Info 6010 Lesson 2
Domain 1 – Part 2
Security and Risk Management

Revision 2

Information Security Management & Network Security Architecture

FANSHAWE

Information Security & Risk Management

Discussion Topics Part Two

- Risk management
- Threat modeling
- Business continuity and disaster recovery
- Personnel security
- Security governance

Risk Management

- Risk management is the core of any business security structure
- Objective is to protect company assets
- Core components serve as foundation of a corporation's security program
- Goal is to reduce risk to acceptable level
  - Can not be reduced to zero

Information Risk Management

- An effective security program must be initiated by senior management, given appropriate level of authority, implemented, explained to all employees and monitored for effectiveness
- Because each employee comes to the company with a unique set of personal values and experiences senior management must implement a top down approach ensuring everyone understands their role in implementing an effective Security Program

Information Risk Management

- Physical Damage
  - Fire, Water, Vandalism, Power Loss, Natural Disasters
- Human Interaction
  - Accidental or intentional action or inaction
- Equipment Malfunction
  - Failure of Systems or Peripherals
- Inside and Outside Attacks
  - Hacking, Cracking, Attacking
- Misuse of data
  - Sharing trade secrets, fraud, espionage and theft
- Loss of Data
  - To unauthorized receivers
- Application error
  - Computational, input, buffer overflows

Holistic Risk Management

- Organizational tier: business as a whole – defines risk tolerance level.
- Business process tier: major functions – defines the criticality of information flows.
- Information systems tier: address risk from an information systems perspective.

Information Risk Policy Team

- Objectives of IRM Policy
  - Set objective for IRM team
  - Determine level of risk acceptable to company
  - Set formal processes of risk identification
  - Identify connection between IRM and Corporate Planning
  - Define roles and responsibilities that fall under IRM
  - Mapping of risk to internal controls
  - Set approach to change staff behaviors and resource allocation to reduce risk
  - Mapping of risks to performance, targets and budgets
  - Monitoring the effectiveness of controls

Information Risk Management

- Proper Risk Management requires commitment from senior management
- Requires a documented process
- Must support corporate mission
- Have a designated Information Risk Management Team
- A documented Information Risk Management Policy
  - IRM – Information Risk Management

Security Management Core Components

- Risk management
- Information Security Policies
  - Procedures, Standards, Guidelines
- Information classification
- Security organization
- Security education

Risk Management Process

- **Frame risk:** defines the context within which all other risk activities take place.
  What are our assumptions, constraints and priorities?
  What is the risk tolerance of senior management?

- **Assess risk:** Before action to mitigate risk can be taken, it has to be assessed.

- **Respond to risk:** Threats, vulnerabilities, and attacks vectors have been identified. Responding to the risk becomes a matter of matching resources with our prioritized set of controls in order to mitigate those risks.

- **Monitor risk:** the environment will change, new threats emerge or a new system brought new vulnerabilities hence continuously monitor the effectiveness of controls against the risks.

Threat Modeling

- Threat modeling is the process of describing feasible adverse effects on assets caused by threat sources.
- Only consider dangers that are reasonably likely to occur.
- Threat intelligence is used by the risk teams, security operations, development, and management teams.
  - Threat modeling is isolated from the larger discussion of risk assessment as it allows an organization to understand what is in the realm of the probable and not just the possible.

Identify Threats

- Some threats may be easier to identify
- Many different types of threat agents can affect different vulnerabilities
- There may be a delay before a threat or vulnerability is identified
- Some threats may affect other assets in the form of a cascading error
  - Output from one process may be used as input in second process
  - If first process output has a computational error it affects the accuracy of second process

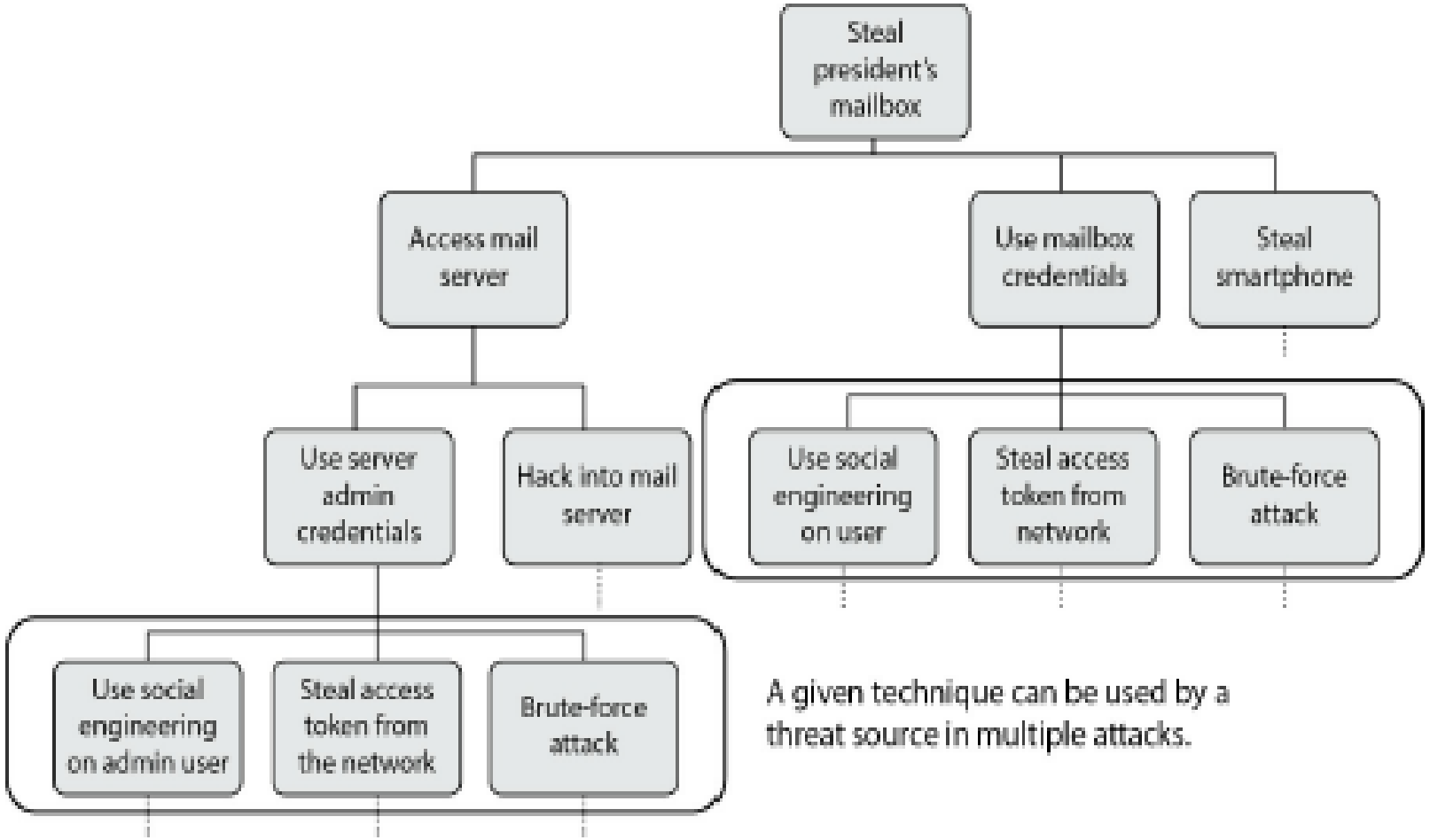
Identify Threats

- There may be a delayed loss due to a threat
  - Such loss may not always be immediate, may be delayed from few minutes to years
- Example: web server is offline
  - Online store is impacted now
    - Customers may go to competitor
    - Current and future revenue suffers
    - May impact year end bottom line
- These types of issues make identifying and qualifying threats hard

Attack Trees

- Typically, there are multiple ways to accomplish a given objective e.g. if someone wanted to steal the contents a mailbox, this could be accomplished by either accessing the e-mail server, obtaining the password, or stealing the targets laptop.
- A successful attack, then, is one in which the attacker traverses from a leaf node all the way to the root of the tree. See diagram on next slide:-

Attack Trees



Reduction Analysis

- Reduce the number of attacks to be considered, then reduce the threat posed by the attacks.
- From the previous diagram: To satisfy the conditions for logging into the mail server or the user's mailbox, an attacker can use the exact same three techniques. Thus the number of conditions requiring mitigation are reduced by finding these commonalities.
- These three sample conditions apply to a variety of other attacks, hence the number of conditions can be reduced to a manageable number.
- The second aspect of reduction analysis is the identification of ways to mitigate or negate the attacks identified.
- Each tree has one root but many leaves and internal nodes. The closer to the root when a mitigation technique is implemented the more leaf conditions will be defeated with one control. This allows easy identification of the most effective techniques to protect the entire organization.

Risk Analysis

- Risk Analysis is tool for Risk Management
- Risk Analysis is used to determine whether security is cost effective, relevant, timely and responsive to threats
- Risk Analysis helps prioritize their risks and how much money should be spent to safeguard against risks

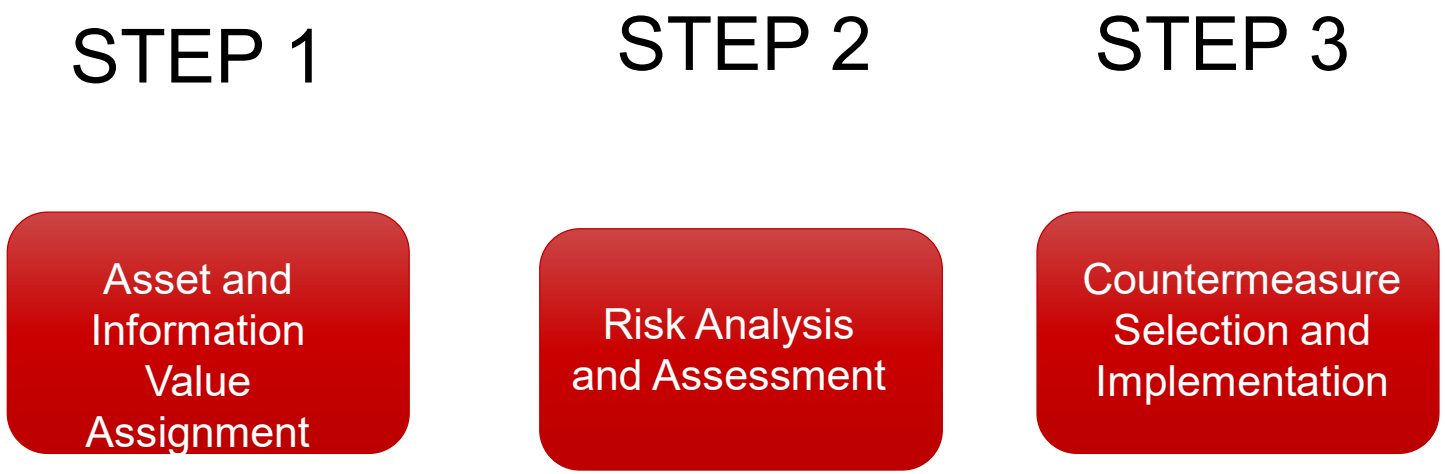
Risk Analysis

- Goal of risk analysis
  - Identify assets and their value to organization
  - Identify vulnerabilities and threats
  - Quantify the probability and impact of these threats
  - Provide economic balance between the impact and cost of countermeasure
- Risk analysis provides a COST/BENEFIT comparison
  - Return on investment for installing safeguards

Risk Analysis

- Identify assets
- Identify threats against these assets and estimates the possible damage and potential loss
- Construct a budget with the funds to protect identified assets and develop applicable security policies that provide direction for security activities
  - Return on investment (ROI)
- Security education and awareness keeps everyone properly informed and working toward the same security goal

Risk Analysis Process



Source: All-In-One CISSP Exam Guide Edition by Shon Harris

Management Responsibility

- Determine objectives, scope, policies, priorities and strategies
- Clear direction for employees to follow
- Identifying and value company's assets
- Implement security policies, procedures, standards and guidelines
- Security is not solely the responsibility of the IT department

Management Responsibility

- Security program requires a top-down approach
  - Direction from senior management through middle management to staff members
- Allocate necessary resources and funding
  - Human, capital, hardware, training
- Assign responsibilities
- Integrate into business environment
- Monitor and measure accomplishments

Information Risk Management

- Companies focus on business processes, efficiencies and generating revenue
- Very few people in business are trained in risk management
- Slowly penetrating corporate culture as security becomes recognized as a business issue

Information Risk Management

- Process of identifying and assessing risk
- Reducing it to an acceptable level
- Implementing mechanisms to maintain acceptable risk level
- Risk may come in many different forms, not all computer related
- Each risk must be identified, classified by category and evaluated
- GOAL: Evaluate potential damage to company

Risk Analysis Team

- Risk analysis team must include individuals from all departments
- Risk analysis team members must understand the processes within their own departments
- Risk analysis includes
  - What event could occur?
  - What could be the potential impact?
  - How often could it happen?
  - What level of confidence do we have to answers of above three questions?
  - Most answers to above questions is gathered through interviews, internal surveys and workshops

Information Risk Management

- Assets can have either or both a *qualitative* and *quantitative* value
- Actual value is determined by cost to acquire, develop and maintain
- Value may be determined by the importance it has to the owner or user
- Value should reflect all identifiable costs that would arise if asset were destroyed or impaired
  - Understanding true value of an asset is first step in determining what security mechanism should be in place to protect the asset

Information Risk Management – Costs That Make Up the Value

- The following should be considered when assigning value to an asset
  - Cost to acquire
  - Cost to maintain and protect
  - Value to owners and users
  - Value of asset to adversaries
  - Value of Intellectual Property during development of asset
  - Price others are willing to pay for the asset
  - Operational and production activities affected if asset is unavailable
  - Liability issues if the asset is compromised
  - Usefulness and role of the asset in the organization

Information Risk Management

- Tangible assets
  - Computers
  - Facilities
  - Supplies
- Intangible assets
  - Reputation
  - Data
  - Intellectual property
  - Difficult to put a value on intangible assets

Identifying Vulnerabilities and Threats

Threat Agent	Can Exploit This Vulnerability	Resulting in This Threat
Malware	Lack of antivirus software	Virus infection
Hacker	Powerful services running on a server	Unauthorized access to confidential information
Users	Misconfigured parameter in the operating system	System malfunction
Fire	Lack of fire extinguishers	Facility and computer damage, and possibly loss of life
Employee	Lack of training or standards enforcement Lack of auditing	Sharing mission-critical information Altering data inputs and outputs from data-processing applications
Contractor	Lax access control mechanisms	Stealing trade secrets
Attacker	Poorly written application Lack of stringent firewall settings	Conducting a buffer overflow Conducting a denial-of-service attack
Intruder	Lack of security guard	Breaking windows and stealing computers and devices

Meathodoligies for Risk Assessment

1. Prepare for the assessment.
2. Conduct the assessment:
   a. Identify threat sources and events.
   b. Identify vulnerabilities and predisposing conditions.
   c. Determine likelihood of occurrence.
   d. Determine magnitude of impact.
   e. Determine risk.
3. Communicate results.
4. Maintain assessment.

Failure Modes & Effect Analysis - FEMA

- Failure Modes and Effect Analysis – **FMEA**
  - Method for identifying functions, functional failures, causes of failures and their failure effects through a structured process
  - FMEA was first developed for systems engineering
- Application of the process helps determine where failure is most likely to occur
  - Helpful in determining where vulnerability exists
  - Helpful in determining scope of vulnerability
- Helpful in applying a corrective fix
  - Effective application of resources to resolve issue

Failure Modes & Effect Analysis

- Failure Modes and Effect Analysis – FMEA
  - Start with a block diagram
  - Consider what happens if each block fails
  - Draw up a table
    - Failures are paired with effects and evaluation of the effects
  - Correct the design and adjust table until you've removed unacceptable problems
  - Have several engineers review the failure modes and effects analysis

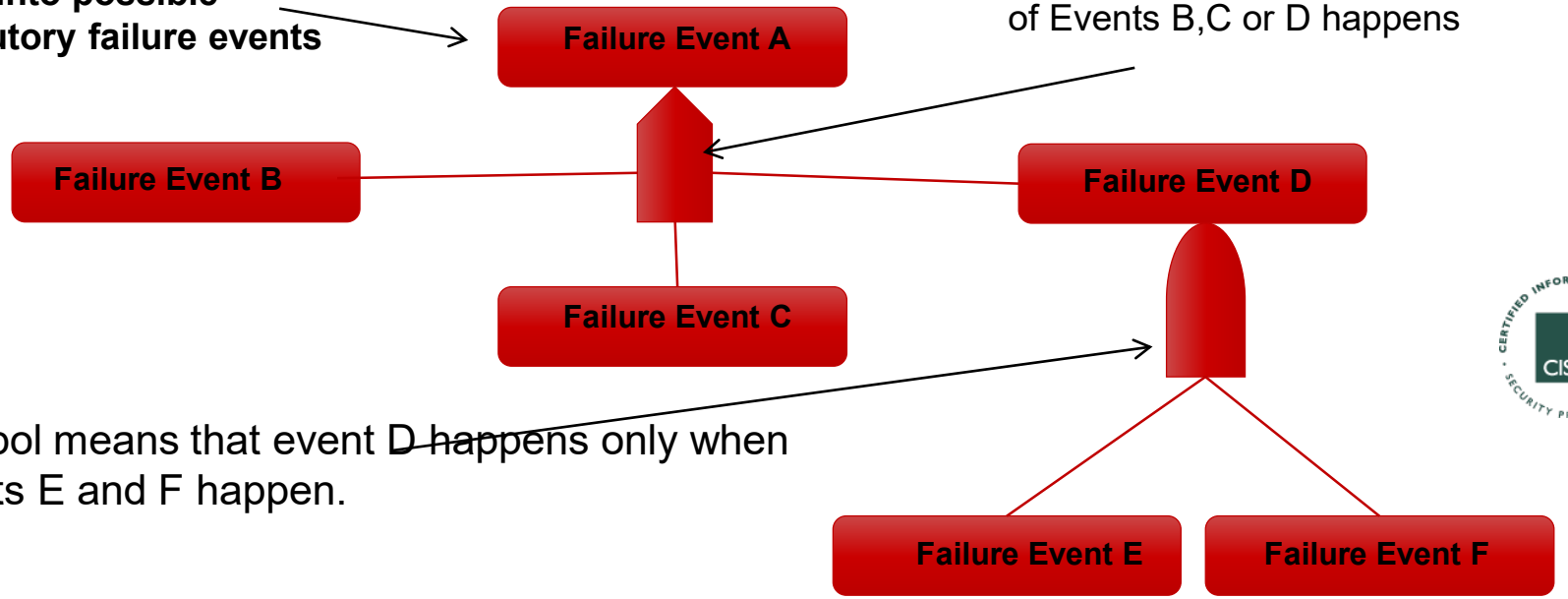
Failure Modes & Effect Analysis

Fault-Tree Analysis

- Useful in determining failures within more complex environments and systems

Top Level failure event is broken into possible contributory failure events

OR – means that Event A happens when one or more of Events B,C or D happens



AND symbol means that event D happens only when both events E and F happen.

Source: All-In-One CISSP Exam Guide 8th Edition by Shon Harris et al

Failure Modes & Effect Analysis

- Building a Fault-Tree
- List all threats or faults
- Branches can be divided into categories
  - Physical, Network, Software, Internet, Component Failure
- Prune tree by removing branches with no effect to system in question
  - If a system is not connected to the Internet you can remove entire branch

Quantitative Risk Analysis

- Assign real and meaningful numbers to all elements of risk analysis process
  - Provides concrete probability of threats
    - Physical, Network, Software, Internet, Component Failure
- Assign dollar value to risk analysis process
  - Asset value
  - Safeguard cost
  - Business impact
  - Threat frequency
  - Safeguard effectiveness
  - Exploit probabilitie**S**

Quantitative Risk Analysis

- Step 1: Assign Value to Assets
- For each asset answer the following questions
  - What is the value of the asset to the company?
  - How much does it cost to maintain?
  - How much does it make in profits?
  - How much would it be worth to my competitors?
  - How much would it cost to recreate or recover?
  - How much did it cost to acquire or develop?
  - How much liability do you face if the asset is compromised?

Quantitative Risk Analysis

- Step 2: Estimate Potential Loss per Threat
- For each asset answer the following questions
  - What physical damage could the threat cause and how much would it cost?
  - What is the value lost if confidential information is disclosed?
  - What is the cost of recovering from this threat?
  - What is the value lost if critical devices were to fail?
  - What is the **Single Loss Expectancy** (SLE) for each asset and each threat?

Quantitative Risk Analysis

- SLE = (asset value) x (exposure factor)
- EF (exposure factor) = percentage of loss
  - For example a Server room worth $100,000 is protected by a fire suppression system. You estimate 10% loss in case of fire (EF = 10% or 0.10)

Quantitative Risk Analysis

- Step 3: Perform a Threat Analysis
- Gather information from all departments about the likelihood of a threat
  - Examine past records and official security resources
- Calculate the **Annualized Rate of Occurrence** (ARO)
  - How many times a threat can take place in a 12 month period
- ARO = estimated frequency of threat taking place within 1 year period

Quantitative Risk Analysis

- Step 4: Derive the Overall Annual Potential Loss Per Threat
- Combine potential loss and probability
- Calculate the **Annualized Loss Expectancy** (ALE)
  - Using information from first 3 steps
- Choose measures to counteract each threat
  - Include Cost/Benefit Analysis for each countermeasure
- ALE = (SLE) x (ARO)
- ALE = economical dollar value company can spend annually to safeguard asset

Quantitative Risk Analysis

- STEP 5: Reduce, Transfer, Avoid or Accept the Risk
- Risk Reduction Methods
  - Install Security Controls and Components
  - Improve Procedures
  - Alter the Environment
  - Provide Early Detection Methods to catch the Threat as its happening
  - Erect barriers to the threat
  - Carry-out security awareness training

Quantitative Risk Analysis

- STEP 5: Avoid, Transfer, Mitigate (Reduce), or Accept the Risk
- Risk Avoidance
  - Discontinue the activity causing risk
- Risk Transfer
  - Buy Insurance
- Mitigate
  - Implement controls
- Risk Acceptance
  - Live with risk and spend no more money

Qualitative Risk Analysis

- Qualitative analysis does not assign monetary values to components or losses
- Qualitative examine different scenarios or risk possibilities,
- Rank the seriousness of the threats and the validity of the different possible countermeasures based on opinions

Qualitative Risk Analysis

- Qualitative Techniques Include:
  - Judgment
  - Best Practices
  - Intuition
  - Experience
- Examples of Qualitative Techniques:
  - Brainstorming, Storyboarding
  - Focus groups
  - Interviews, surveys & questionnaires
  - Team performing the analysis must gather people with experience and education on the threats being examined

Quantitative vs Qualitative (1)

- Qualitative analysis drawbacks
  - Assessments and results are subjective
  - Eliminates the opportunity for cost/benefit discussions
  - Difficult to track Risk Management objectives with subjective measures
  - Standards are not available

Quantitative vs Qualitative (2)

- Quantitative analysis drawbacks
  - Calculations are more complex
  - Process is extremely labour intensive
  - More preliminary work is required to gather detailed information
  - Standards are not available

Protection Mechanisms - Control Selection

- Countermeasures or safeguards must make good business sense
  - Must be cost effective
  - Benefits outweigh the cost to implement
    - This requires a new type of analysis called cost/benefit analysis (ROI)
- Common Cost/Benefit Analysis formula:
  - (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) = value of safeguard to the company

Control Selection - Safeguards

- Example
  - ALE if hacker brings down web server = $12,000
  - ALE after safeguard implemented = $3,000
  - Cost of safeguard $650
  - Value of implementing safeguard = $8,350
- Value of safeguard may include
  - Product cost
  - Implementation cost
  - Testing costs
  - Maintenance cost
  - Monitoring costs
  - Repair update cost

Control Selection - Safeguards

- Functionality and effectiveness of each countermeasure should be evaluated by the analysis team.
- Example: Camera system should be highly visible rather then concealed.
  - A potential attacker seeing camera system may move on to an easier target

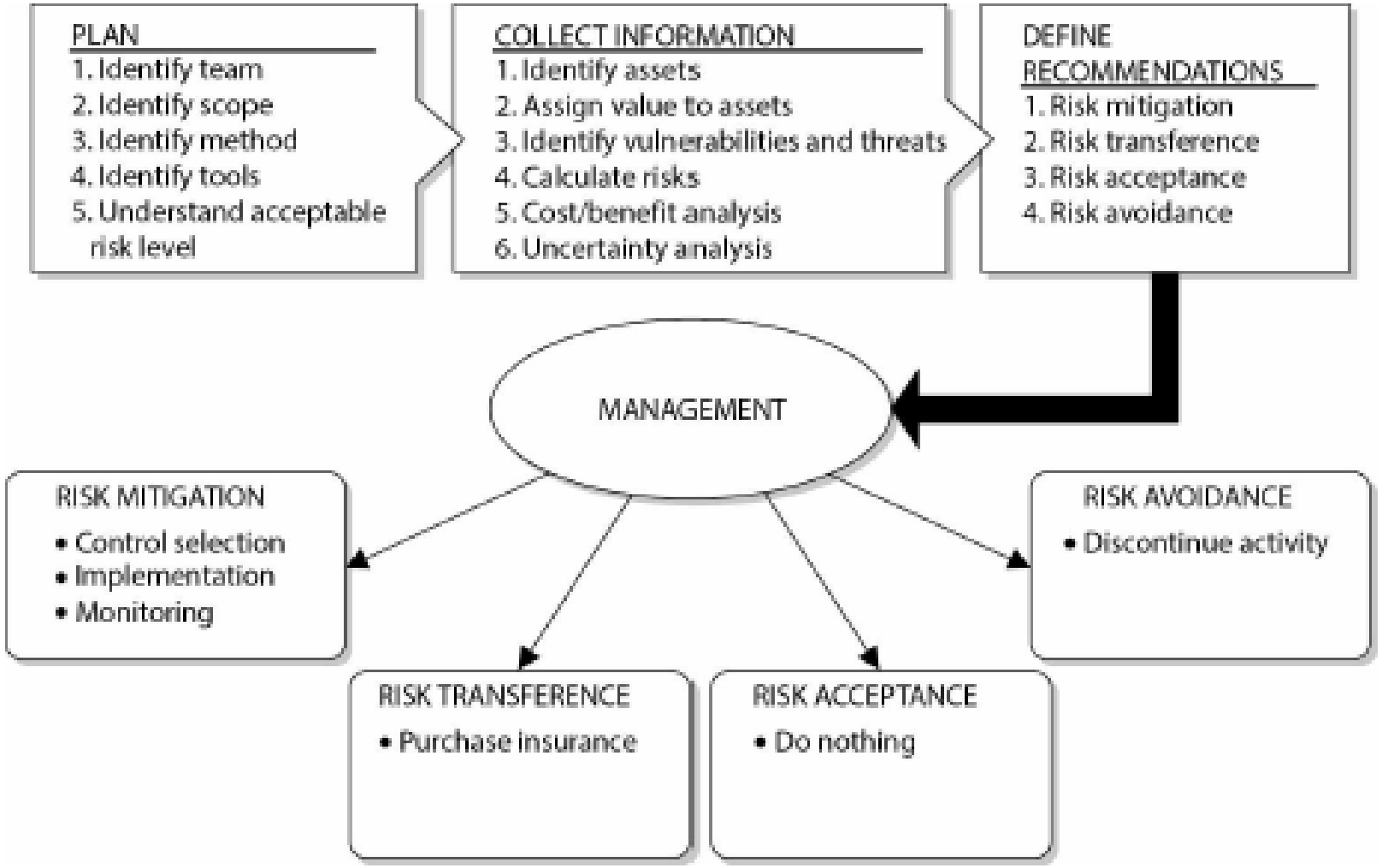
Control Selection - Safeguards

- Steps for selecting a safeguard or countermeasure
  - Decide what assets require protection and to what extent
  - Decide on amount of money allocated to protecting asset
  - Evaluate functionality of available safeguard
  - Determine which safeguard is most appropriate for your environment
  - Compare cost of safeguards
- This process allows the management team to make a sound business decision

Total Risk vs. Residual Risk

- Total Risk vs. Residual Risk
- No one or company is safe from risk 100%
- No countermeasure will give you 100% risk reduction
- Risk level remaining after implementing a countermeasure is referred to as *Residual Risk*
- If a company chooses against implementing a countermeasure they are 100% at risk
  - This is often referred to as *Total Risk*

Risk Management Program set up



Handling Risk

- Handling Risk:
- Once a company knows risk exposure level they can choose one of 4 actions;
  - Transfer Risk
  - Reject Risk
  - Reduce Risk
  - Accept Risk
  - Or put another way: Avoid, Transfer, Mitigate or Accept ☺

Information Risk Management

- Risk Transfer
  - Purchasing Insurance transfers risk to Insurance Company
- Risk Avoidance
  - Cease activity which creates or increases level of risk
- Risk Mitigation
  - Risk is reduced to level considered acceptable
  - Implement Countermeasure
- Risk Acceptance
  - Understand level of risk as well as the potential cost of damage and live with it
  - Do Not Implement Countermeasure

Supply Chain Risk Management

- A supply chain is a sequence of suppliers involved in delivering some product.
- The supply chain also includes suppliers of services, such as maintaining the day to day operations of your facilities.
- Whether a problem is upstream or downstream from your company it's still a problem and it will affect your company.

Service Level Agreements – SLA's

- Review the service provider's security program
- Conduct onsite inspection and interviews
- Review contracts to ensure security and protection levels are agreed upon
- Ensure service level agreements are in place
- Review internal and external audit reports and third-party reviews
- Review references and communicate with former and existing customers
- Review Better Business Bureau reports
- Ensure the service provider has a business continuity plan (BCP) in place
- Implement a nondisclosure agreement (NDA)
- Understand the provider's legal and regulatory requirements

Risk Management Frameworks

- A *risk management framework (RMF) is* a structured process that allows an organization to identify and assess risk, reduce it to an acceptable level, and ensure that it remains at that level.
- A RMF is a structured approach to risk management.

Commonly Accepted Risk Management Frameworks

- **NIST RMF (SP 800-37r1)** U.S. federal government agencies are required to implement the provisions of this document. It takes a systems life-cycle approach to risk management and focuses on certification and accreditation of information systems.
- **ISO 31000:2018** This international standard focuses on the uncertainty that leads to unanticipated effects. It acknowledges that there are things outside our control and that these can have negative (e.g., financial loss) or positive (e.g., business opportunity) consequences.

  This framework is not focused on information systems, but can be applied more broadly to an organization.

- **ISACA Risk IT** This framework, developed by ISACA in collaboration with a working group of academic and corporate risk professionals, aims at bridging the gap between generic frameworks such as ISO 31000 and IT-centric ones such as NIST's. It is also integrated with COBIT.

RMF Steps

- The NIST RMF outlines the following six-step process of applying the RMF, each of which will be addressed in turn in the following sections:

1. Categorize information system.
2. Select security controls.
3. Implement security controls.
4. Assess security controls.
5. Authorize information system.
6. Monitor security controls.

Categorize Information Systems

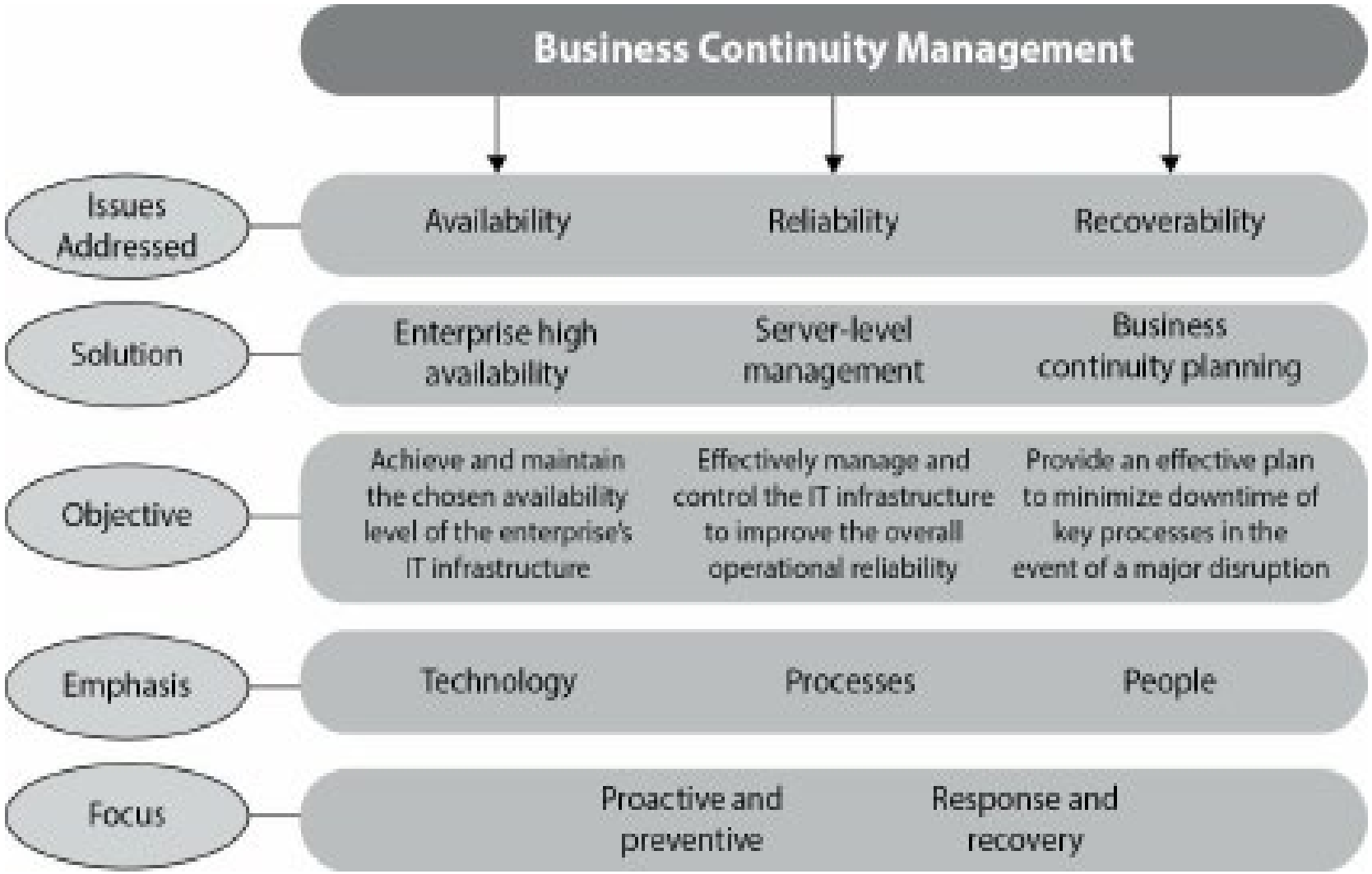
- Find out what your company has and:
- How is the information system integrated into the enterprise architecture?
- What types of information are processed, stored, and transmitted by the system?
- Are there regulatory or legal requirements applicable to the information system?
- How is the system interconnected to others?
- What is the criticality of this information system to the business?

Security Controls

- A security control is a mechanism used to mitigate (reduce) a potential risk.
  - Assess the risk exposure before selecting security controls for the information systems.
  - Then determine if there are any risks that are specific to it or have been introduced into the overall architecture by the introduction of a new system i.e. risk assessment both before and after any changes.
  - Select implement and document appropriate controls.
- The effectiveness of the controls needs to be assessed on a regular basis and whatever the result is, a senior officer needs to authorise the use of any system by accepting the results of the risk assessment (assuming the result is acceptable to the organisation).

Business Continuity and Disaster Recovery

FANSHAWE


Business Continuity Management
Issues Addressed
Availability
Reliability
Recoverability
Solution
Enterprise high availability
Server-level management
Business continuity planning
Objective
Achieve and maintain the chosen availability level of the enterprise's IT infrastructure
Effectively manage and control the IT infrastructure to improve the overall operational reliability
Provide an effective plan to minimize downtime of key processes in the event of a major disruption
Emphasis
Technology
Processes
People
Focus
Proactive and preventive
Response and recovery

Business Continuity & Disaster Recovery

- Continual themes repeated throughout this course:
- Availability:
  - Ensuring company resources are available and operating efficiently for employees and customers (Primary theme of Business Continuity and Disaster Recovery)
- Integrity:
  - Ensuring data input and output is correct, without tampering or alteration
- Confidentiality:
  - Ensuring data deemed sensitive (secret) is not compromised during or following disaster recovery. Data classification must remain in tact

Disaster Planning

- Companies have tangible resources
  - Intellectual property
  - Employees
  - Physical structures
  - Computers
  - Electronic data
  - Network connections to other vendors
  - Online data and online backup storage

  If any of these is disrupted companies are crippled or even go out of business
- The longer these are unavailable the less likely for a business to recover

Disaster Planning

- Plans can be put in place to reduce impact on business when failures occur
  - Reduce dollar loss
  - Quick recovery from failure by roll over to a redundant system
  - No single point of failure
- Companies that survive major disasters had plans in place to restart business operations

Disaster Planning

- Disaster Recovery:
  - Minimizes the effects of a disaster
  - Take steps to ensure business processes are able to resume operation in a timely manner
- Disaster Recovery Plan
  - How to handle problems right after they occur
  - Short term goal to get systems back online
  - Usually IT focused

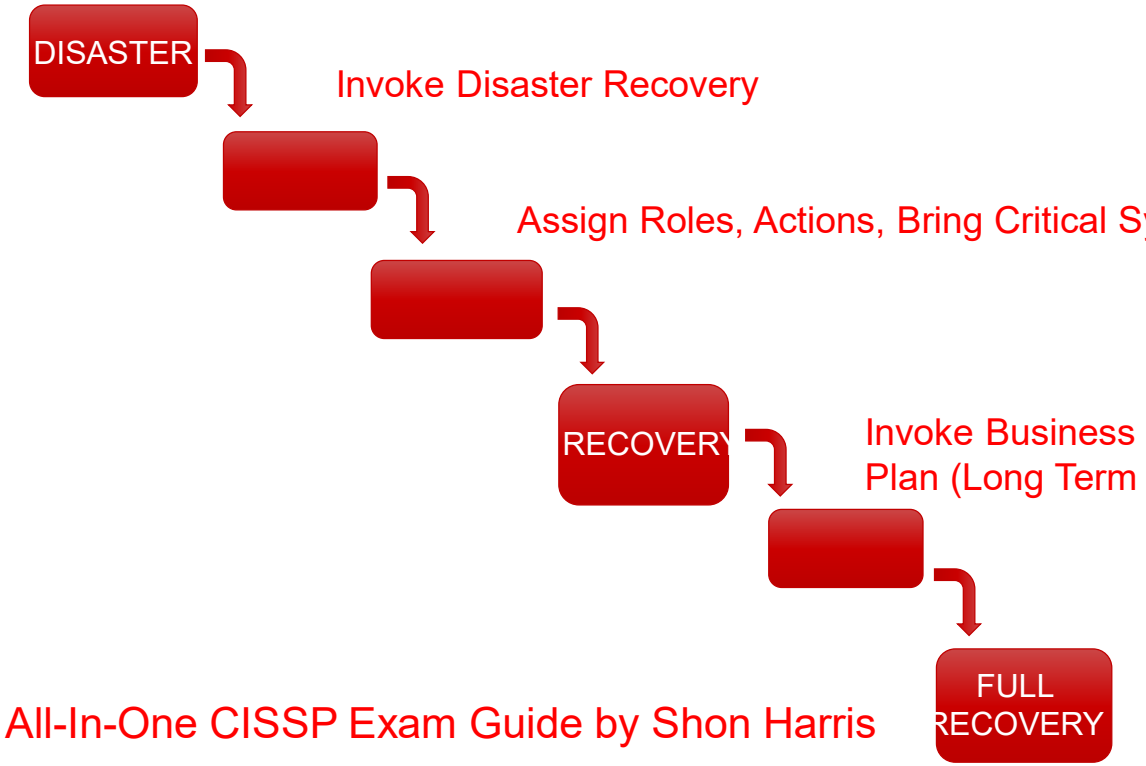
Business Continuity Planning

- Business Continuity Planning:
  - Provides methods and procedures for dealing with longer-term outages and disasters
  - Plans to move business operations to another location while repairs are made to original facilities
  - Getting right people to right places
  - Define a different plan of operation until operation can return to normal
  - How to continue to deal with customers, partners, shareholders and suppliers

Business Continuity Planning

- Business may be more vulnerable after disaster
- Usual safeguards not available
- Confidentiality & integrity must still be maintained
- Availability is main theme of business continuity plan
  - Backups available, redundant systems in place
  - Alternate communication lines
  - Plan for how automated tasks can be done manually

Business Continuity Planning



Source: All-In-One CISSP Exam Guide by Shon Harris

Business Cont & Disaster Recovery Plan

- Provides an immediate response to emergency
- May protect lives and ensures safety
- Reduce business impact
- Resume critical business functions
- Ensure outside vendor and customer relationships do not suffer
- Reduce confusion (both employee, customer and suppliers)
- Ensure survivability of a business after disaster
- Reduce time required for recovery

NIST Business Cont Steps

- NIST - The National Institute of Standards and Technology has outlined the following steps
  - http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

1. Develop Continuity Statement:
   - Write a policy that provides the guidance necessary to develop the plan
   - Assigns authority to the necessary roles to carry out tasks
2. Conduct Business Impact Analysis
   - Identify critical functions and systems and prioritize them based on necessity,
   - Identify vulnerabilities, threats and calculate risks

NIST Business Cont Steps

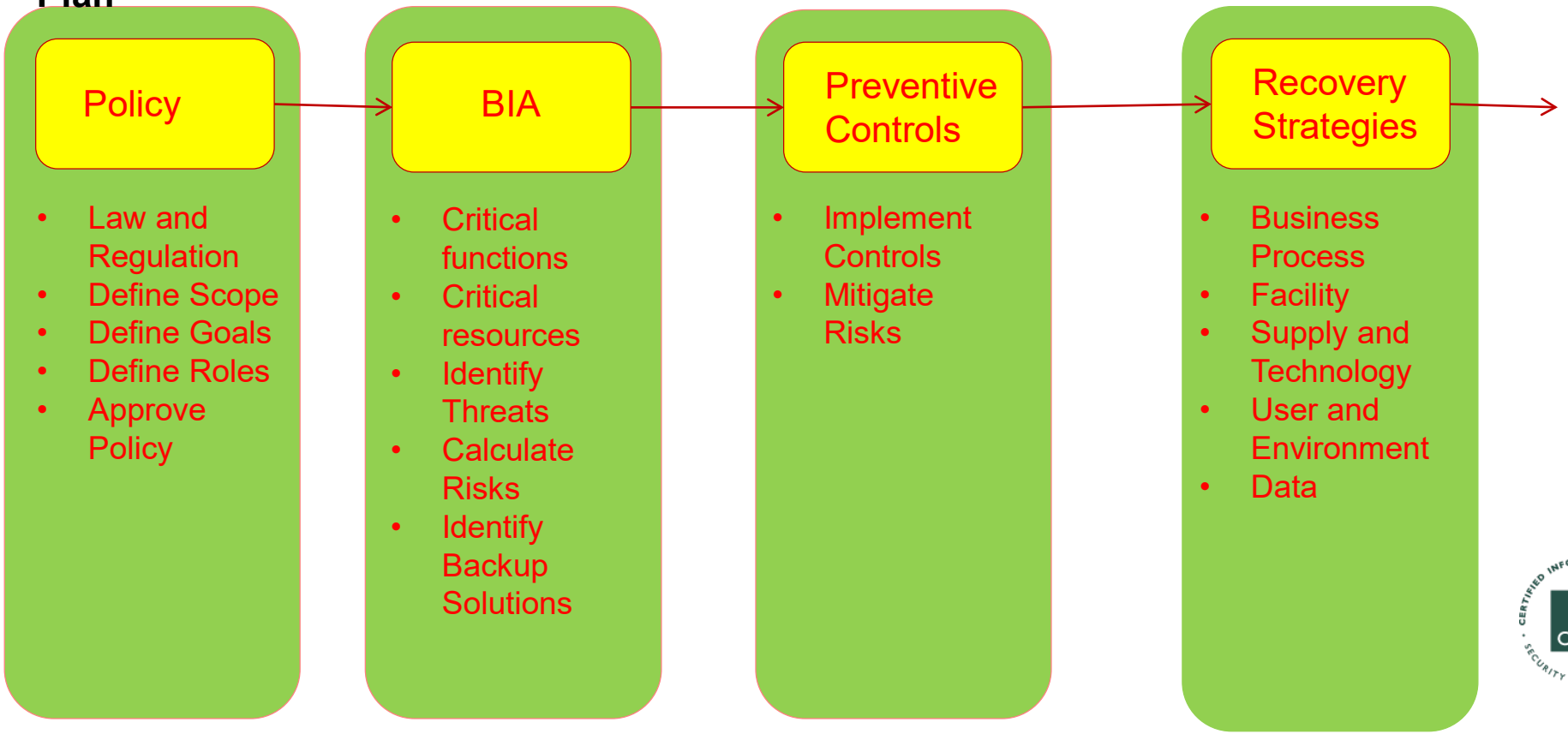
3. Identify Preventive Controls
   - Once threats are recognized, identify and implement controls and countermeasures to reduce the organization's risk level in an economical manner
4. Develop Recovery Strategies
   - Formulate methods to ensure systems and critical functions can be brought online quickly
5. Develop Contingency Plan
   - Write procedures and guidelines for how the organization can still stay functional in a crippled state

NIST Business Cont Steps

6. Test the Plan and Conduct Training Exercises
   - Test the plan to identify deficiencies and conduct training to properly prepare individuals on their expected tasks
7. Maintain the Plan:
   - Put in place steps to ensure the plan is a living document that is updated regularly

NIST Business Cont Steps

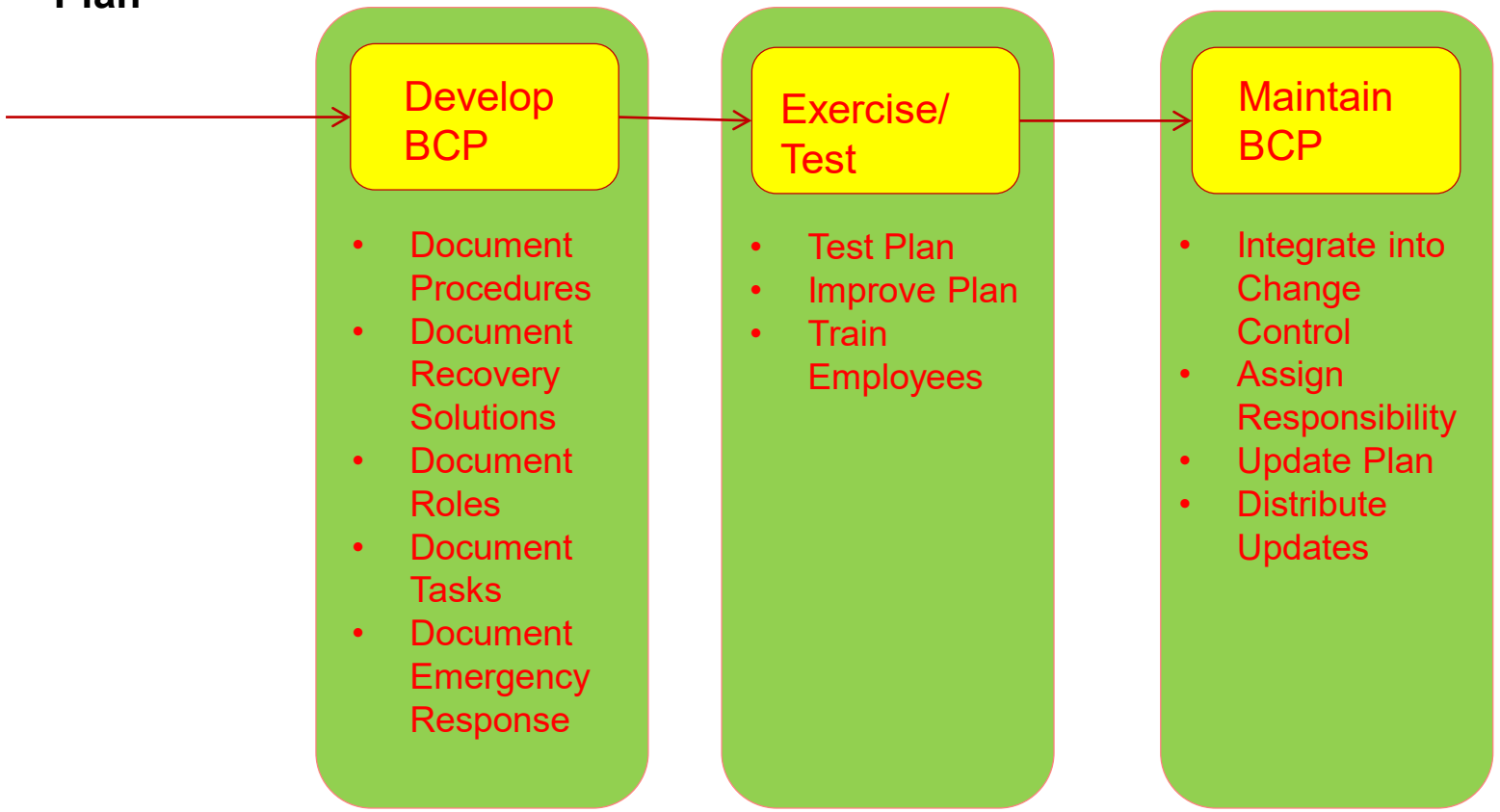
Process for developing Business Continuity Plan



Source: All-In-One CISSP Exam Guide by Shon Harris

NIST Business Cont Steps

Process for developing Business Continuity Plan



Source: All-In-One CISSP Exam Guide by Shon Harris

BCM Part of Enterprise Security Program

- Before a Business Continuity Plan is possible a company must understand and document its internal processes.
  - No one person knows every detail of every business process
- Model of requirements of business processes
  - www.intervista-institute.com/resources/zachman-poster.pdf
  - Examines data, function, network, people, time & motivation and how they relate to roles in a company

BCM Part of Enterprise Security Program

BCP Plan

- Before a Business Continuity Plan is possible a company must understand and document its internal processes.
  - No one person knows every detail of every business process
- Model of requirements of business processes
  - www.intervista-institute.com/resources/zachman-poster.pdf
  - Examines data, function, network, people, time & motivation and how they relate to roles in a company

BCP Project Components

- The BCP becomes part of the corporate security program and business decision process
  - BCP goal is to reduce the financial loss by improving ability for a company to resume operations

BCP Project Components

- Management support is most important before any BCP tasks can begin
- Management should appoint a “Business Continuity Coordinator”
  - Leader of BCP team
  - Will oversee development, implementation, testing and maintenance of BCP
  - Person should have good social skills with political streak
  - Must be credible and have authority as granted by senior management

BCP Project Components

- BCP team must include individuals from all departments
  - These individuals must have a solid understanding of internal processes and tasks within their respective departments
  - Representatives from
    - Business units
    - Senior management
    - IT department
    - Security department
    - Communications department
    - Legal department

BCP Project Components

- Members of the BCP team should be responsible for executing portions of BCP for their respective departments or business units
  - This ensures “buy-in”, sense of “ownership”
  - Increases success rate
- Management must provide BCP scope and specify priorities (tasks)

BCP Statement

- Layouts the “scope” of the BCP project
  - The role of each BCP team member
  - The goal of each BCP team member
  - The goals of the BCP project
- Document lays out required tasks for BCP team
  - Confirms agreement by everyone involved
- Documents should be reviewed by Management after completion
  - No assumptions or omissions

BCP Statement

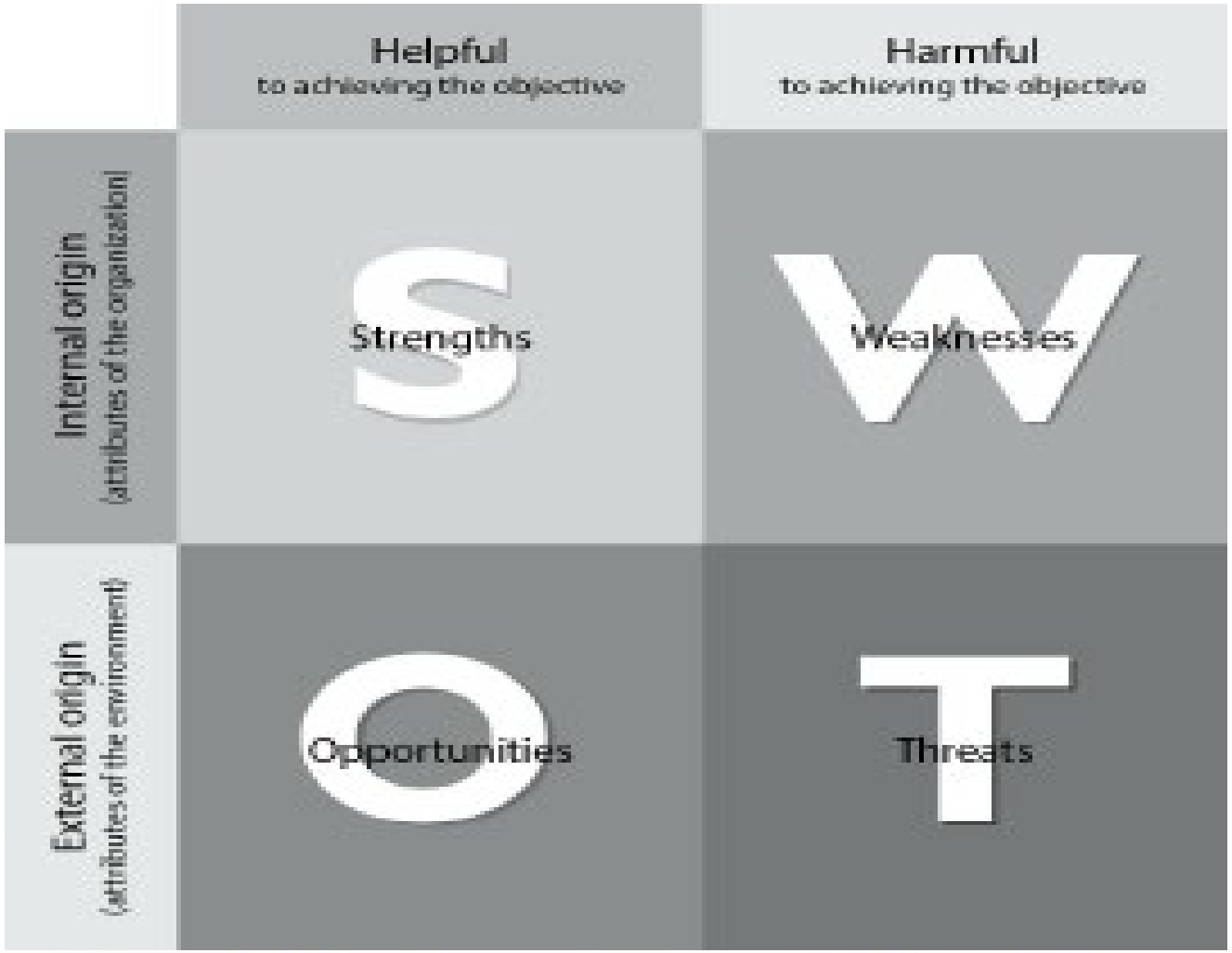
- After the BCP statement is approved a project plan is developed with the following components;
  - Objective to task mapping
  - Resource to task mapping
  - Milestones
  - Budget estimates
  - Success factors
  - Deadlines

BCP Policy

- The policy provides a framework for BCP, it's design and governance.

1. Identify and document the components of the policy.
2. Identify and define policies of the organization that the BCP might affect.
3. Identify pertinent legislation, laws, regulations, and standards.
4. Identify "good industry practice" guidelines by consulting with industry experts.
5. Perform a gap analysis. Find out where the organization currently is in terms of continuity planning, and spell out where it wants to be at the end of the BCP process.
6. Compose a draft of the new policy.
7. Have different departments within the organization review the draft.
8. Incorporate the feedback from the departments into a revised draft.
9. Get the approval of top management on the new policy.
10. Publish a final draft, and distribute and publicize it throughout the organization.

Project Management - SWOT



BCP Planning Requirements

- Due Diligence
  - Determining vulnerabilities and risks.
  - Risk analysis
- Due Care
  - Implementing countermeasures against risks and threats
  - By developing Policies, Standards, Baselines and Guidelines a company has taken responsibility for activities under its control.
  - Taken steps to protect assets, employees and resources from threat.
- Company that does not practice Due Care and Due Diligence may be legally responsible for its activities

Business Impact Analysis

- Business Impact Analysis is a functional analysis
- Deals with unknown and uncertainty
- We cannot predict every disaster but we can plan for one
- Brainstorm all possible disasters, problems, and other risks and plan for recovery
  - If a flood hits tomorrow what would you do?
  - What is required for your business to survive and function?
- Estimate potential damage and loss
- Categorize and prioritize
- Develop alternatives in case these event actually do happen

Business Impact Analysis

- Functional Analysis
- BCP Team collects data through interviews, documentary sources
  - Documents business functions, activities and transactions
- Develops hierarchy of business functions
- Applies classification scheme
  - Indicate each individual function's criticality level

Business Impact Analysis

- Identify threats and map them to the following characteristics
  - Maximum tolerable downtime
  - Operational disruption and productivity
  - Financial considerations
  - Regulatory responsibilities
  - Company reputation

Business Impact Analysis

- Requires information from each business unit or department
  - Processes and interdependencies
  - Transactions and services
- Team must decide how they will collect information
  - Surveys, interviews, workshops
- BCP team must analyze collected information and decide criticality level for each
  - Must outline which items are Tier 1, Tier 2 and so on…

Business Impact Analysis

- BCP team must identify **all** possible threats to each transaction, process, service identified in previous steps and the likelihood of them happening
- BCP team must assign value to each asset that could be affected by identified threat scenarios
  - Qualitative and quantitative values

Business Impact Analysis

- Apply ‘loss criteria’ to each identified threat
  - Loss of reputation and public confidence
  - Loss of competitive advantage
  - Increase in operational expenses
  - Violations in contract agreements
  - Violation of legal or regulatory requirements
  - Delayed income costs
  - Loss of revenue
  - Loss of productivity

Business Impact Analysis

- Identify required resources for critical business processes to take place
  - Personnel, procedures, tasks, computers, suppliers, vendor support
- Estimate maximum ‘outage’ for any of these critical systems before severe company impact
  - This is referred to as MTD
    - Maximum Tolerable Downtime

Business Impact Analysis

- Example (MTD) Values
  - Nonessential: 30 days
  - Normal: 7 days
  - Important: 72 hours
  - Urgent: 24 hours
  - Critical: Minutes to hours
- Each asset, process, transaction or service should be placed in one of these categories

Business Impact Analysis

- Usually presented as a work flow analysis
- Contains roles, responsibilities and resources required for each step
  - Required roles
  - Required resources
  - Input and output mechanisms
  - Workflow steps
  - Required time for completion
  - Interfaces with other processes

Business Impact Analysis

- Once all threats are identified attention turned to reducing these risks.
  - Fortification of facility (construction)
  - Redundant servers and communication links
  - Dual transformer power lines
  - Redundant vendor support
  - Purchasing Insurance
  - Purchasing power generators or uninterruptible power supply
  - Data backup technologies
  - Media protection safeguards
  - Increased inventory of critical equipment
  - Fire detection and suppression system

Business Impact Analysis - Interdependencies

- Company tasks, transactions and processes are complex and have many interdependencies
- The BCP team must identify all
  - Define supporting functions and supporting departments
  - Identify all possible disruptions to mechanisms enabling interdepartmental functions
  - Identify and document threats that could disrupt interdepartmental communication
  - Gather qualitative and quantitative information for all interdepartmental functions
  - Provide alternative methods or mechanisms to restore functionality and communication

Personnel Security

FANSHAWE

Personnel Security

- Unfortunately people are the weakest link in the Security chain
- Separation of duties and layers of responsibility ensure a successful security program
- Appropriate level of training and transparency is required for everyone to understand their responsibilities within the company
- Clear structure and chain of command is required

Personnel Security

- Clear duty descriptions ensure everyone understands their role within the company
- Policies ensure everyone understands expected behaviour.
  - Clearly define acceptable and unacceptable behaviour including reprimand
- Separation of Duties ensures there is no collusion amongst employees
  - Collusion – Two or more employees working together to cause a destructive or fraudulent act against the company

Personnel Security

- Management hierarchy must be in place
  - Ensure everyone has a manager or supervisor scrutinizing their actions and work performance
- Rotation of duty
  - Tool to not only cross train employee in many different roles
  - If an employee stays in a single position for too long they may become complacent and have too much influence over a specific process
- Mandatory vacation
  - Should be enforced for all employees
  - Required for employee health
  - Also tool for the company to detect fraud or destructive practices within the company

Hiring Practices

- Appropriate screening should be completed before an employee is hired to ensure the right person is hired for the job
- Non Disclosure Agreement should be discussed and signed by all employees before hiring
- Complete reference checks should be completed including;
  - Employment , criminal, education, professional credentials
  - By completing a comprehensive background check you are mitigating possible risk brought to company by the employee

Hiring Practices

- Appropriate Drug Testing should be performed
- Employment history
  - Look for unexplained gaps
- Use search engine -- search candidates full name
- Review social websites like Facebook
- Typically it is harder to do background checks after the individual is hired
  - There must be legal ground for background checks after the fact

Termination

- Termination can occur for many reasons
- Company should have documented procedure
  - This can mitigate legal law suits against the company
- Employee must surrender all company issued items including security badges
- All user privileges should be revoked
    - User accounts disabled
    - Passwords must be changed

Security Training

- Security requirements are established by management through policies, standards and guidelines
- Training outlines expected behaviour and reinforces common goals and sets appropriate expectations
  - Everyone should be familiarized with expected behaviour and action results based on policies, standards and guidelines
- Security can only be successful if everyone is informed
- Because everyone has different experiences and values, formal training ensures employees are taught identical curriculum

Security Training

- Training is created for 3 types of audience
- Management
  - Concerned with High Level Business Goals
- Staff
  - Operational business processes and their results
- Technical Staff
  - Concerned with operational implementation and monitoring of processes

Security Training

- Management
  - Short and focused training
  - Corporate Assets
  - Financial Gains and Losses related with Security
  - Negative Impact of Security Breach
  - Explain Possible Threats and their Impact

Security Training

- Mid-Management
  - More in depth and detailed training
  - Detailed explanation of policies, standards and guidelines
  - Explain why security is important to their departments
  - Explain their specific responsibility with enforcement
  - Understand consequences of non compliance

Security Training

- Staff
  - Detailed training with many examples
  - Outline acceptable and unacceptable behavior
  - Outline why security is important with examples of consequences when security is not enforced
  - Explain in detail any reprimand or non compliance consequences
  - Use signed document (by each staff) confirming they've been given training and understand consequences of non compliance
  - This reinforces Policies, standards and Guidelines

Security Training

- Tech Staff
  - Training requirements which correspond to their daily tasks
  - Detailed technical configurations
  - Recognizing security breach or compromise situation
  - Understand detailed incident handling procedures
  - Understand incident reporting structure
    - who they report to

Security Governance

- Security governance is a framework that allows for the security goals of an organization to be set and expressed by senior management, communicated throughout the different levels of the organization. It grants power to the entities needed to implement and enforce security, and provides a way to verify the performance of these necessary security activities. Not only does senior management need to set the direction of security; it also needs a way to be able to view and understand how their directives are being met or not being met.

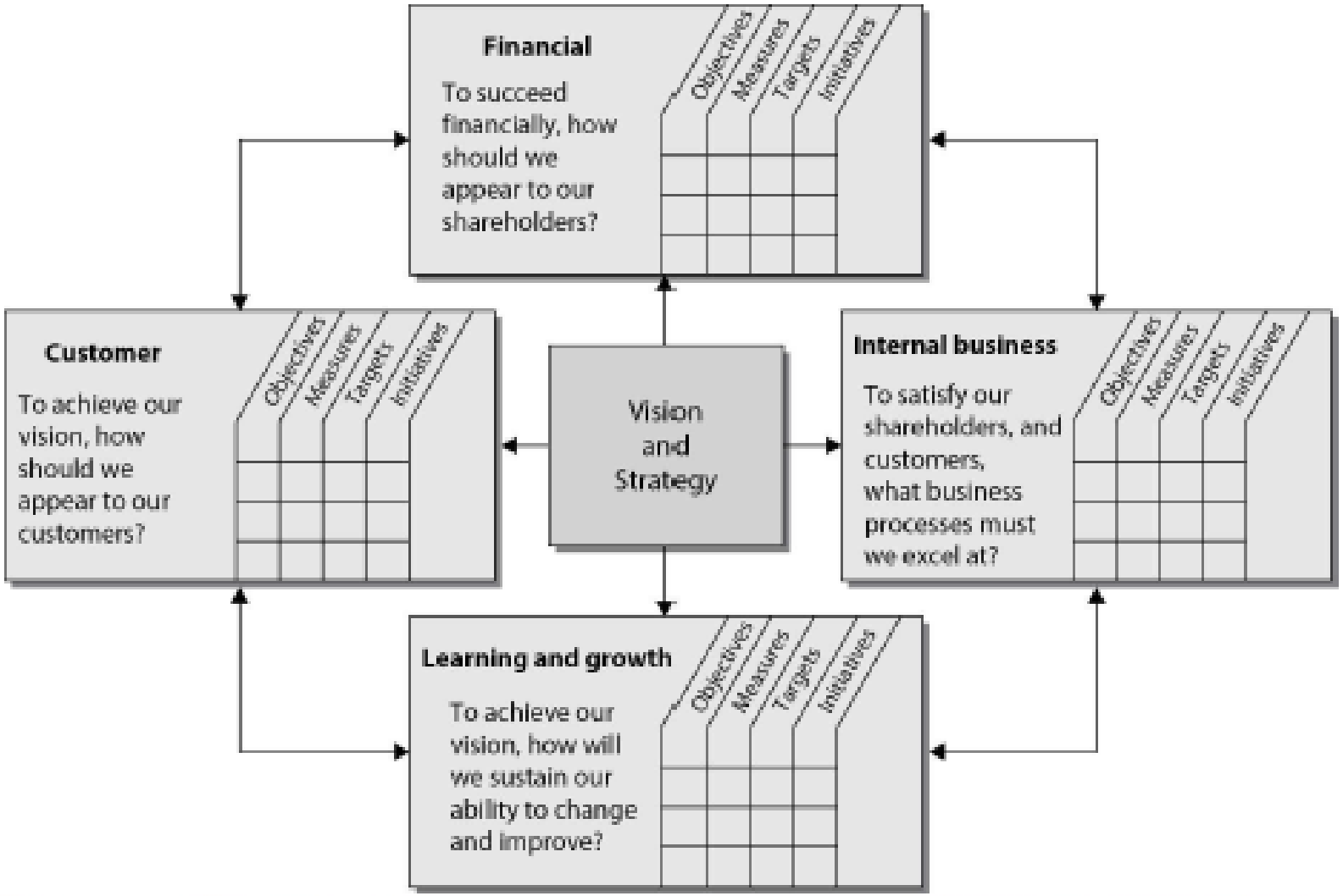
Security Governance Cont.

- Governance is a company's strategy for **reducing the risk of unauthorized access to information technology systems and data**.
- Security governance is a company's strategy for reducing the chance that physical assets owned by the company can be stolen or damaged.

Security Metrics

- The effectiveness of work done needs to be assessed to:
- identify deficiencies,
- prioritize the things that still need work.
- facilitate decision making,
- performance improvement,
- accountability through collection, analysis, and reporting of the necessary information.

Security Metrics – Balanced Scorecard



Ethics

- (ISC)2 requires all certified system security professionals to commit to fully supporting its Code of Ethics
- If a CISSP intentionally or knowingly violates this Code of Ethics, he or she may be subject to a peer review panel, which will decide whether the certification should be relinquished
- Act honorably, honestly, justly, responsibly, and legally, and protect society
- Work diligently, provide competent services, and advance the security profession

Ethics

- Encourage the growth of research—teach, mentor, and value the certification
- Discourage unnecessary fear or doubt, and do not consent to bad practices
- Discourage unsafe practices, and preserve and strengthen the integrity of public infrastructures
- Observe and abide by all contracts, expressed or implied, and give prudent advice

Ethics

- Avoid any conflict of interest, respect the trust that others put in you, and take on only those jobs you are fully qualified to perform
- Stay current on skills, and do not become involved with activities that could injure the reputation of other security professionals

Risk Management Summary

- Risk management requires
  - Risk analysis to identify assets, vulnerabilities and threats and consequences
  - ROI required to determine business case for safeguards
  - Quantitative & qualitative
- Security policy is modular document
  - Consists of standards, guidelines, procedures & baselines
- Information classification
  - Determines level of protection and responsibility

Risk Management Summary

- Risk management
- Threat modeling
- Business continuity and disaster recovery
- Personnel security
- Security governance

Homework

- Read the relevant chapter in the set book ‘All In One CISSP Exam Guide’ – by Shon Harris.

- Depending on which edition you have the relevant sections will be in different places – so use the index.

- Then identify and do the practice m/c questions relating to this subject.

Questions?