenance and deactivation of user objects as they exist in one or more systems, directories or applications, in response to automated or interactive business processes.

3 Attribute Provisioning	The creation, maintenance and deactivation of user attributes as they exist in one or more systems, directories or applications, in response to automated or interactive business processes.
2 Authentication Services	The function or API or process of determining if someone or something is who or what it is declared to be.
3 SAML Token	Security Assertion Markup Language (SAML) tokens are XML representations of claims. SAML tokens carry statements that are sets of claims made by one entity about another entity.
3 Risk Based Authentication	A non-static authentication system which takes into account the profile(IP address, User-Agent HTTP header, time of access, and so on) of the agent requesting access to the system to determine the risk profile associated with that transaction. The risk profile is then used to determine the complexity of the challenge. Higher risk profiles leads to stronger challenges, whereas a static username/password may suffice for lower-risk profiles. Risk-based implementation allows the application to challenge the user for additional credentials only when the risk level is appropriate
3 Multi Factor Authentication	A form of authentication that relies on two or more 'factors' where a factor is 'something you have' such as a smartcard, 'something you know' such as a password or pin, and 'something you are' such as a physical fingerprint or a behavioral keyboard cadence.
3 OTP	One Time Password (OTP) is a valid password for a short period (e.g., only one login session or transaction) and is aimed at avoiding several shortcomings associated with traditional static passwords. One of the most popular approaches for generating OTPs is time-synchronization between the authentication server and the client. OTP implementations are often used in two-factor authentication solutions where the user enters a pin used as a variable in an algorithm that generates evidence of identity sent to an enforcement agent that determines if the identity is valid.
3 Smart Card	A smart card (aka microprocessor card, chip card, or integrated circuit card) has traditionally taken a pocket-sized card with embedded integrated circuits. Smart cards are often used in two-factor authentication solutions where the user enters a pin which is used by an operating system on the smart card to release evidence of identity such as a digital certificate or to allow a private key to sign an identity token which is sent to an enforcement agent that determines if the identity is valid.

3 Password Management	The process to specify multiple password policies, define password composition constraints, maintain password history, restrict passwords, configure password validity period, create password rules, etc.
3 Biometrics	Biometrics consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. Biometrics are considered a form of identity and are used for authentication and access control.
3 Network Authentication	Authentication services provide methods/protocols for users (or devices) to logon to a network and other benefits (e.g., SSO).
3 Single Sign On	Access control feature where a user logs in once and gains access to many other systems without being prompted to log in again at each of them. One implementation of SSO is Kerberos.
3 WS-Security	A flexible and feature-rich extension to Simple Object Access Protocol (SOAP) to apply security to web services. The protocol specifies how integrity and confidentiality can be enforced on messages and allows the communication of various token formats such as SAML, Kerberos, and X.509.
3 Middleware Authentication	Authentication of applications/services/components that users never, ever see directly.
3 Identity Verification	The process of identifying living individuals by using their physiological and behavioral characteristics, or derived documents issued by an authority.
3 Out of the Box (OTB) Authentication	A method for implementing user login functionality in the applications through the identity provider's service without custom authentication code.
2 Authorization Services	A function, API or process that facilitates access control to restricted areas of the operating system/application/service/data and allows the administrator to restrict a user's or device's access to particular features.
3 Entitlement Review	A process checking appropriate existing user and role authorization access.
3 Policy Enforcement	A phase in Authorization Services, where access requests are approved or disapproved.
3 Policy Definition	A phase in authorization services that describe course or fine grained access or constraints to resources.
3 Policy Management	A process or platform for centralized policy creation, repository and management.

3 Principal Data Management	The capability for the management of all attributes regarding the subjects of access control decisions. These principals can be users, machines, or services. Authorization decisions may need to consider many attributes about the principals, including role, location, relationships to accounts, other principals, etc.
3 Resource Data Management	Authorization plays a key role in data management by simultaneously providing access and protection to application information resources.
3 XACML	eXtensible Access Control Markup Language is a declarative access control policy language implemented in XML.
3 Role Management	A role represents a set of permissions and privileges, and role management assures that roles are correctly defined to include only the required permissions and privileges and adequately assigned to entities.
3 Obligation	In XACML, an obligation is a directive from the Policy Decision Point to the Policy Enforcement Point on what action must be completed before or after an access is granted.
3 Out of the Box (OTB) Authorization	A method that allows authorization to be externalized from applications, for example, by providing an authorization plug-in. This allows developers to avoid the expense and trade-offs of creating custom access control. OTB Authorization solutions can provide full-featured authorization that includes a complete RBAC model, policy storage, user interface, built-in application group support, rule and query support, integrated system auditing, and performance optimization.
2 Privilege Usage Management	Management of access to sensitive information resources by privileged users such as administrators. Characteristics of robust management include that it be centralized, policy-driven, automated, granular, and auditable. A privileged user management system can control access to the administrative accounts used to install, configure, administer, and manage operating systems, applications, and databases.
3 Keystroke / Session Logging	Methodologies for capturing a detailed record of interactions with an entity (either at the level of individual keystrokes or interactions with the entity)
3 Password Vaulting	A software based solution to securely store and manage multiple passwords.
3 Privilege Usage Gateway	A gateway to grant/deny connection for sessions based on usage privilege on that workload.

3 Resource Protection	Prevention of misuse of computer resources.
3 Hypervisor Compliance and Governance	The capability of privilege management and monitoring by role and user associated with hypervisor administrators. This also includes the management of virtual networks, servers, and applications in a cloud environment.
1 Threat & Vulnerability Management	This discipline deals with core security, such as vulnerability management, threat management, compliance testing, and penetration testing. Vulnerability management is a complex endeavor in which enterprises track their assets, monitor, scan for known/emerging vulnerabilities, and take action by patching the software, changing configurations, or deploying other controls to reduce the attack surface at the resource layer. Threat modeling and security testing are also part of activities to identify the vulnerabilities effectively. This discipline aims to proactively inspect the infrastructure that runs the cloud to address new security threats using vulnerability scanning, virtual patching, and other aspects of security testing and response.
2 Compliance Testing	Compliance testing determines the degree to which information security policies, standards, and control procedures are being adhered to. One example is scanning to detect the presence or absence of mandated patches and updates on virtual and physical machines.
3 Databases (DBs)	Compliance testing against a collection of data that is organized so that its contents can easily be accessed, managed, and updated.
3 Servers	Compliance testing against a software program or the computer on which that program runs provides a specific kind of service to client software running on the same computer or other computers on a network.
3 Networks	Compliance testing against a series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain subnetworks.
2 Vulnerability Management	The cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities (generally in software).
3 Application	Computer software designed to help the user to perform specific tasks. Examples include enterprise software, accounting software, office suites, graphics software, and media players.

3 Infrastructure	A shared, evolving, open, standardized, and heterogeneous installed base and as all of the people, processes, procedures, tools, facilities, and technology which supports the creation, use, transport, storage, and destruction of information (also referred to as information infrastructure).
3 DB	See Databases (earlier)
2 Penetration Testing	A method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders (who do not have an authorized means of accessing the organization's systems) and malicious insiders (who have some level of authorized access), also referred as pentest.
3 Internal	It focuses on attacks that could be launched by an insider. In contrast to a remote attacker, this attacker may have some form of authorized access and already has access to the internal network. The insider can also have more knowledge of the location of valuable data.
3 External	Focuses on the ability of a remote attacker to get to the internal network. This form of penetration testing aims to access data located within the internal network by exploiting externally exposed devices, including servers, clients, applications and wireless access points.
2 Threat Management	Threat Management focuses on threats, threat sources, and threat agents that can compromise confidentiality, integrity, and availability of data. Threat management can leverage a threat taxonomy to provide structure. Threat management also contributes to the overall risk assessment process.
3 Source Code Scanning	The method of identifying security bugs in software with static code analysis tools.
3 Risk Taxonomy	A taxonomy to identify, capture, and classify known threats. One example used in the SABSA threat modeling framework defines threat domains (people, processes, systems, external events) and threat categories based on experience and observation.

1 Infrastructure Protection Services	Infrastructure Protection Services secure Server, Endpoint, Network, and Application layers. This discipline uses a traditional defense in depth approach to ensure containers and pipes of data are healthy. The controls of Infrastructure Protection Services are usually considered as preventive technical controls such as Intrusion Detection/Prevention Systems (IDS/IPS), Firewall, Anti-Malware, White/Black Listing, and more. They are relatively cost-effective in defending against the majority of traditional or non-advanced attacks.
2 Server	See Servers
3 Behavioral Malware Prevention	The ability to identify the behavior of malware based on events. For example, an inbound email with attached targeted malware to be filtered via the use of a secure virtual machine to identify when the payload is triggering atypical activity.
3 White Listing	A list or register of entities that, for one reason or another, are being provided a particular privilege, service, mobility, access or recognition.
3 Sensitive File Protection	The ability to protect sensitive information from being read or modified by administrators who have access to a file system but are not authorized to read the protected data within certain files. Also, the ability to monitor changes to sensitive files to audit who is making changes to them or reading them.
3 HIPS / HIDS	Host Intrusion Detection Systems (HIDS) can detect actions that attempt to compromise the confidentiality, integrity, or availability of a resource. Host Intrusion Prevention Systems (HIPS) includes taking a preventive measure without direct human intervention.
3 Anti-Virus	See Anti-Virus, Anti-Spam, Anti-Malware.
3 Host Firewall	A form of protecting Endpoints is the use of personal firewalls, which are typically applications that control network traffic to and from a computer, permitting or denying communications based on a security policy implemented as a rule set. An Endpoint firewall differs from a firewall appliance that is often placed on a network and serves the Endpoints.
2 Endpoint	Computing devices used by users (e.g., desktop, tablet, smartphone).
3 Anti-Virus, Anti-Spam, Anti-Malware	A software program used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worm, trojan horses, spam, spyware, and adware.

3 HIPS / HIDS	Host-based Intrusion Detection is the capability to detect actions that attempt to compromise the confidentiality, integrity, or availability of a resource at the host or Endpoint. Host-based Intrusion Prevention includes taking a preventive measure without direct human intervention.
3 Host Firewall	A software program or function running on a single host that can restrict incoming and outgoing network activity for that host only
3 Media Lockdown	Also referred to as removable media lockdown, a control to block user access to writable devices such as USB Flash memory sticks and CD/DVD-RW drives to prevent data leak.
3 Hardware-Based Trusted Assets	Assets with trust rooted to hardware (e.g. computers with TPM chip).
3 Behavioral Malware Prevention	The ability to identify the behavior of malware based on events. For example, an inbound email with attached targeted malware to be filtered via the use of a secure virtual machine to identify when the payload is triggering atypical activity.
3 Inventory Control	To provide management control and accountability over the organization's physical and digital assets. Cloud and virtualization can create a challenge in terms of attempting to inventory virtual machines in the way physical machines have traditionally been tracked.
3 Content Filtering	The technique whereby content is blocked or allowed based on analysis of its content, rather than its source or other criteria. It is most widely used on the internet to filter email and web access.
3 Forensic Tools	Assures that the proper tools are available to authorized parties and processes to facilitate identification and preservation of relevant digital artifacts pertinent to an investigation (e.g., policy violation, e-discovery request or criminal investigation)
3 White Listing	Whitelisting is a form of filtering where a list is created that registers entities that are granted access or are welcomed signatures. When a whitelist is used, the default is to "deny all" except for those entries that are enumerated in the filter. These are typically used when it is easier (or a shorter list) to identify what is desirable rather than what is not desirable.
2 Network	See Networks
3 Behavioral Malware Prevention	The ability to identify the behavior of malware based on events. For example, an inbound email with attached targeted malware to be filtered via the use of a secure virtual machine to identify when the payload is triggering atypical activity.

3 Firewall	A firewall is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate network-traffic to pass. Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components.
3 Content Filtering	The technique whereby content is blocked or allowed based on analysis of its content, rather than its source or other criteria. It is most widely used on the internet to filter email and web access.
3 DPI	Deep Packet Inspection (DPI) (also called complete packet inspection and Information extraction - IX -) is a form of computer network packet filtering that examines the data part (and possibly also the header) of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions or predefined criteria to decide if the packet can pass or if it needs to be routed to a different destination, or to collect statistical information.
3 NIPS / NIDS	Network Intrusion Prevention includes taking a preventive measure without direct human intervention. Network Intrusion Detection is the capability to detect actions that attempt to compromise the confidentiality, integrity, or availability of a resource over the network.
3 Wireless Protection	Protection of data in transit over wireless media, including 802.11 Wi-Fi, cellular, and Bluetooth. Some forms of encryption are the typical protection approach, e.g., Wi-Fi Protected Access (WPA) leveraging TKIP or AES.
3 Link Layer Network Security	Protection of data can be applied at the OSI Layer 2 Data Link Layer. Network switches are key components at Layer 2 communications and are susceptible to attacks such as CAM table overflow, VLAN hopping, spanning-tree protocol manipulation, MAC address spoofing, and ARP attacks. Mitigations include configuration of port security on a switch, modification to VLAN configurations, ACLs' configuration on router ports, and 802.1X.
3 Black Listing Filtering	"Blacklisting is a form of filtering where a list is created that registers entities that are prohibited access or are unwelcome signatures. When a blacklist is used, the default is to 'permit all' except for those entries that are enumerated in the filter. These are typically used when it is easier (and therefore a shorter list) to determine what entities should not be allowed."

2 Application	See Applications
3 XML Appliance	A special-purpose network device used to secure, manage and mediate XML traffic. They are most popularly implemented in Service-Oriented Architectures to control XML based Web Services traffic, and increasingly in cloud-oriented computing to help enterprises integrate on-premise applications with off-premise cloud-hosted applications. XML Appliances are also commonly referred to as SOA Appliances, SOA Gateways, XML Gateways, Cloud Brokers.
3 Secure Messaging	A server-based approach to protect sensitive data when sent beyond the corporate borders and provides compliance with industry regulations such as HIPAA, GLBA and SOX.
3 Application Firewall	A form of firewall which controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls that do not meet the firewall's configured policy.
3 Secure Collaboration	A technology or solution for securing collaboration service (e.g., SharePoint) to extend access to employees on the go, partners, vendors, and even customers.
3 Real Time Filtering	A control to track use patterns and information like what sites are visited and blocked some in real-time based on policies.
1 Data Protection	In the information age, data is an asset. However, most data is valuable only if it is protected. Data protection needs to cover all data lifecycle stages, data types, and data states. Data stages include create, store, access, roam, share, and retire. Data types include unstructured data such as word processing documents, structured data such as data within databases, and semi-structured data such as emails. Data states include data at rest (DAR), data in transit (DIT) (aka data in motion, data in flight), and data in use (DIU). Data Protection controls include data lifecycle management, data loss prevention, intellectual property protection with digital rights management, and cryptographic services such as key management and PKI/symmetric encryption.
2 Data Life Cycle Management	The Data Life Cycle Management covers the following six phases: create, store, use, share, archive, and destroy. Although it is shown as a linear progression, once created, data may flow between stages without restriction, and may not pass through all stages during usefulness.

3 Meta Data Control	Controlling what types of metadata accompany the underlying data (e.g., the record of changes to a document maintained as metadata by a word processing application should not be released with the document)
3 eSignature (Unstructured Data)	An electronic signature indicates that a person adopts the contents of digital data or that the person who claims to have written a message is the one who wrote it. This is most frequently used on unstructured data.
3 Data De-Identification	The process for removing identifying information from datasets, most commonly to protect the privacy of individuals, by using methods such as data masking. Data de-identification may also be used to protect organizations, such as businesses included in statistical surveys, or other information such as the spatial location of mineral or archaeological finds or endangered species.
3 Life Cycle Management	Policies, processes, and procedures for managing the lifecycle of data from creation through use, archiving and eventual destruction
3 Data Masking	The process of obscuring (masking) specific data elements within data stores. It ensures that sensitive data is replaced with realistic but not real data. The goal is that sensitive data are not available outside of the authorized environment.
3 Data Obscuring	A method of protecting fields or records of data by some form of obfuscation such as encryption. Data obscuring techniques can be used in source code, for example, to prevent reverse engineering of applications. There are also low tech solutions such as ink stamps to redact sensitive information on hard copies.
3 Data Tagging	A data tag is a keyword or term assigned typically as a form of metadata to a piece of information. It helps describe an item and facilitates it being found again by browsing or searching.
3 Data Seeding	A way of detecting and tracking data scraping, plagiarism, and theft is to seed the data with either easily identifiable items to trace where the data ends up or with bogus records to destroy the value of the data. For example, by inserting a record in a phone number database with an odd name, the true originator/ owner could identify that bogus record if it appears in a competitor's database.

2 Data Loss Prevention	DLP refers to systems that enforce policies to safeguard critical data such as Intellectual Property and customer information and ensure it doesn't escape from the enterprise to unintended parties. These solutions discover and classify sensitive data, define and manage policies based on content and context, monitor and enforce movement of data, as well as report, audit, and document incidents of data leakage.
3 Data Discovery	Scanning and classifying data held in Network, Endpoint, and Server.
3 Network (Data in Transit)	See Data in Transit Encryption (DLP in this case)
3 Endpoint (Data in Use)	See Data in Use Encryption (DLP in this case)
3 Server (Data at Rest)	See Data at Rest Encryption (DLP in this case)
2 Intellectual Property Protection	The activity (e.g. applying process or technical control) of preventing misuse and improper disclosure of intellectual property.
3 Intellectual Property	A term referring to a number of distinct types of creations of the mind for which a set of exclusive rights are recognized-and the corresponding fields of law. Under intellectual property law, owners are granted certain exclusive rights to various intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs. Common types of intellectual property rights include copyrights, trademarks, patents, industrial design rights, and trade secrets in some jurisdictions.
3 Digital Rights Management	DRM is a term for access control technologies used by hardware manufacturers, publishers, copyright holders, enterprises, and individuals to limit the use of digital content and devices. The term has taken on at least two meanings. One refers to technology supporting the 1998 Digital Millennium Copyright Act to protect copyrighted media, maintain royalties, and ensure artistic control. The other definition applies to enterprise rights management technologies that attempt to put security controls closer to the enterprise data itself, often in encryption and metadata that carry access control information.
2 Cryptographic Services	A set of cryptographic functions (e.g., encoding and decoding, encryption and decryption), which computer application programs may use, to implement security solutions (e.g., strong user authentication or secure email). For example, in Microsoft Windows, a Cryptographic Service Provider (CSP) is a software library that implements the Microsoft CryptoAPI (CAPI).

3 Key Management	Key management covers the entire lifecycle of keys beginning to end including generation, communication and distribution, storage, entry, and installation, checking the validity, usage, changing the active key, archiving, destruction, an audit of key operations and usage, key backup and recovery, and emergency reserve keys.
4 Symmetric Keys	Also referred to as a symmetric cryptographic cipher, both parties must use the same key for encryption and decryption. The encryption keys must be shared between the parties before any decryption of the message can take place.
4 Asymmetric Keys	Also referred to as an asymmetric cipher, the encryption key and the decryption keys are separate. In an asymmetric system, each person has two keys. One key, the public key, is shared publicly. The second key, the private key, should never be shared with anyone.
3 PKI	Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store and revoke digital certificates to support the use of public key cryptography for all participants in the business community. Components include registration authorities and certificate authorities. The PKI is typically a hierarchical model that consists of the root certificate authorities, registration authorities, and certificate authorities.
3 Signature Services	A software program or function to provide an electronic coded message which is unique to both the document and the signer and binds both of them together. The digital signature ensures the authenticity of the signer. After it is signed, any changes made to the document invalidate the signature, thereby protecting against signature forgery and information tampering.
3 Data-in-Use Encryption (Memory)	Encryption of "Data in Use" (data in resident memory, or swap, or processor cache or disk cache, etc.).
3 Data-in-Transit Encryption (Transitory, Fixed)	Encryption of "Data in Transit" (data being transferred between two nodes in a network).
3 Data-at-Rest Encryption (DB, File, SAN, Desktop, Mobile)	Encryption of "Data at Rest" (data recorded on storage media).

1 Policies & Standards	Security policies are part of a logical abstraction of an Enterprise Security Architecture. They are derived from risk-based business requirements and exist at several different levels including, Information Security Policy, Physical Security Policy, Business Continuity Policy, Infrastructure Security Policies, Application Security Policies, and the overarching Business Operational Risk Management Policy. Security Policies are statements that capture requirements specifying what type of security and how much should be applied to protect the business. Policies typically state what should be done while avoiding reference to particular technical solutions. Security Standards are an abstraction at the component level and are needed to ensure that the many different components can be integrated into systems. There are many internationally recognized standards for security from standards bodies such as ISO, IETF, IEEE, ISACA, OASIS, and TCG. Direction can also be provided in operational security baselines, job aid guidelines, best practices, correlation of regulatory requirements, and role-based awareness. One way to approach security policy and its implementation is to classify information and associate policies with the resulting classes of data.
2 Operational Security Baselines	A baseline specifies a policy compliant starting point that may be further specialized (e.g., a move to production process may include a baseline configuration that requires all default users/ passwords, SNMP community names, etc. be changed from their default values before the equipment may be used in production. If the equipment were subject to additional hardening, such as deployment in the DMZ, further specialized baselines would apply).
2 Job Aid Guidelines	A job aid (aka Standard Operating Procedures or Playbooks) stores information or instruction external to a user and guides them to perform a task correctly. It is used during the actual performance when the user needs to know the information or procedure. It can be consulted quickly when needed and provides specific, concise information to the user. It reduces the need for individuals to remember so much information and is an efficient method to reduce problems associated with relying strictly on recall to perform in certain situations.
2 Role Based Awareness	Association of policy with a given role. For example, a user might be designated as a 'local user' and a function such as data transfers might be configured to only be available to the 'local user' role and not be available to a user with a role of 'mobile user'.

2 Information Security Policies	Broad statements of management intent that guide the information security operations of an organization. Policies are implemented by standards and procedures and compliance can be verified through audits.
2 Technical Security Standards	Stipulate how specific technical security controls must be implemented (for example, a security policy might mandate at-rest encryption for a particular class of data and a technical security standard might specify that the encryption implementation must be FIPS 140-2 certified AES-256).
2 Data / Asset Classification	A way to approach security policy and its implementation that involves the classification of information into one of several categories, each of which has an associated security policy. Other assets such as servers and endpoints, can be similarly classified. In some cases, data can only be processed or stored on computers that share the same classification designation.
2 Best Practices & Regulatory Correlation	A mapping of best practices to mandated regulatory requirements. If a regulatory mandate requires a certain type of data to be encrypted (e.g., PHI in HIPPA), then a vendor best practice document would be correlated with the regulatory mandate to show how the best practices implement it for compliance.

Example

An employee working from home must log into the corporate VPN using the one-time password token on his key fob. A new website being built is tested for compliance with corporate security policies. A thief cannot read data on a stolen laptop if its hard drive has been encrypted.

Services Provided

Governance Risk and Compliance: GRC encompasses, integrates, and aligns activities such as corporate governance, enterprise risk management, and corporate compliance with applicable laws and regulations. Components include compliance management (which assures compliance with all internal information security policies and standards), vendor management (to ensure that service providers and outsourcers adhere to intended and contractual information security policies applying concepts of ownership and custody), audit management (to highlight areas for improvement), IT risk management (to ensure that risk of all types are identified, understood, communicated, and either accepted, remediated, transferred, or avoided), policy management (to maintain an organizational structure and process that supports the creation, implementation, exception handling and management of policy that represent business requirements), and technical awareness and training (to increase the ability to select and implement effective technical security mechanisms, products, process and tools).

Associated Components:

- 2 Compliance Management
- 2 Policy Management
- 3 Exceptions
- 3 Self-Assessment
- 2 Vendor Management
- 2 Audit Management
- 2 IT Risk Management
- 2 Technical Awareness & Training

Information Security Management: The main objective of Information Security Management is to implement the appropriate measurements to minimize or eliminate the impact that security-related threats and vulnerabilities might have on an organization. Measurements include Capability Maturity Models (which identify stages of development of an organization, from an immature state through several levels of maturity as the organization gains experience and knowledge), Capability Mapping Models (which describe what a business does to reach its objectives, and which promote a strong relationship between the business model and the technical infrastructure that supports the business requirements, resulting in a view that can be understood by both the business and IT), Roadmaps in the form of security architectures (which provide a guideline to be followed by individual projects serving individual business initiatives), and Risk Portfolios (where identified risks are registered, monitored, and reported). Dashboards for security management and risk management are used to measure and report the level of effectiveness of decisions and help the organization make new decisions that will maintain and improve that effectiveness. Analysis and plans for remediating residual risks are also part of the overall risk management framework.

Associated Components:

- 2 Capability Mapping
- 2 Maturity Model
- 2 Risk Portfolio Management
- 2 Risk Dashboard
- 2 Residual Risk Management

Privilege Management Infrastructure: Privilege Management Infrastructure ensures users have access and privileges required to execute their duties and responsibilities with Identity and Access Management (IAM) functions such as identity management, authentication services, authorization services, and privilege usage management. This security discipline enables the right individuals to access the right resources at the right times for the right reasons. It addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments and meet increasingly rigorous compliance requirements.

The technical controls of Privilege Management Infrastructure focus on identity provisioning, password, multi-factor authentication, and policy management. This security practice is a crucial undertaking for any enterprise. It is also increasingly business-aligned, and it requires business skills, not just technical expertise.

Associated Components:

- 2 Identity Management
- 3 Domain Unique Identifier
- 3 Federated IDM
- 3 Identity Provisioning
- 3 Attribute Provisioning
- 2 Authentication Services
- 3 SAML Token
- 3 Risk Based Authorization
- 3 Multi Factor Authentication
- 3 OTP
- 3 Smart Card
- 3 Password Management
- 3 Biometrics
- 3 Network Authentication
- 3 Single Sign On
- 3 WS-Security
- 3 Middleware Authentication
- 3 Identity Verification
- 3 Out of the Box (OTB) Authentication
- 2 Authorization Services
- 3 Entitlement Review
- 3 Policy Enforcement
- 3 Policy Definition
- 3 Policy Management
- 3 Principal Data Management
- 3 Resource Data Management
- 3 XACML
- 3 Role Management
- 3 Obligation
- 3 Out of the Box (OTB) Authorization
- 2 Privilege Usage Management
- 3 Keystroke / Session Logging
- 3 Password Vaulting
- 3 Privilege Usage Gateway
- 3 Resource Protection
- 3 Hypervisor Compliance and Governance

Threat and Vulnerability Management: This discipline deals with core security, such as vulnerability management, threat management, compliance testing, and penetration testing. Vulnerability management is a complex endeavor in which enterprises track their assets, monitor, and scan for known vulnerabilities, and take action by patching the software, changing configurations, or deploying other controls in an attempt to reduce the attack surface at the resource layer. Threat modeling and security testing are also part of activities to identify the vulnerabilities effectively.

Associated Components:

- 2 Compliance Testing
- 3 Databases (DBs)
- 3 Servers
- 3 Networks
- 2 Vulnerability Management
- 3 Application
- 3 Infrastructure
- 3 DB
- 2 Penetration Testing
- 3 Internal
- 3 External
- 2 Threat Management
- 3 Source Code Scanning
- 3 Risk Taxonomy

Infrastructure Protection Services: Infrastructure Protection Services secure Server, Endpoint, Network, and Application layers. This discipline uses a traditional defense-in-depth approach to make sure containers and pipes of data are healthy. The controls of Infrastructure Protection Services are usually considered as preventive technical controls such as IDS/IPS, Firewall, Anti-Malware, Allow/Deny Listing, and more. They are relatively cost-effective in defending against the majority of traditional or non-advanced attacks.

Associated Components:

- 2 Server
- 3 Behavioral Malware Prevention
- 3 White Listing
- 3 Sensitive File Protection
- 3 HIPS / HIDS
- 3 Anti-Virus
- 3 Host Firewall
- 2 Endpoint
- 3 Anti-Virus, Anti-Spam, Anti-Malware
- 3 HIPS / HIDS
- 3 Host Firewall
- 3 Media Lockdown
- 3 Hardware-Based Trusted Assets
- 3 Behavioral Malware Prevention
- 3 Inventory Control
- 3 Content Filtering
- 3 Forensic Tools
- 3 White Listing
- 2 Network
- 3 Behavioral Malware Prevention

- 3 Firewall
- 3 Content Filtering
- 3 DPI
- 3 NIPS / NIDS
- 3 Wireless Protection
- 3 Link Layer Network Security
- 3 Black Listing Filtering
- 2 Application
- 3 XML Appliance
- 3 Secure Messaging
- 3 Application Firewall
- 3 Secure Collaboration
- 3 Real Time Filtering

Data Protection: In the information age, data is an asset. However, most data remains valuable only if it is protected. Data protection needs to cover all data lifecycle stages, data types, and data states. Data stages include create, store, access, roam, share, and retire. Data types include unstructured data, such as word processing documents, structured data, such as data within databases, and semi-structured data, such as emails. Data states include data at rest (DAR), data in transit (DIT) (also known as "data in motion" or "data in flight"), and data in use (DIU). Data Protection controls are data lifecycle management, data leakage prevention, intellectual property protection with digital rights management, and cryptographic services such as key management and PKI/symmetric encryption.

Associated Components:

- 2 Data Life Cycle Management
- 3 Meta Data Control
- 3 eSignature (Unstructured Data)
- 3 Data De-Identification
- 3 Life Cycle Management
- 3 Data Masking
- 3 Data Obscuring
- 3 Data Tagging
- 3 Data Seeding
- 2 Data Loss Prevention
- 3 Data Discovery
- 3 Network (Data in Transit)
- 3 Endpoint (Data in Use)
- 3 Server (Data at Rest)
- 2 Intellectual Property Protection
- 3 Intellectual Property
- 3 Digital Rights Management
- 2 Cryptographic Services
- 3 Key Management
- 4 Symmetric Keys
- 4 Asymmetric Keys

- 3 PKI
- 3 Signature Services
- 3 Data-in-Use Encryption (Memory)
- 3 Data-in-Transit Encryption (Transitory, Fixed)
- 3 Data-at-Rest Encryption (DB, File, SAN, Desktop, Mobile)

Policies and Standards: Security policies are part of a logical abstraction of Enterprise Security Architecture. They are derived from risk-based business requirements and exist at several different levels, including Information Security Policy, Physical Security Policy, Business Continuity Policy, Infrastructure Security Policies, Application Security Policies as well as the overarching Business Operational Risk Management Policy. Security Policies are statements that capture requirements specifying what type of security and how much should be applied to protect the business. Policies typically state what should be done, while avoiding reference to particular technical solutions. Security Standards are an abstraction at the component level and are needed to ensure that the many different components can be integrated into systems.

Internationally recognized standards for various aspects of security from standards bodies include ISO, IETF, IEEE, ISACA, OASIS, and TCG. Direction can also be provided in the form of operational security baselines, job aid guidelines, best practices, correlation of regulatory requirements, and role-based awareness. One way to approach security policy and its implementation is to classify information and associate policies with the resulting classes of data.

Associated Components:

- 2 Operational Security Baselines
- 2 Job Aid Guidelines
- 2 Role Based Awareness
- 2 Information Security Policies
- 2 Technical Security Standards
- 2 Data / Asset Classification
- 2 Best Practices & Regulatory Correlation

Relationships to other Domains

SRM provides the security context for IT Operations and Support. Security aspects of ITOS capabilities and functions are critical to the delivery of IT services supporting a business. SRM is a key component of Operational Risk Management under Business Operation Support Services, as Security Risks are crucial data points of the organization's business intelligence, which supplies information necessary to make sound business decisions. Human Resources supports the SRM agenda through vigilant attention to the workforce. SRM provides Identity and Access Management services that are prerequisites to the presentation of data to users. Protection of data in transit, at rest, and in use is a critical underpinning to the processing and manipulating of data by application services. SRM has a dependency on the core components and capabilities provided by Infrastructure Services, including the physical security of facilities and patch management.