CISSP® 2015

Domain 1 Security & Risk Management

V1

A. Understand & apply concepts of CIA

- **Security management:**
  - Objective: protect the company and its assets
  - **Management Support** and commitment is essential
  - Topics:
    - CIA
    - Governance
    - Compliance
    - Legal and regulatory issues
    - Policy Chain
    - Business Continuity requirement
    - Personnel
    - Risk Management
    - Threat Modelling
    - Acquisitions strategy and practice
    - Education, Training & awareness

CIA Principles

- **Fundamental principles of security**
  - **Confidentiality**: protection of information within systems so that unauthorized people cannot access.
    - Shoulder surfing, social engineering, not encrypting
    - Consider: access control, encryption
  - **Integrity**: protection of information from intentional and accidental unauthorized changes.
    - Intentionally (by attacker) or unintentionally (user mistake)
    - Consider: input verification; strict access control, intrusion detection, message hashing
    - Contains (1) accuracy and (2) completeness
  - **Availability**: assurance that information is accessible by authorized users whenever needed.
    - Consider: HA, BCP, backup, Identify single point of failure, prevention, monitoring

Principles

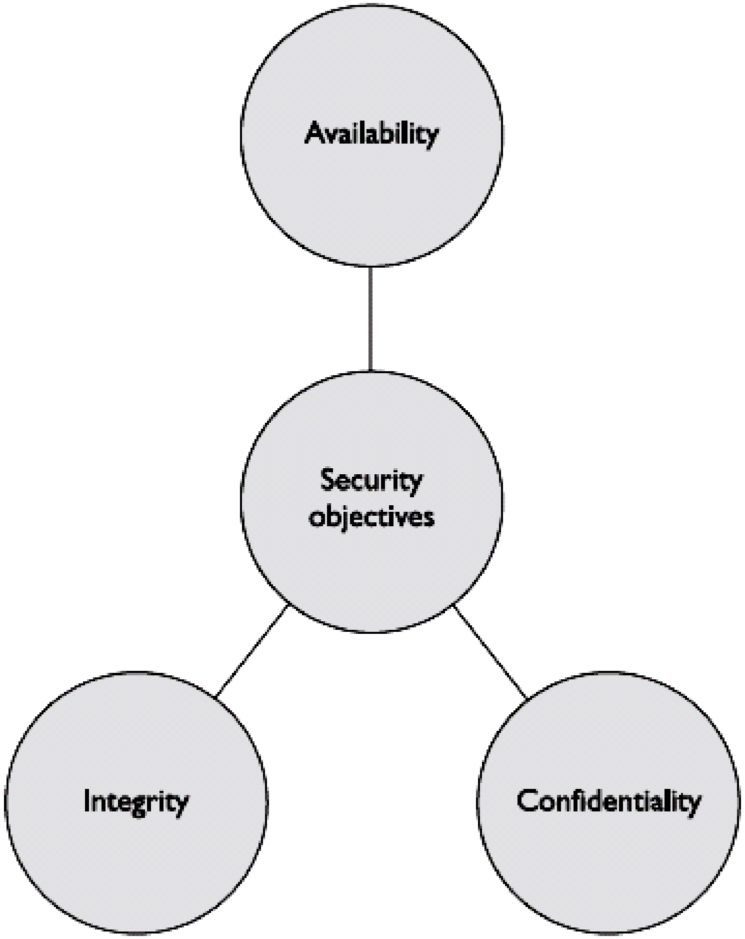


Figure 3-2 The AIC triad

Question

Which factor is the most important item when it comes to ensuring security is successful in an organization?

A. Senior management support

B. Effective controls and implementation methods

C. Updated and relevant security policies and procedures

D. Security awareness by all employees

Obscurity

- **Security through obscurity**
  - Example: put the door key under the carpet; use complicated folder structure to hide information
  - debate: should or should not keep encryption algorithm secret?
  - can damage result

Other Security Frameworks (not important in exam)

- **COSO**:
  - Committee of Sponsoring Organizations of the Treadway Commission
  - control environment; Risk Assessment; Control Activities; Information & Communication
  - is Corporate governance, strategic level; IT and non-IT
- **COBIT 5**:
  - 37 IT Governance and IT Management processes
  - A rich publication collections include IT security, assurance, process model, and assessment guide
  - Certifications
    - Foundation
    - Implementation
    - Assessor

Other Security Frameworks (not important in exam)

- **ISO/IEC 27001**
  - An internationally recognized Information Security Management System (ISMS) standard for certifying an organisation's ISMS
  - ISO 27001: certification requirements
  - ISO 27002: code of practices and control objectives
  - Coverage is similar to CISSP domains
  - Personnel certifications
    - Foundation
    - Lead Auditor

Security Governance

- Governance: how senior management governs the technical functions
- Governance basic components
  - Business alignment
  - Resources Management
  - Value delivery
  - Performance measurement
  - Risk Management

Security Governance

- As security profession in an organization, should understand:
  - Goals, Mission and Objectives of the organization
  - Organizational Processes:
    - Acquisitions and mergers
    - Divestitures and Spinoffs
    - Forming Governance Committees

Alignment (Security to Business)

- Alignment of security functions to business' strategy, goal, mission and objective
- **Why:** Security is not primary objective in most organizations
- **Top-Down approach**: (1) from senior to general staff, (2) from business to security (or IT) (3) from policy to procedure
- **How**: Via organizational processes such as business case, budget, resource management, acquisition process etc.

Security roles & responsibilities (R&R)

- **Layer of Responsibility**
  - Security is everyone's business
  - Differ layer → differ knowledge or vision → differ concern on security
- **Security organization**
  - **Board of directors**
    - elect from shareholder, should be independent to work, avoid conflict of interest.
    - Hold personal responsible for SOX, GLBA…. (these specific regulation will not cover in CISSP exam.

Detail Position – not important in the exam.

- **Executive Management**
  - **CEO**: day-to-day management responsibilities, oversees everything, including finances, planning and operation at a high level.
    - More and more regulations dealing with IS are holding CEO responsibility
  - **CFO:** responsible corporation’s account and financial…
  - CFO & CEO are responsible for informing stakeholders about financial and health condition.
    - Risk appetite: How much risk the company should take on
  - Chief Information Officer (**CIO**): responsible for strategic use and management of information systems and technology.
    - Bridge of technology and business
    - Responsible for the security program

Detail Position – not important in the exam.

- Chief Privacy Officer (**CPO**): ensuring that customer, company and employee data are kept safe.
  - Newer position, often report to Chief Security officer
  - Involve setting policies on how data are collected, protected and give out to 3rd party
- Chief Security Officer (**CSO**): responsible for understanding the risk and mitigating risk to acceptable level. Also responsible for creating and maintain security program.
  - role extends beyond IT and reach into business process, legal issue, operation issue, revenue generation, reputation protection, risk management.

Detail Position – not important in the exam.

- Chief Information Security Officer (**CISO**)
  - Communicate Risks to Executive Management
  - Maintain business relationships
  - Manage Security Budget and resource
  - Setup Metric & Measurement for improvement
  - Establishing Information security strategies
    - Strategic Planning (> 3 years)
      - Example: Establish polices, promote user awareness
    - Tactical Planning (1-3 years)
      - Example: Implementing Hot site, Identity mgt solution
    - Operational & Project Planning (within 1 year)
      - Example: conduct risk mgt, develop policies, train end-users, Monitor compliance

Detail Position – not important in the exam.

- Chief Information Security Officer (**CISO**)
  - Reporting Models (ie. Reporting to?):
    - **CEO**: reduce filtering, ideal structure
    - **IT**: technology driven, but conflict of interest
    - **Corporate Security**: mainly physical security
    - **Administrative or HR**: more difficult to understand boh business and security, and to communicate technical solutions to senior management
    - **Risk Management**: similar direction, but not technical
    - Internal audit: conflict of interest
    - **Legal**: good in regulated industries

Detail Position – not important in the exam.

- **IS Security Steering committee**: responsible for making decision on tactical and strategic security issues.
  - including CEO, CFO, CIO department managers, internal audit etc.
  - meet at least quarterly
  - See ebook for the list of responsibilities
- **Audit Committee**: appointed by board of directors to review and evaluate internal operations, internal audit system, financial reporting…
- **Data Owner** (or information owner): usually in charge of a business unit and is responsible for the protection and use of specific subset of information.
  - Have to do data classification
  - ensuring necessary security controls are in place
  - approve of access, disclosure, backup requirement,
  - is not technical role, but business role
  - can delegates responsibility of day-to-day maintenance of the data protection mechanisms to data custodian

Detail Position – not important in the exam.

- **Data Custodian** (or information custodian): responsible for maintaining and protecting the data.
  - usually by IT or security department
  - including performing regular backup, periodically validating integrity, restore, retaining records of activity, follow security policy, standard….
- **System Owner:**
  - responsible for integrating security consideration in application and system purchase decisions development projects
  - also ensuring adequate security controls, password management, remote access controls operation system configuration.
  - Also ensuring assess for vulnerabilities and must report incident response team and data owner.
  - different from data owner
- **Security Administrator**
  - not just holding root or administrator password
  - creating new system user accounts
  - implementing new security software
  - issuing new password

Detail Position – not important in the exam.

- **Security Analyst**
  - strategic level
  - helps develop policy, guideline, baseline…
  - helps define the security program elements
  - more on design level than implementation level
- **Application Owner**
  - usually business unit manager for business unit specific application (such as accounting)
  - Responsible for user access right
  - responsible for the security of unit’s application, including test, patch, change control, any other protection control to the application
- **Supervisor (or user manager)**
  - responsible for user activity, assets created and owned by users
  - responsible to security, distributing initial password, user account information update
  - inform security administrator about employee termination, transfer, new hire, access right change

Detail Position – not important in the exam.

- **Change Control Analyst**
  - responsible for approving or rejecting request of change
  - make sure the change is not vulnerabilities, is tested, is roll out properly
  - need to understand the change impact
- **Data Analyst**
  - responsible for ensuring data stored making most sense
  - responsible for architecting new system or advise the purchase
- **Process Owner**
  - Responsible for defining improving and monitoring the process (including business process)
  - Not necessary form one dept
  - Complex process involves many different dept, technologies and data types.
- **Solution Provider**
  - external to the company (eg. PKI solution provider)
  - works with business unit manager, data owner and senior management to develop and deploy solution for the company

Detail Position – not important in the exam.

- **User**
  - use data for work
  - follow operation security procedure to ensure data's C I A
- **Product Line Manager**
  - not company produced product, but external product
  - search right product for company
  - ensuring compliance to license agreement
  - spell requirement etc. to producer
  - product version
- **Auditor**
  - provide a method for ensuring independently that management and shareholders of an organization can rely upon the appropriateness of security objectives and information reporting
- **Personnel**
  - people (or staff) is important, but also is weakest link in security circles
  - solutions: hiring most qualified, background checks, Job description, training, access control, termination procedure

Question

Who is ultimately responsible for making sure data is classified and protected?

A. Data owners

B. Users

C. Administrators

D. Management

B4. Control Frameworks

- **Security Administration and Supporting control**
  - **What is Control**: an action to reduce the risk (say install sprinkler to reduce the risk of fire, input validation to reduce of risk of human error)
  - **Example** of Control Frameworks
    - National Institute of Standards and Technology’s Special Publication 800-53r4: 285 controls in 19 families
    - International Standard Organization (ISO) 27001:2013 Standard

B5 & B6: Due Diligence and Due Care

- **Due Care and Due Diligence**
  - **Due Diligence** (do detect): the act of investigating and understanding the risks the company faces
    - More **preemptive** than Due Care
    - **Example:** background check of employees, Credit check of business partner, penetration test, risk assessment, contingency testing, ….
  - **Due Care** (do correct): to exercise and by developing and implementing security policy, procedure and standard
  - legally charged with negligence in most of countries

C. Compliance

- GRC: Coordination of Governance, Risk management Compliance
  - **Governance**: ensure business focus on core activities
  - **Risk Management**: Identify, analyze, evaluate, remediate and monitor risk
  - **Compliance**: ensure behavior complies with established rules
    1. Legislative & Regulatory Compliance
    2. Privacy Requirement Compliance

C. Compliance

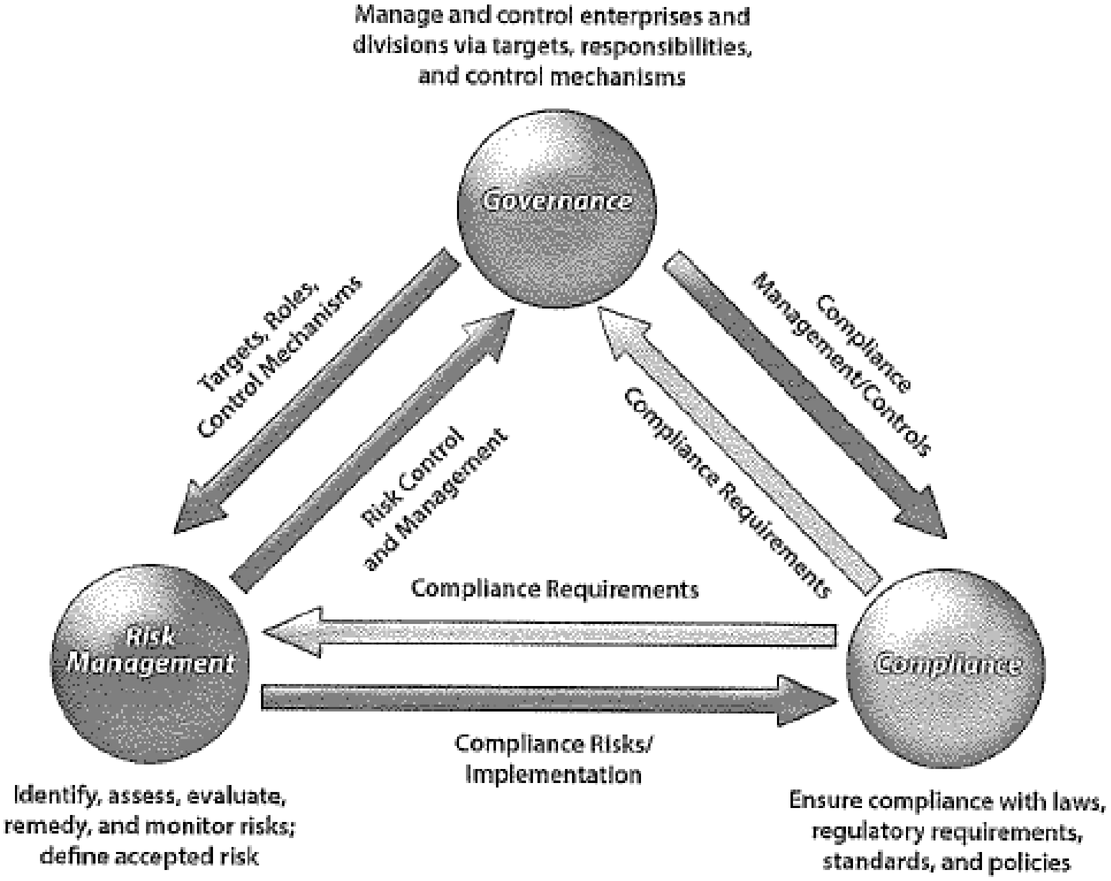

Manage and control enterprises and divisions via targets, responsibilities, and control mechanisms
Governance
Targets, Roles, Control Mechanisms
Risk Control and Management
Compliance Requirements
Compliance Management/Controls
Compliance Requirements
Risk Management
Compliance
Compliance Risks/ Implementation
Identify, assess, evaluate, remedy, and monitor risks; define accepted risk
Ensure compliance with laws, regulatory requirements, standards, and policies

Figure 1.6 – **GRC overview** *

D. Understand legal and regulatory issues that pertain to information security in global context

D1. Computer Crimes

- **Computer / Cyber Crime**:
  - Virus, Spyware, phishing, Fraud Scheme, hacking, Child Pornography, etc.
- **Difficult to prosecute**
  - The law is behind the technology, and information is intangible asset
  - Complexities in Cybercrime
  - Hacker can cover the footsteps by cleaning the log and use spoof ID etc.
  - Use innocent’s resources, such zombies
  - Organization may not report for reputation reason

D2. Licensing & intellectual property

- **Intellectual Property Laws**
  - common type of Intellectual Property are Trade secret, copyright, trademark, patent, software piracy
- **Trade Secret:**
  - protects certain type of information or resources from unauthorized use or disclosure
  - something is proprietary to a company and **important for its survival and profitability**
  - example: formula for soft drink
  - company gets employee to **sign NDA**, company reserves the right to fire employee, if employee disclose trade secret

IP

- **Copyright**
  - In many countries, it protects the right of author to control the public distribution, reproduction, display and adaptation of his original work.
  - Many categories: pictorial, graphic, musical, dramatic literary…..
  - Usually protect author’s writing, artist’s drawing or programmer’s source code
  - Extend to program and manual, user interface
  - *Does not* extend to any method of operations, process, concept or procedure, but *still protect* unauthorized copying and distribution of a work.
- **Trademark**
  - protect a word, name, symbol, sound, shape, color or combination of these
  - ensuring others **cannot copy and use it**

IP

- **Patent**
  - to grant legal ownership of invention
  - enable them to exclude others from using or copying the invention covered by the patent
  - time limit
  - may sell the right to use
- **Software Piracy**
  - vendor develops application, profit from license,
  - License agreement contains provision relating to the use and security of the software and manuals
  - Common security issues: employees use the company’s SW for their home use; decompile vendor object code for (1) attack or (2) modify the function to decrease the security
- **Internal Protection of Intellectual Property**
  - company has to ensure necessary level of access control protection, auditing enabled and a proper storage environment. If not, may not able to sue the employee who disclosed the information.
  - according to the company’s classification

D3. Import/Export Controls

- Need to understand the legal or regulation pertained the import/export controls
- **For example,** firearms, explosives, bombs and rockets, tanks and toxicological agents, etc., and equipment and technology for the production of these weapons
- Sometimes, license or quota is required to perform import/export

D4. Trans-border Data Flow

- = Transfer of computerized data across national borders
- **categories: (Example)**
  - personal data,
  - business data,
  - technical data,
  - organizational data
- **Violations:**
  - Internet Hacking
  - Attacks on ISP
- **Various Types of Security:**
  - **Network Protection** - Firewall
  - **Host and Server Protection** - access control
  - **Data Protection** - encryption of files and data on disks
  - **Assessment/Compliance and Intrusion Detection**
  - **Desktop Security** - antivirus, code protection
  - **Authentication and Certificates**
  - **Central Management and Single Sign-On**

D5 & D6. Data Breaches & Privacy

- **Privacy**: Talking about protecting Personally Identifiable Information (PII) etc., about law, purpose, secure, retention…

- **Data Breach** = Data Leaking = Data Spill
- = Intentional or unintentional release of secure information to an untrusted environment
- Being copied, transmitted, viewed, stolen or used by unauthorized individual

E. Understand professional ethics

E1. Exercise (ISC)2 Code of Professional Ethics

- **Ethics**
  - read the full version of code of Ethics before the CISSP exam
  - http://www.isc2.org/ethics/default.aspx
  - Mainly address:
    - Protect society, the commonwealth, and the infrastructure.
    - Act honorably, honestly, justly, responsibly, and legally.
    - Provide diligent and competent service to principals.
    - Advance and protect the profession.

E2. Support organization’s Code of Ethics

- Organization must promote a culture of ethical computer use within organization.
- **Golden Rule**: Treat others as you wish to be treated. For example, “Is your company using unlicensed software although your company itself sells software?”

Questions

If your company gives you a new PC and you find residual information about confidential company issues, what should you do based on the (ISC)^2 Code of Ethics?

A. Contact the owner of the file and inform him about it. Copy it to a disk, give it to him, and delete your copy

B. Delete the document because it was not meant for you

C. Inform management of your findings so it can make sure this type of thing does not happen again

D. E-mail it to both the author and management so everyone is aware of what is going on

F. Develop and implement documented security policy, standards, procedures, and guidelines

- **Policy**
  - Senior Management’s statement, the role of security plays
  - State “Why”
  - Policy in **broad term** to cover many subjects in a general fashion, more detail in procedure, standard and guideline
  - Technology and solution independent
  - Tiering:
    - **Tier 1: Organizational security policy**: program setup, goals, responsibilities, strategic, tactical, law, regulation, liability, scope, direction
    - **Tier 2: Issue-specific policy (or functional implementing policy)**: to address specific issue, for example email monitoring policy to specific what mgt can do and cannot do.
    - **Tier 3: System Specific Policy**: Example HR system; HR DB etc.

Policy, Standard, Guideline and procedure

- **Standards**
  - mandatory activities, actions or rules
  - support policy’s reinforcement in direction
  - internal or external
  - to specific technology, application, parameters and procedure
  - uniform manner a cross the organization
  - **example**, wearing badges, encryption

Policy, Standard, Guideline and procedure

- **Guidelines**
  - recommended actions and operation guides to user, IT staff, operation staff and others
  - when no standard apply; gray areas exist
  - methodologies of technology, personnel or physical security
  - **Example**: To avoid splitting the wood, a pilot hole should be drilled first
  - standard more mandatory rules, guideline is general approach, more flexible

Policy, Standard, Guideline and procedure

- **Procedures**
  - detailed step-by-step task
  - can apply to many group of staff
  - example: how to install O/S, configure, setup user account
  - lowest level in the policy chain, spell out how policy, standard and guideline are implemented

Policy, Standard, Guideline and procedure

- **Modular Elements**
  - separation of documentation for diff purpose and audience
  - Modular enables the distribution and update easier
- **Implementation**
  - not for audit purpose only
  - visibility
  - awareness training, manual, presentation, newsletter and legal banner
  - senior mgt direction, management support, employee’s understanding and expectation for non-compliance

Questions

What are security policies?

A. Step-by-step directions on how to accomplish security tasks

B. General guidelines used to accomplish a specific security level

C. Broad, high-level statements from the management

D. Detailed documents explaining how security incidents should be handled

G. Understand Business Continuity Requirements

G1. Develop and document project scope & plan

- BCP provides method and procedures for dealing with longer-term outages and disaster
- May not be IT focused
- Include:
  - Response to **emergency situation**
  - **Protect life and ensure safety**
  - Reduce business impact
  - **Resume critical** business functions
  - Work with outside vendors
  - Ensure survivability of business
  - Get “up and running” quickly after a disaster
  - procedure how to work in diff environment
  - getting right **people** to right place
  - **dealing with customer, partners, shareholders**

Business Continuity Planning (BCP)

- **Why need BCP?**
  - Letting business partners, shareholder, boards, customer, etc. know the company is prepared
  - Regulation
- **Main concerns**
  - Controlled and ***secure* manner**, such as access control
  - Integrity of data and system in a ***reduced capacity***
  - Configure and operate **IT equipment**
  - Understand how to perform process from automatically *to **manually***

Business Continuity Steps

Different company may have slightly different steps

1. Project Initiation and Management
2. Risk Evaluation and Control (understand the organization)
3. BIA (**B**usiness **I**mpact **A**nalysis)
4. Developing Business Continuity Strategy
5. Emergency Response and Operations
6. Developing and implementing Business Continuity Plans
7. Awareness and Training Programs
8. Maintaining and exercising Business Continuity Plans
9. Public Relations and Crisis Communication
10. Coordination with Public Authorities

Questions

What is one of the first steps in developing a business continuity plan?

A. Identify backup solution

B. Decide whether the company needs to perform a walk-through, parallel, or simulation test

C. Perform a business impact analysis

D. Develop a business resumption plan

What is the most crucial piece of developing a business continuity plan?

A. Business impact analysis

B. Implementation, testing, and following through

C. Participation from each and every department

D. Management support

BCP

- **Project Initiation**
  - identify “**Business Continuity Coordinator**” who leads BCP team and oversees development, implementation and testing
  - establish **BCP Committee**: include *at least* Business unit, senior management, IT, security, communication and Legal etc.
  - develop “**Continuity Planning Policy Statement**”, including scope, goal, role etc.
  - **Project management skill**: Objective-to-task, Resource-to-task, Milestone, budget, success factors, deadline

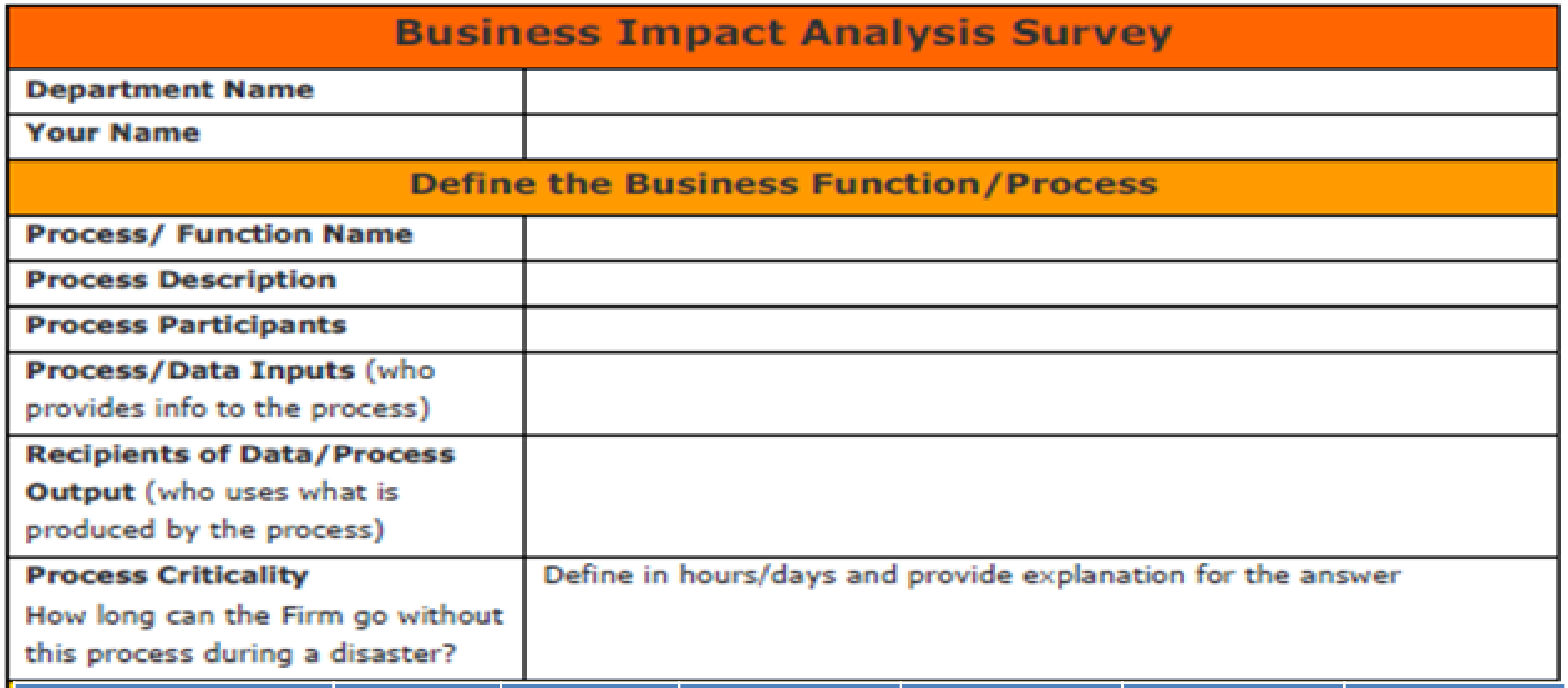
G2. Conduct Business Impact Analysis (BIA)

- **Business Impact Analysis (BIA)**
  - also called **functional analysis**
  - to **collect data** of each business unit about their processes, classification, tolerable downtime, financial consideration, regulatory responsibilities, reputation…
  - through **interviews** and documentary sources

BCP

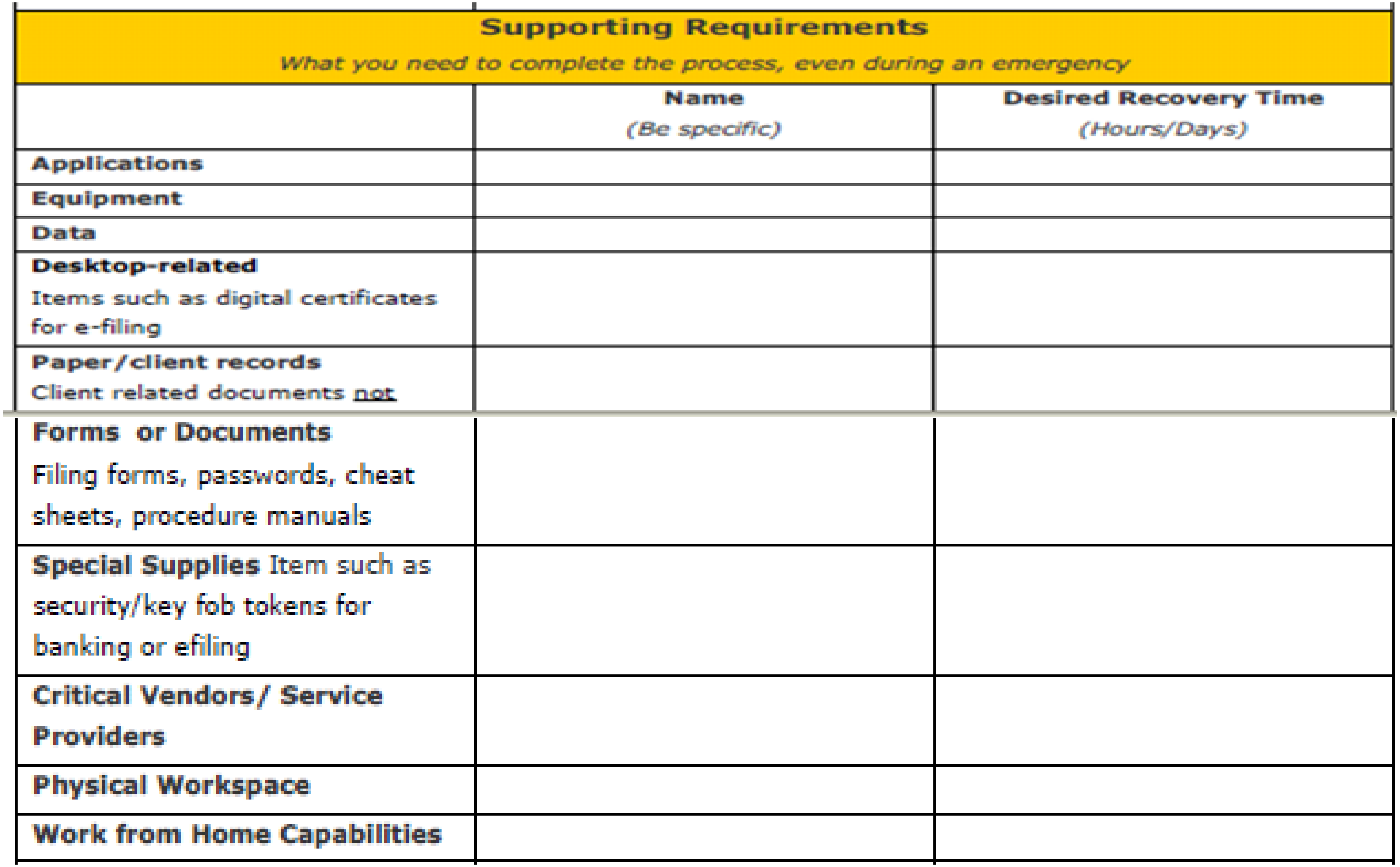
- **BIA steps:**
  1. Select interviewer
  2. Create data-gathering techniques (survey, questionnaires, qualitative or quantitative..)
  3. **Identify critical business function**
  4. Identify **resources** these functions depend upon
  5. Calculate how long these functions can survive without these resources
  6. Identify vulnerabilities and threats
  7. Calculate Risk for each unit
  8. **Document** finding and **report to management**

First Time BIA Sample



Business Impact Analysis Survey	
Department Name	
Your Name	
Define the Business Function/Process	
Process/ Function Name	
Process Description	
Process Participants	
Process/Data Inputs (who provides info to the process)	
Recipients of Data/Process Output (who uses what is produced by the process)	
Process Criticality How long can the Firm go without this process during a disaster?	Define in hours/days and provide explanation for the answer

	1 hour	4 hours	8 hours	1 day	1 week	1 month
Financial	10k	20k	100k	150k	500k	1M
Customer Service	G	G	A	A	R	R
Reputation	G	A	A	R	R	R



Supporting Requirements

What you need to complete the process, even during an emergency

	Name *(Be specific)*	**Desired Recovery Time** *(Hours/Days)*
Applications		
Equipment		
Data		
Desktop-related Items such as digital certificates for e-filing		
Paper/client records Client related documents <u>not</u>		
Forms or Documents Filing forms, passwords, cheat sheets, procedure manuals		
Special Supplies Item such as security/key fob tokens for banking or efiling		
Critical Vendors/ Service Providers		
Physical Workspace		
Work from Home Capabilities		

BCP Frameworks

- Maximum Tolerable Downtime (MTD)
  - By application
  - The amount of time organization can function without that application before significant impact
- Recovery Time Objective (RTO)
  - Example: take 4 hours to restore and resume the application
- Recovery Point Objective (RPO)
  - The point in time to recover to, say restore last Friday weekly backup may loss maximum of 1 week of data.

Other BCP Frameworks

ISO

- ISO 22301
  - Requirements for Business Continuity Management System
- ISO 24762
  - ICT Disaster Recovery
    - ICT = Information and communications technology

Question

Which item will a business impact analysis not identify?

A. Whether the company is best suited for a parallel or full-interrupt test

B. What areas would suffer the greatest operational and financial loss in the event of a particular disaster or disruption

C. What systems are critical for the company and must be highly protected

D. What amount of outage time a company can endure before it is permanently crippled

H. Contribute to Personnel Security Policies
H1. Employment candidate screening

- **Structure**
  - include **clear** responsibilities, line of authority, activities
- **Hiring Practices**
  - HR process, right people, right skill
  - **Employment Candidate Screening**: Reference Check, Background Investigation, Credit History, Criminal History, Driving Record, Drug & Substance testing, Prior Employment, Education, Licensing and Certification verification, Social Security Number verification and validation, Suspected Terrorist Watch list etc.
  - **Timing of check**: Hard to carry those checks after hiring
  - **Benefit**: mitigate risk, lower hiring cost, lower turnover rate

H2 & H3: Employment Policies & Termination

- **Employment Agreements & Policies**
  - **Job Rotation** (or Rotation of duties or Rotation of assignments): prevent key man dependency
  - **Mandatory vocation**: of a specified consecutive-day (1-2 weeks), not allow to perform the job functions and remote access is disabled as well, Mainly detect fault or irregularities, sometimes can prevent key man dependency,
  - **Separation (Segregation) of duties (SoD)**: dual or multi-layer control to prevent fraud (**Example**: Tx processing with different input, check and approve staff, Dual signatures on the cheque, Programmer cannot touch production env.). **Collusion** may compromise SoD.
  - **Least Privilege (Need to Know):** granting least access that are required to perform job functions.

H2 & H3: Employment Policies & Termination

- **Termination**
  - **Friendly** Terminations / **Unfriendly** Terminations
  - different reactions: different set of procedures
  - Return of asset, revoke of access
  - Require **Exit Meeting** about continued responsibility for confidentiality of information
  - sounds cold and difficult, but necessary

H4-6. Vendor, Consultant, Contractor controls

- **Issues:**
  - Different risk, different objective than internal employee's
  - You can transfer the work and service to third parties, but not the ultimate risk
- **Compliance:**
  - Provide minimum Security Requirement (physical and logical)
  - NDA, Contract, SLA, SOW
  - **Regular review**
  - Escort, background check, virtually monitoring,
- **Privacy:**
  - All individuals have expectation of privacy, but varies by culture and people. Example, CCTV in working area are acceptable, but not in washroom, locker room etc.
  - Security profession must understand the expectation and privacy requirement. One of solutions is to mention in privacy policy.

I. Understand & apply Risk Management concept

I1. Identify Threats and vulnerabilities

Security Definitions (Risk related)

- **Threat**: the occurrence of event which could have an undesirable impact on the well-being of asset; the danger such as Fire, HW or SW failure, Terrorist
- **Vulnerability**: SW, HW or procedural weakness provides attacker the open door
  - **Cause of Threat, say someone smoke to cause fire, Absence of Patch Management, Absence of security guard**
- **Threat Agent**: someone or something identify vulnerability and use it against the company
- **Likelihood:** probability of occurrence
- **Impact (or Exposure)**: instance of being exposed to loss from a specific threat
- **Risk (or Risk Level) =** Likelihood X Impact
- **Countermeasure** = **Measure** = **Safeguard** = **Control**

Information Risk Management

- **IRM** is process of identifying, assessing risk, reducing to acceptable level and implementing mechanism to maintain that level
  - risk is company specific, not all computer related.
  - example of categories: Human interaction; equipment malfunction; Inside and outside attacks; misuse of data, loss of data; application error.
  - Espionage = spy
  - Accuracy is impossible, prioritizing is possible
  - IRM is before-the-fact

Risk Assessment

Asset	Value	Threat or Vulnerability	Probability or likelihood	Impact	Control	Control cost	Recommendation
Web Server	100K	Hacking	1%	10K	IDS	5K	Not go
Web Server	100K	Hacking	1%	10K	Firewall	7K	Go
Web Program	500K	SQL Injection	L	M	Penetration test	H	Go

Information Risk Management

- **Risk Ownership**
  - no straight forward answer
  - Primary responsibility may be operation or IT etc.
  - Ultimate responsibility should be senior management.
- **The value of information and asset**
  - important to know the value of asset, to decide protection cost and time
  - related to parties involved, work required, maintain cost, lost impact, enemies pay, liability penalties…

Information Risk Management

- **Cost to make up the value**
  - quantitative or qualitative
  - consideration: acquire, maintain, value to owner & user, adversaries (enemy) intellectual property, replace, impact, liability, usefulness, loss of productivity
  - why: cost/benefit analyses, selection of safeguards, insurance cost, understand risk impact, legal requirement
  - tangible: computer, facilities…
  - intangible: reputation, data, intellectual property

I2. Risk Assessment/Analysis

- **Quantitative Risk Analysis**
  - Assign percentage, dollar amount etc. to all elements of risk analysis process (safeguard cost, asset value….probability….
  - Purely quantitative is not possible, because not everything is quantifiable
  - Advantage: good decision making tools
  - Disadvantage: high afford
- **Qualitative Risk Analysis**
  - no calculation, more opinion and scenario based
  - example: **Delphi**, brainstorming, storyboarding, focus groups, survey, questionnaire checklist, one-on-one meeting and interview.
  - Scale can be HML, or 1 to 5 or 1 to 10
- **Quantitative vs qualitative**
  - afford vs result
- **Results of risk analysis**
  - reviewed and signed by management;
  - demonstration of due diligence and due care

Information Risk Management

- **Other terms**
  - **Exposure factor (EF)** : Percentage of loss, (eg. 95% lost at Fire)
  - **SLE: Single loss expectancy** (eg. Lost a notebook cost 10k or Fire costs 1 million)
  - **ARO: Annualized rate of occurrence** (eg. Lost 5 notebooks in one year; Fire in 10 years = 0.1)
  - **ALE: Annualized loss expectancy** (eg. 50k for notebook; 100k for fire annually)

I4. Countermeasure selection

- **Countermeasure Selection (or safeguard)**
  - Make good business sense or cost-effective or benefit outweighs its cost
  - ALE before – ALE after – cost = value of safeguard
  - 100,000 – 50,000 – 20,000 = 30,000 (sprinkler head)
  - Full cost should be considered
- **Total Risk vs Residual Risk**
  - Total risk: if no safeguard
  - Residual risk: always some risks left over to deal with.

I3. Risk assignment/acceptance

- **Handling Risk**
  - 4 types of countermeasures
    - **Transfer (or share)**: insurance or outsourcing
    - **Avoidance**: avoid process (not use IM), person or location (move data center)
    - **Mitigation**: risk is decreased to a acceptable level, eg. Firewall, training, intrusion detection…
    - **Acceptance**: understand the risk and accept, different from risk ignorance
      - accepting risk: (1) acceptable level (2) countermeasure costs more than potential loss (need to consider intangible factor, such as reputation, life, health etc.)

15. Implementation

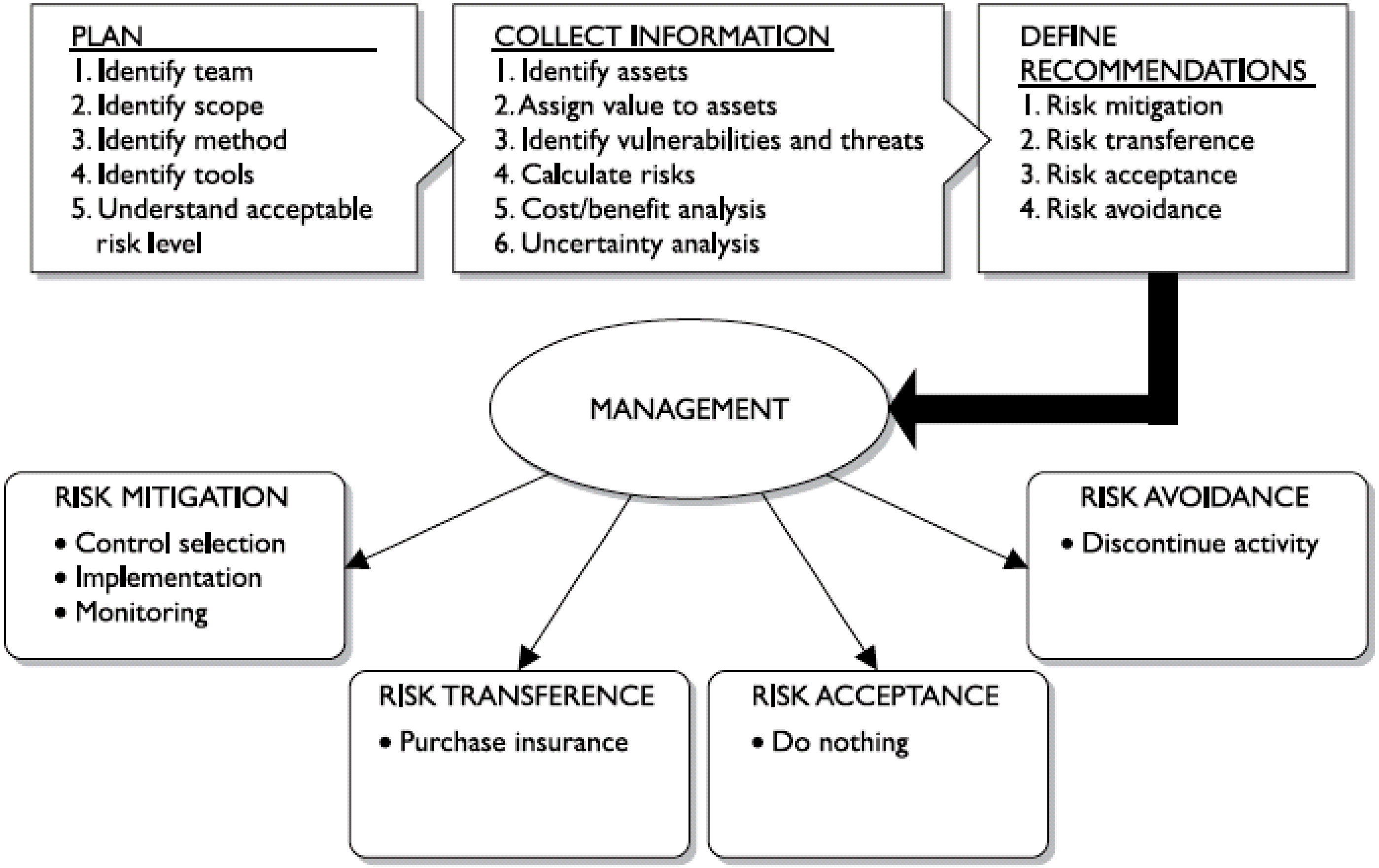


Figure 3-10 How a risk management program can be set up

I6: Type of Controls

7 types of controls

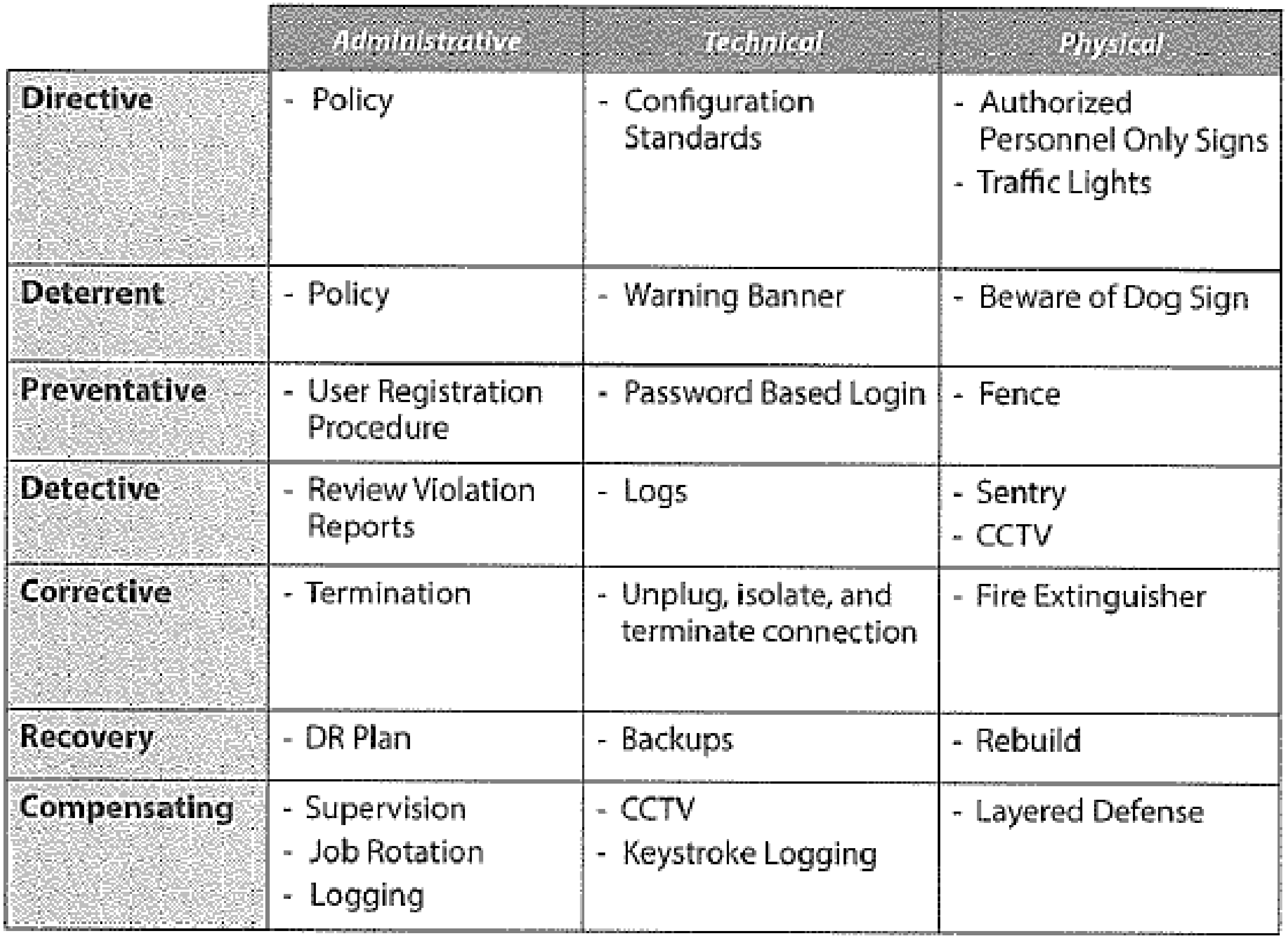
- **Deterrent:** Intended to discourage a potential attacker (Sign, Fence, lighting)
- **Preventive**: intended to avoid an incident from occurring (lock, security guard)
- **Corrective**: Fixes components after an incident has occurred (Antivirus, server image)
- **Recovery**: Intended to bring control back to regular operations (data restore, activate BCP)
- **Detective**: Help to identify an incident’s activities (IDS)
- **Compensating**: controls that provide for an alternative measure of control (guard is too expense, so use fence, lock…)
- **Directive**: Mandatory controls, due to regulations or environmental requirement (BCP for bank)

- Plan preventive first, able to detect quickly, then corrective action.

B4. Control Frameworks

- **Access Control Types**
  - **Administrative** control (or Management Control): use of policy, procedure, Personnel security, Monitoring, User Management, Privilege management, training etc. (say issue memo to prohibit smoking in office)
  - **Technical** control (or logical control): electronic hardware and software to control Network access, remote access, system access, application access, Malware control, Encryption, etc.
  - **Physical** control (or Operational Control): to protect people and physical environment, such as locks, fire management, gates, guards

7 X 3 = 21



	Administrative	*Technical*	*Physical*
Directive	- Policy	- Configuration Standards	- Authorized Personnel Only Signs - Traffic Lights
Deterrent	- Policy	- Warning Banner	- Beware of Dog Sign
Preventative	- User Registration Procedure	- Password Based Login	- Fence
Detective	- Review Violation Reports	- Logs	- Sentry - CCTV
Corrective	- Termination	- Unplug, isolate, and terminate connection	- Fire Extinguisher
Recovery	- DR Plan	- Backups	- Rebuild
Compensating	- Supervision - Job Rotation - Logging	- CCTV - Keystroke Logging	- Layered Defense

I7 to I8: Control assessment, monitoring & measurement

- Why?
  - Evidence about effectiveness
  - An indication of quality
- How? (by tools)
  - **Vulnerability Assessment**: to seek vulnerability from physical, network, procedure etc.
  - **Penetration Testing** (or ethical hacking, tiger teaming, red teaming vulnerability test): simulate an attack
  - **Application Security Testing**: example, encryption, authentication….
  - **Denial-of-Service (DoS) Testing**: should not test on live production
  - **War Dialing**: seek modem from a range of telephone numbers
  - **Wireless Network Testing**: vulnerable to wired network
  - **Social Engineering**: to employee, suppliers, contractors etc.to gather information for hacking
  - **PBX and IP Telephony Testing**

I7 to I8: Control assessment, monitoring & measurement

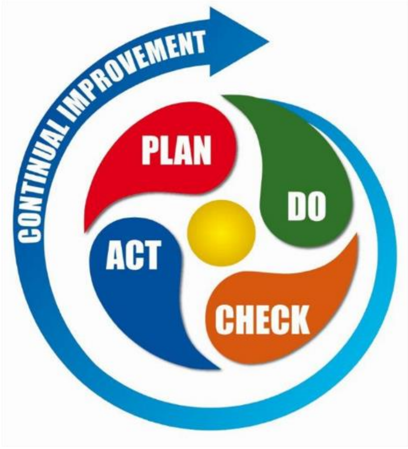
- Penetration Test Methodology
  1. **Reconnaissance / Discovery** – Identify and document information about the target.
  2. **Enumeration** – Gain more information with intrusive method.
  3. **Vulnerability Analysis** – Map the environment profile to known vulnerabilities
  4. **Execution** - Attempt to gain user and privileged access.
  5. **Document Findings** – Document the results of the test.

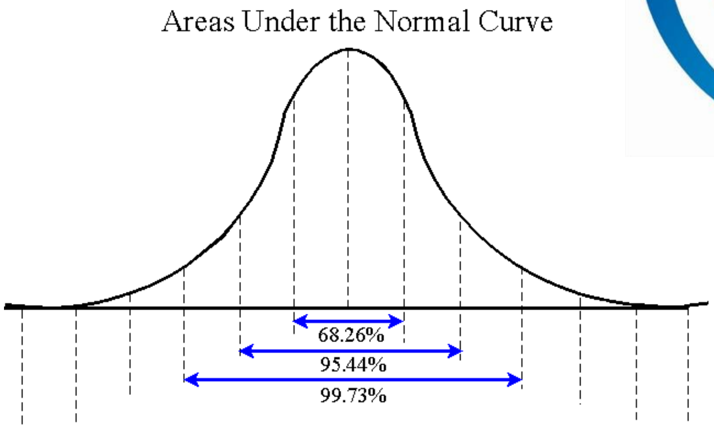
I9 to I10: Asset valuation & Reporting

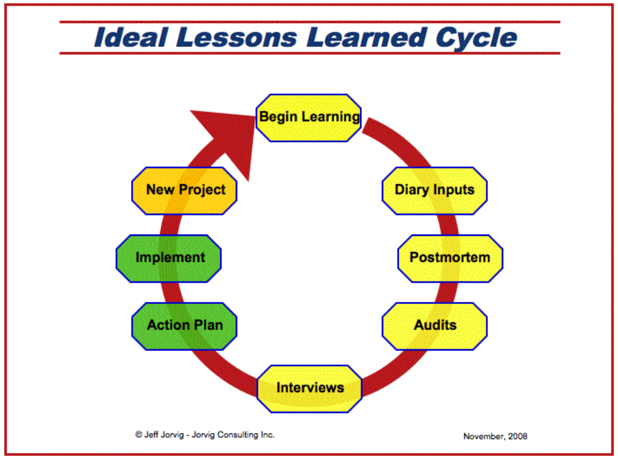
- Asset valuation
  - To understand the value -> to fund in protection
  - **Tangible**: have a physical presence, server etc.
  - **Intangible**: Trademarks, Patents, Copyrights, Business processes, Brand recognition.
  - Think widely
- Reporting
  - Allow company to understand the current situation in Risk
  - Periodical or
  - Event Driven: say Avian Flu alert arose

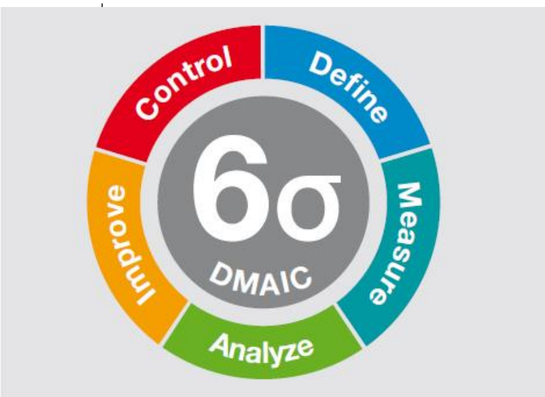
I11: Continuous improvement

- Some models:
  - PDCA: Plan Do Check Act
  - Six sigma: 3.4 defects per million
  - Lesson Learnt





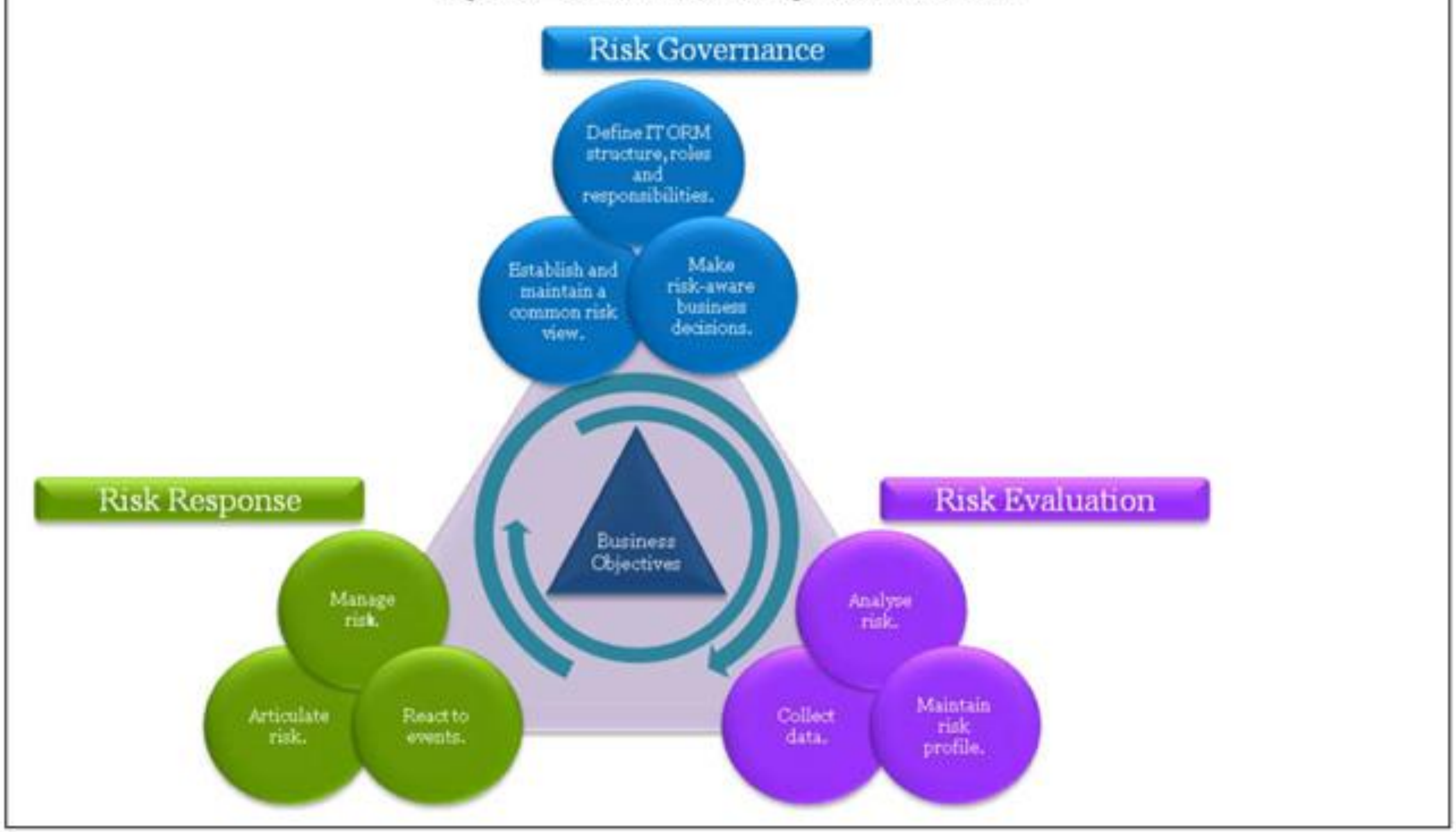




I12. Risk Frameworks

1. IT Risk Management Framework

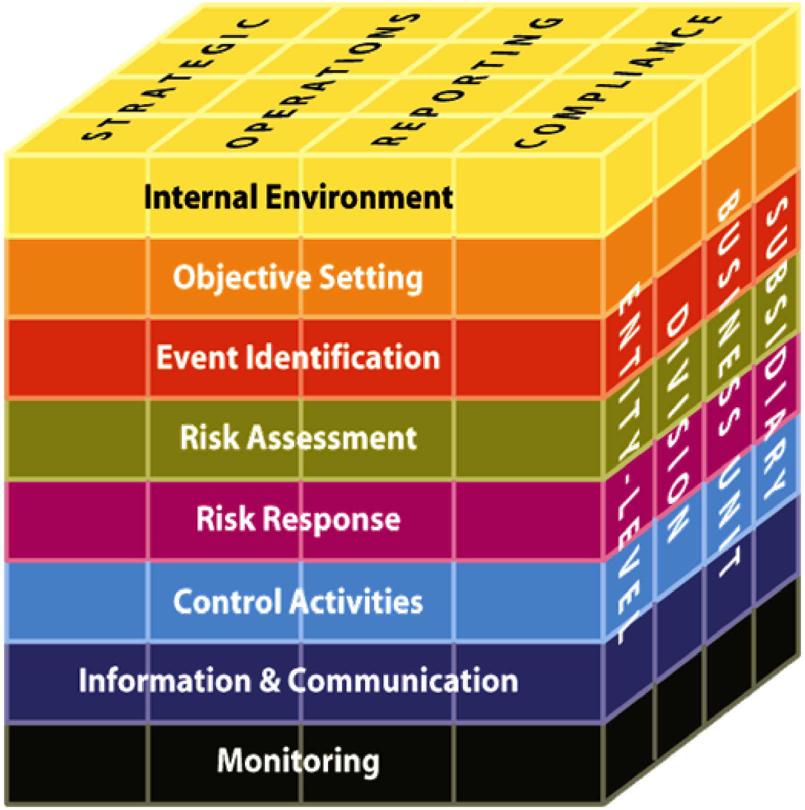
Figure 3—NSE's IT Risk Management Framework



Risk Frameworks

2. COSO ERM:

The Committee of Sponsoring Organizations – Enterprise Risk Management



Risk Frameworks

3. CRISC:

Certified in Risk and Information System Control

Risk Frameworks

4. ISO

- ISO 31000: Generic Risk Management Framework
- ISO/IEC 27005: IT Risk Management Framework

J. Understand & apply Threat Modeling

J.1 Identifying threats

1. **Assessment Scope** - like databases of information or sensitive files and value them in tangible and intangible ways.
2. **Identify Threat Agents and possible Attacks** – identify different groups of people who might be able to attack your application. These groups should include insiders and outsiders, intentionally or unintentionally.
3. **Understand existing Countermeasures** - The model must include the analysis of the existing countermeasures
4. **Identify exploitable Vulnerabilities** - analyze for new vulnerabilities which may cause negative consequences.
5. **Prioritized identified risks** - Prioritization is everything in threat modeling, as there are always lots of risks that simply don't rate any attention. For each threat, you estimate a number of likelihood and impact factors to determine an overall risk or severity level.
6. **Identify Countermeasures to reduce threat** - The last step is to identify countermeasures to reduce the risk to acceptable levels.

J.2 Determining and diagramming potential attacks

- **Social Engineering Attack:** use social skill to obtain info
- **Pretexting Attack:** use invented scenario or lie (pretext) which involves some prior research (ie date of birth, ID number, last bill amount etc.)
- **Phishing Attack:** Malicious email or website seemingly from a reputable organization, often suggesting a problem.
- **Baiting Attack:** leave a malware infected CD or USB (with curiosity-label) in public location, wait for victim to use.
- **Tailgating Attack:** walk in behind an authorized people thru a secured entrance.

J.3 Performing reduction Analysis
J.4 Technologies and processes to remediate threat

- **Some open-ended questions**
  - How Does an Individual Avoid Being a Victim?
  - How can Organizations reduce their security risks?

- **Technologies**: Network security….
- **Process**: procedure, training, awareness….

Questions

Which is the most valuable technique when determining if a specific security control should be implemented?

A. Risk analysis

B. Cost/benefit analysis

C. ALE results

D. Identifying the vulnerabilities and threats causing the risk

Which best describes the purpose of the ALE calculation?

A. Quantifies the security level of the environment

B. Estimates the loss possible for a countermeasure

C. Quantifies the cost/benefit result

D. Estimates the loss potential of a threat in a span of a year

Questions

Which of the following is not a purpose of doing a risk analysis?

A. Delegating responsibility

B. Quantifying the impact of potential threats

C. Identifying risks

D. Defining the balance between the impact of a risk and the cost of the necessary countermeasure

Why is a truly quantitative risk analysis not possible to achieve?

A. It *is* possible, which is why it is used

B. It assigns severity levels. Thus, it is hard to translate into monetary values

C. It is dealing with purely quantitative elements

D. Quantitative measures must be applied to qualitative elements

K. Integrate Security Risk + Acquisition Strategy

- **“Supply Chain”** is now extended for IT services as supplier dependent, such as Internet.
- Require to manage **Supplier risk**
  - Include cybersecurity requirements in **contract**
  - Address **training** to appropriate workforces
  - Establish **Third party management** governance, policy & procedure
- **Control**: Understand Customer’s requirement, SLA, PLA, SOW, NDA, Contract, Standard, Minimum Security Requirement, Regular review, Service Level Report, Audit or SAS70 (a Certificate for service provider)

L. Establish & manage information security education, training, and awareness

- **Security Awareness Training**
  - in order to be successful and effective, all employees should understand
  - company specific, consider culture, business nature…
  - expected responsibilities and behaviors, noncompliance consequence
- **Different types of security-awareness training**
  - at least 3 type audience: Mgt, staff, technical employee

L. Establish & manage information security education, training, and awareness

- **Training topics**
  - Corporate security policies
  - Corporate’s security programs
  - Social engineering
  - BCP
  - Emergency management
  - Risk assessment
  - Proper care and handling of security credentials, such as passwords
  - Physical security

L. Establish & manage information security education, training, and awareness

- **Training content**
  - What is a Corporate Security Policy?
  - Why is Having a Corporate Security Policy Important?
  - How does this Policy fit into my role at the Organization?
  - **What about people who say they do not have any security functions present in their current role?**
  - Do I have to comply?
  - **What are the penalties for noncompliance?**
  - **What is the effect of the Corporate policy on my work? (will it make things harder?)**
  - **Enforcement after training**

Awareness

- **Evaluating the program (awareness program)**
  - monitor and evaluated for effectiveness
  - by questionnaires and survey
  - By quiz
  - by comparing number of security incidents before/after training
- **Specialized Security Training**
  - Do not just concentrate on device and technology, but overlook training
  - people is the weakest link
  - Beware of social engineering; verify caller

B4. Control Frameworks

- **Security Administration and Supporting control**
  - **What is Control**: an action to reduce the risk (say install sprinkler to reduce the risk of fire, input validation to reduce of risk of human error)
    - **Administrative** control: use of policy, procedure, training (say issue memo to prohibit smoking in office)
    - **Technical** control (or logical control): IT mechanism, access control, Firewall, ….
    - **Physical** control: facility, locking system, perimeter, monitoring for intrusion…
  - Importance of security, not only power by technology, devices, software package…..have to balance business or people side.