Information Assurance

Domain 2

Information Security Risk Management

Defining Risk

- Risk: The combination of the probability of an event and its consequences

- ISO definition: The effect of uncertainty upon objectives
  - Uncertainty = probability
  - Effect = consequences
  - Upon objectives = consequences that impact goals

Key Terms

Key Term	Definition
Advanced persistent threat	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives using multiple attack vectors
Impact	Magnitude of loss resulting from a threat exploiting a vulnerability
Likelihood	The probability of something happening
Risk analysis	The initial steps of risk management: analyzing the value of assets to the business, identifying threats to those assets and evaluating how vulnerable each asset is to those threats.

Key Terms

Key Term	Definition
Risk appetite	The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission
Risk assessment	A process used to identify and evaluate risk and its potential effects.
Risk management	The coordinated activities to direct and control an enterprise with regard to risk
Risk tolerance	The acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives
Threat	Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm.
Vulnerability	A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events

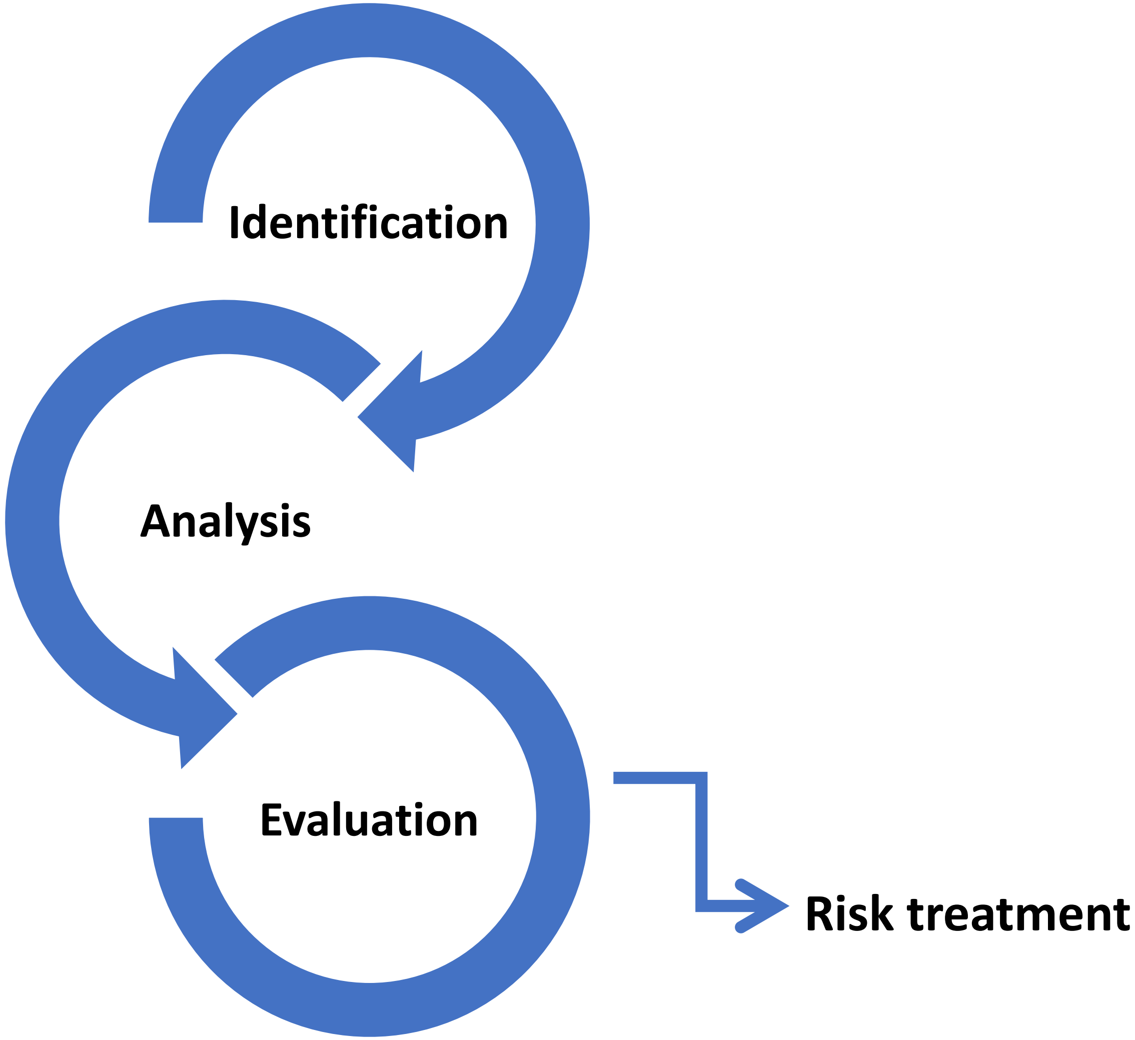
Key Terms

Key Term	Definition
Residual risk	The remaining risk after management has implemented a risk response
Risk acceptance	If the risk is within the enterprise's risk tolerance or if the cost of otherwise mitigating the risk is higher than the potential loss, the enterprise can assume the risk and absorb any losses
Risk avoidance	The process for systematically avoiding risk, constituting one approach to managing risk
Risk mitigation	The management of risk through the use of countermeasures and controls
Risk transfer	The process of assigning risk to another enterprise, usually through the purchase of an insurance policy or by outsourcing the service
Risk treatment	The process of selection and implementation of measures to handle risk

Part A

Information Risk Assessment

Risk Assessment Process



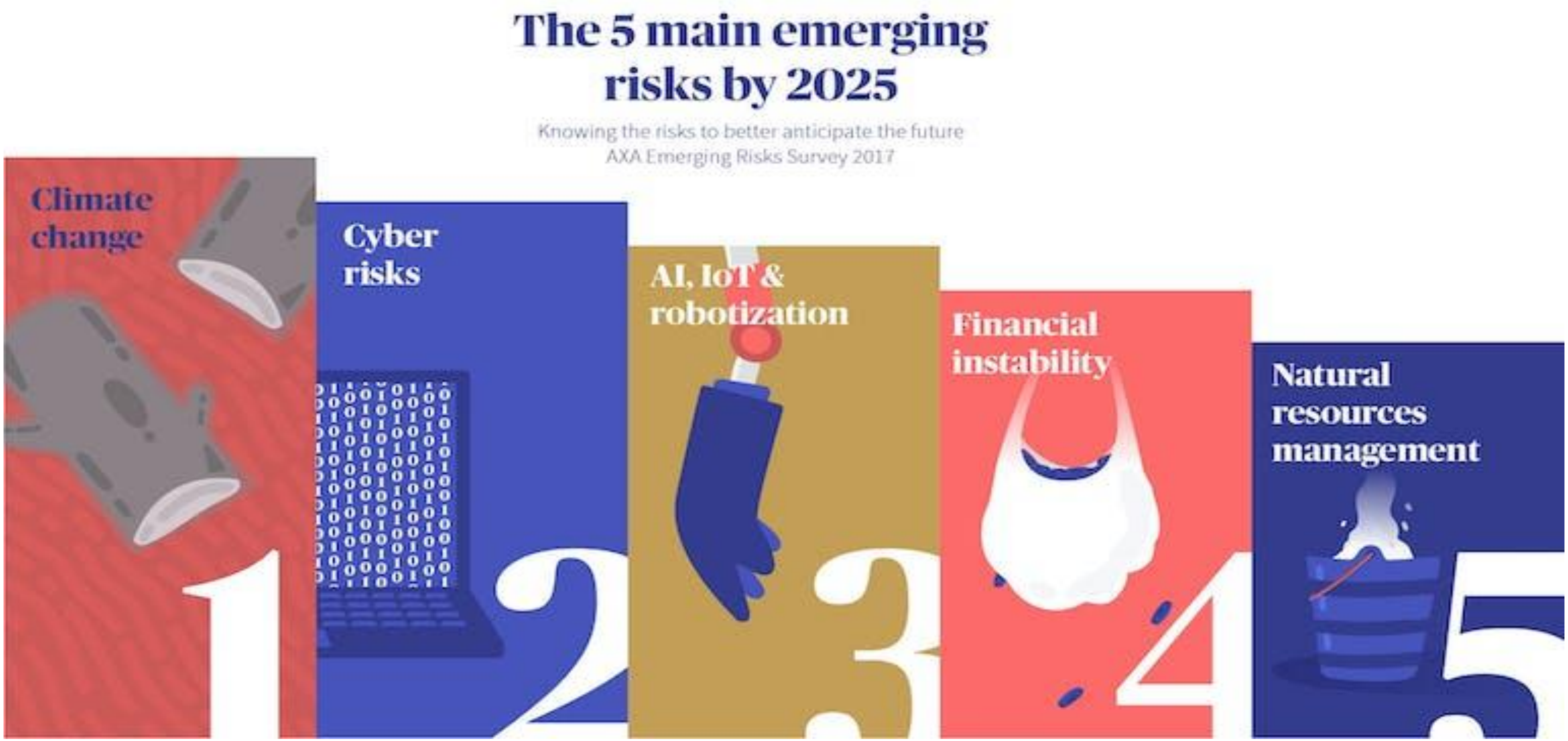
Identification

Analysis

Evaluation

Risk treatment

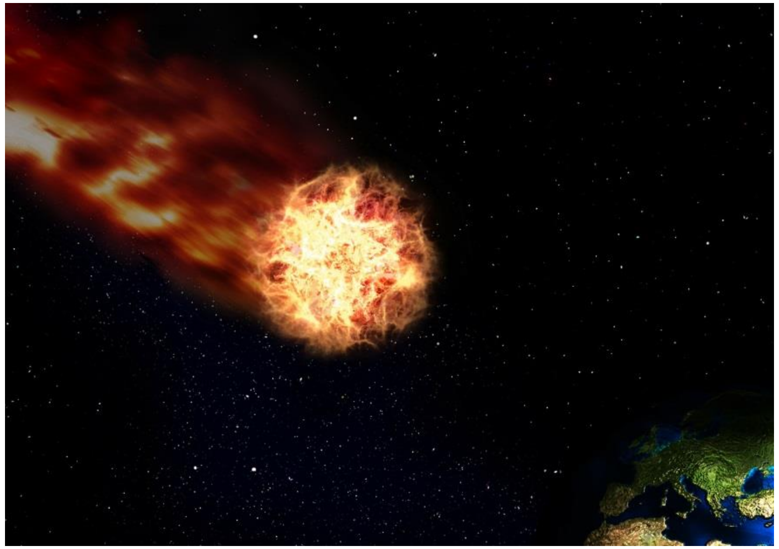
2.1 Emerging Risk and Threat Landscape



The 5 main emerging risks by 2025
Knowing the risks to better anticipate the future
AXA Emerging Risks Survey 2017
Climate change
1
Cyber risks
2
AI, IoT & robotization
3
Financial instability
4
Natural resources management
5

Impact Drives Risk

- ❑ Consequences only matter if they impact the pursuit of business objectives.
- ❑ Something happened: What was affected and how was it affected?



Managing Risk

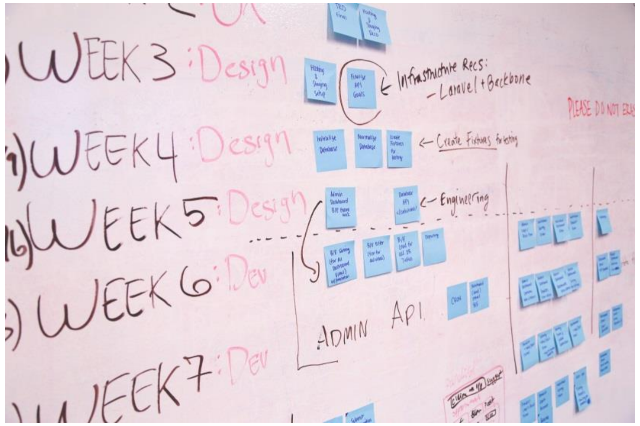
- Management = Estimating risk and choosing an appropriate response

- Goals of information risk management:
  - Keep risk within a tolerable range for the organization’s risk appetite
  - Keep senior management informed of changes

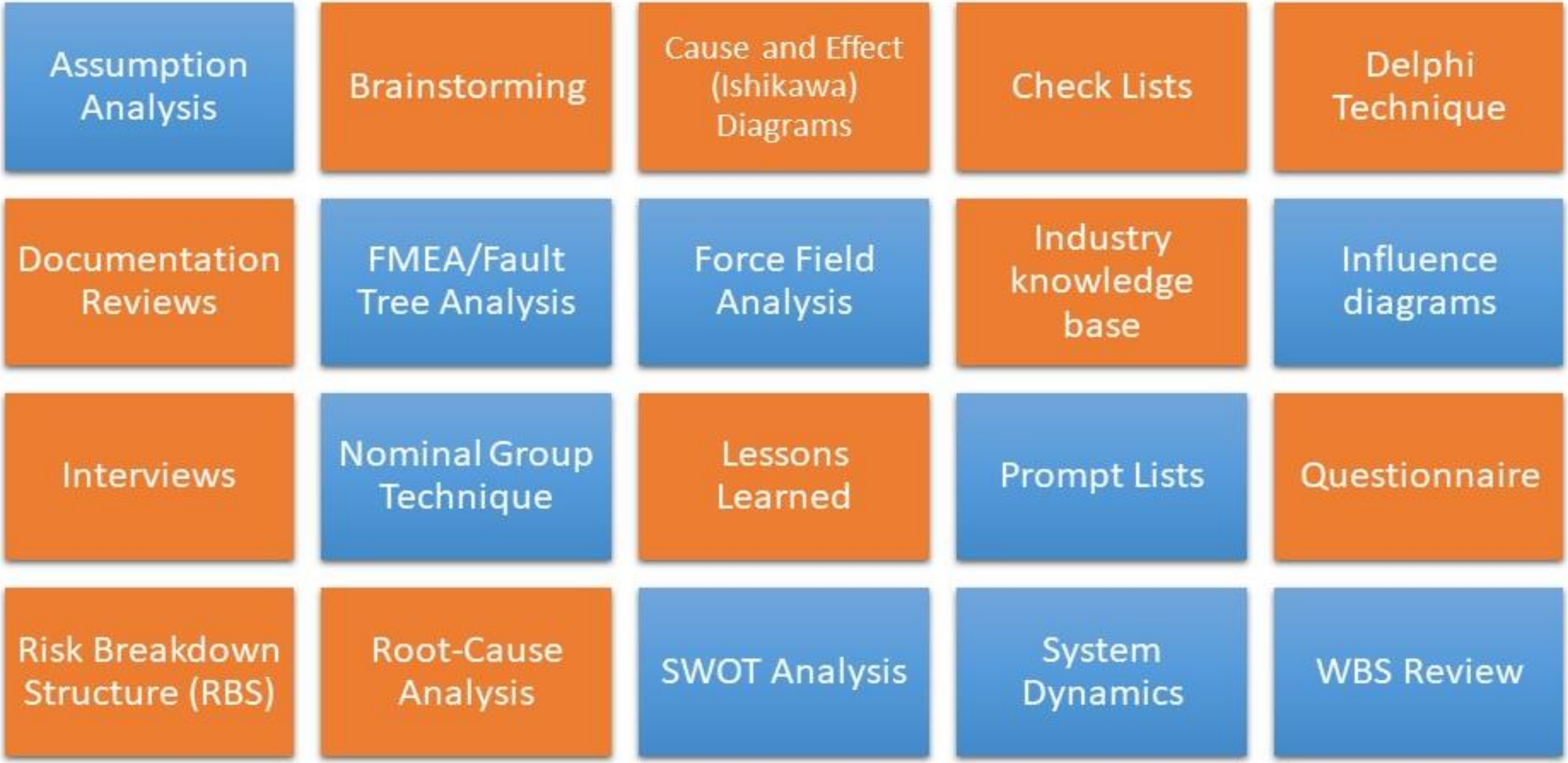
- Must be supported and understood by all members of the organization

Risk Management Program

- Steps in developing a risk management program:
  - Establish context and purpose
  - Define scope and charter
  - Define authority, structure and reporting
  - Ensure asset identification, classification and ownership
  - Determine objectives
  - Determine methodologies
  - Designate a team



2.1.1 Risk Identification



Assumption Analysis	Brainstorming	Cause and Effect (Ishikawa) Diagrams	Check Lists	Delphi Technique
Documentation Reviews	FMEA/Fault Tree Analysis	Force Field Analysis	Industry knowledge base	Influence diagrams
Interviews	Nominal Group Technique	Lessons Learned	Prompt Lists	Questionnaire
Risk Breakdown Structure (RBS)	Root-Cause Analysis	SWOT Analysis	System Dynamics	WBS Review

2.1.1 Risk Identification

- *Assets* are targets of various threats and threat agents.
- Risk assessment involves identifying the organization’s *assets* and identifying *threats/vulnerabilities* to/of those assets.
- Risk identification begins with identifying an organization’s assets and assessing their value.

Asset Identification

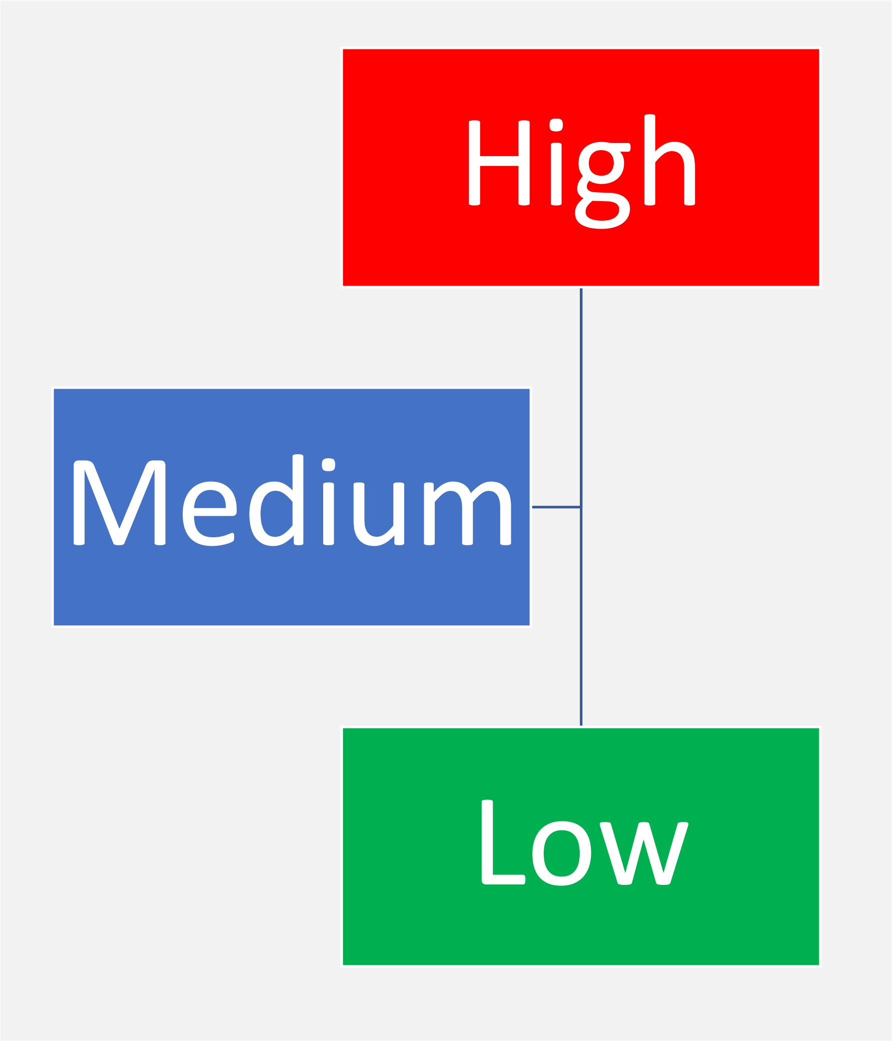
- In order to protect something, you need to identify it.
- Essential to managing risk at an enterprise level
- Systems and data are considered information assets

Valuation of Assets

- Can be straight forward (i.e., hardware costs)
- Can be related to consequential costs (i.e., regulatory sanctions)
- Examples of information assets include:
  - Proprietary information
  - Current financial records and future projections
  - Acquisition/merger plans
  - Strategic marketing plans
  - Trade secrets
  - Patent-related information
  - PII

Valuation of Assets

- ❑ Work with asset owners for estimates
- ❑ Quantitative: Dollar-value figures
- ❑ Qualitative: Perception/judgement of value



Asset Identification, & Valuation

- Iterative process
  - begins with the identification of assets, including all elements of an organization’s system (people, procedures, data and information, software, hardware, networking)
- Assets are then classified and categorized

2.1.2 Threats

- Threat: Anything that is capable of acting against an asset in a manner that can result in harm
- Threat event: Any event during which a threat element/actor acts against an asset in a manner that has the potential to directly result in harm
- Threat actor: A person who initiates a threat event

Threat Identification

- An absence of a threat doesn’t mean the threat no longer exists.
- New threats emerge as behaviors change.
- Sources of threat data:
  - Prior threat assessments
  - News outlets
  - External reports
  - Official notices
  - Industry publications

Types of Internal Threats

- Intentional
  - Malicious
  - Often disgruntled employees
  - Control: Understand frustrations/complaints and seek to resolve them
  - Control: Enforce SoD and least privilege
- Unintentional
  - Doing something they don’t realize is a threat
  - Providing information via social engineering
  - Control: Awareness training and regular reviews

Internal Threats

- A threat actor needs knowledge of the environment.
  - Those operating within a organization are trusted with information and access.
- Screen applicants prior to employment.
- Periodically remind staff of organizational policies.
- At the end of employment, all organizational assets should be returned.

External Threats

- Criminal acts
- Data corruption
- Disease (epidemics)
- Espionage
- Facility flaws
- Fire
- Flooding
- Hardware flaws
- Industrial accidents
- Lost assets
- Mechanical failures
- Power surge/utility failure
- Sabotage
- Seismic activity
- Severe storms
- Software errors
- Supply chain interruption
- Terrorism
- Theft

Advanced Persistent Threat

- Advanced = Method of gaining access include multiple attack vectors
- Persistent = An ability to remain present in a network for a long time without detection
- Threat = Anything that is capable of acting against an asset in a manner that can result in harm
- Often linked to nation-state actors, activist groups or criminal enterprises

Advanced Persistent Threat

- Typical APT life cycle
  - Initial compromise
  - Establish foothold
  - Escalate privileges
  - Internal reconnaissance
  - Move laterally
  - Maintain presence
  - Complete mission

Advanced Persistent Threat

- Sources of APT

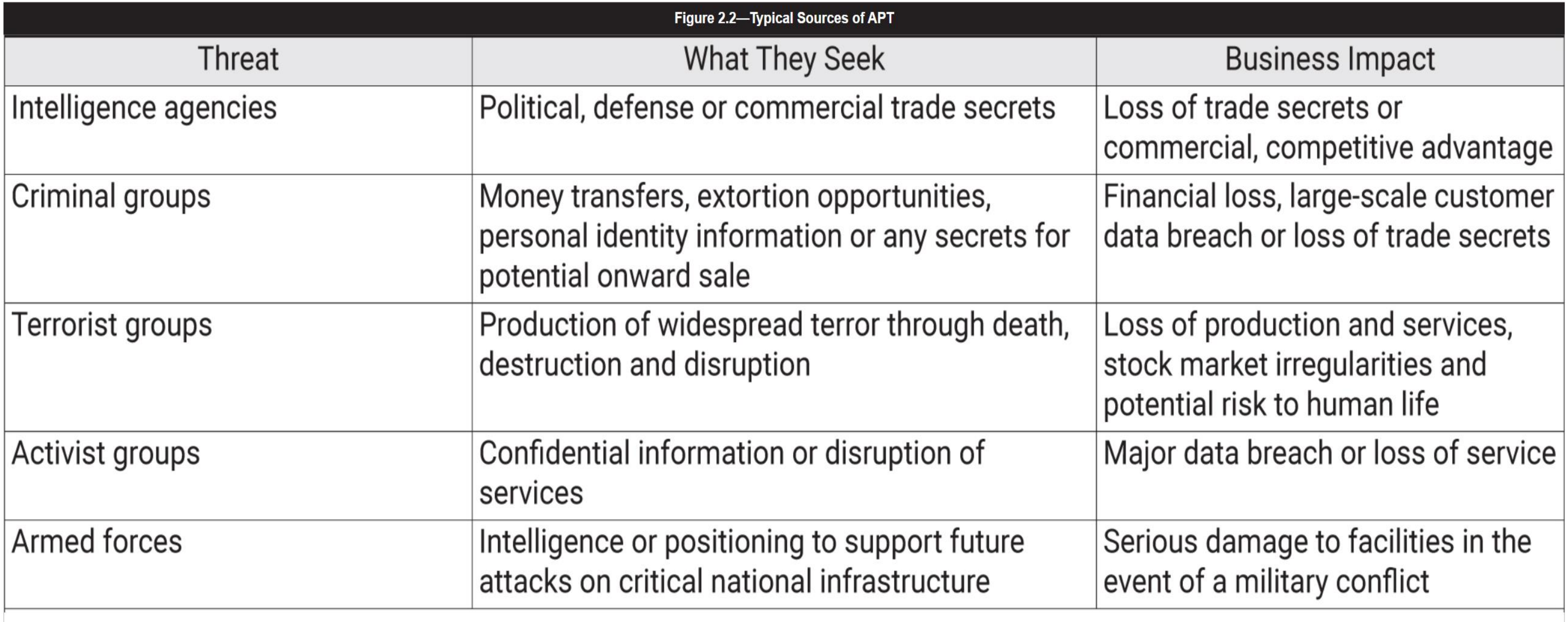


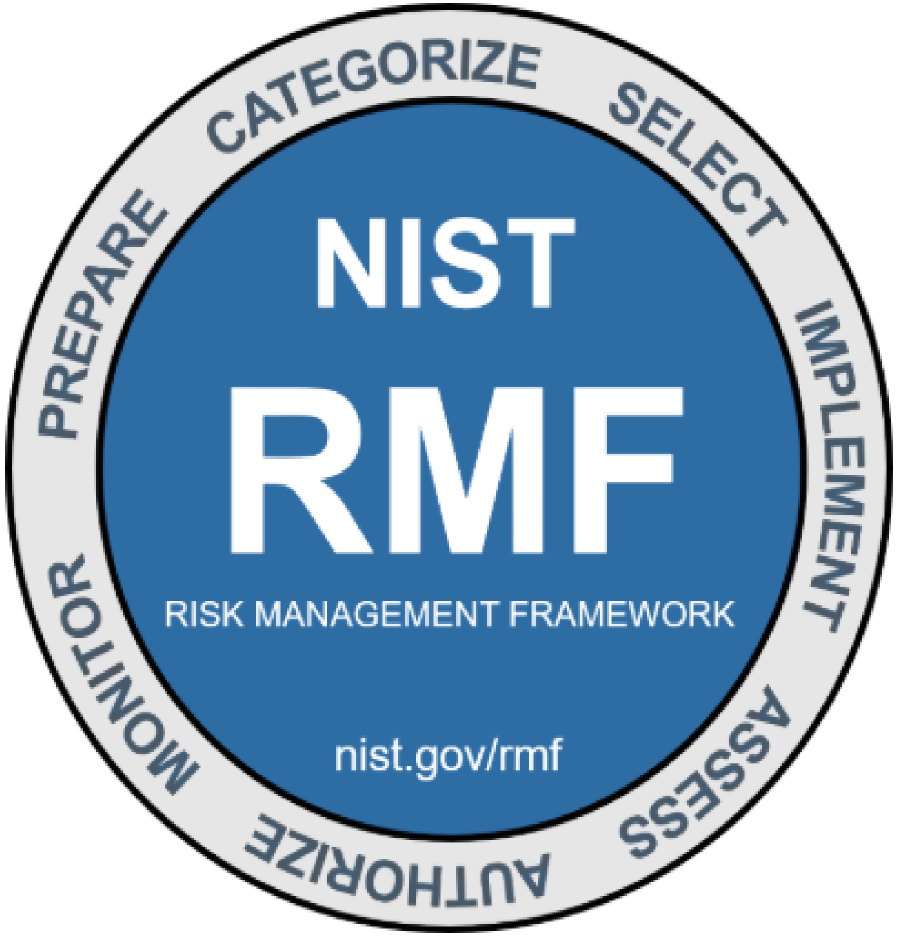
Figure 2.2—Typical Sources of APT

Threat	What They Seek	Business Impact
Intelligence agencies	Political, defense or commercial trade secrets	Loss of trade secrets or commercial, competitive advantage
Criminal groups	Money transfers, extortion opportunities, personal identity information or any secrets for potential onward sale	Financial loss, large-scale customer data breach or loss of trade secrets
Terrorist groups	Production of widespread terror through death, destruction and disruption	Loss of production and services, stock market irregularities and potential risk to human life
Activist groups	Confidential information or disruption of services	Major data breach or loss of service
Armed forces	Intelligence or positioning to support future attacks on critical national infrastructure	Serious damage to facilities in the event of a military conflict

Risk Management Framework

NIST RMF

- The goal of NIST RMF is to:
  - Integrate security and risk management into the system development life cycle (SDLC)
  - Ensure that systems remain secure throughout their entire operation
  - Help decision-makers balance security, cost, and usability



2.1.3 Risk Assessment Framework

1. **Prepare**

   The organization prepares for risk management by setting policies, defining roles, and gathering resources. Establishes risk tolerance and assigns who is responsible for what.

2. **Categorize**

   Categorize the system and information processed, stored, and transmitted based on an impact analysis

3. **Select**

   Controls must be selected and documented that reduce or eliminate the risks at the appropriate impact level required.

2.1.3 Risk Assessment Framework

4. **Implement**

   Put the selected controls into action, both technical (firewalls, encryption) and procedural (policies, training). Document how each control is implemented.

5. **Assess**

   Evaluate if the controls are correctly implemented and effective. Perform vulnerability scans, audits, or penetration testing. Create a Security Assessment Report (SAR).

2.1.3 Risk Assessment Framework

6. **Authorize**

   Senior management (Authorizing Official) reviews all evidence and decides whether the system’s risk is acceptable. If yes, they issue an Authorization to Operate (ATO). If not, the system cannot go live until fixes are made.

7. **Monitor**

   Continuously track the system’s security posture. Detect new threats, review logs, and update controls when needed. Repeat the RMF cycle as the system or environment changes.

Internal & External Environment

- **Internal Environment:**
  - Key business drivers (e.g., market indicators, competitive advantages, product attractiveness)
  - The enterprise’s strengths, weaknesses, opportunities and threats
  - Internal stakeholders
  - Organizational structure and culture
  - Assets in terms of resources (i.e., people, systems, processes, capital)
  - Goals and objectives, and the strategies already in place to achieve them
  - The amount of loss the enterprise is willing to accept in pursuit of the organization’s strategy
  - The acceptable and unacceptable risk criteria for programs, projects at operational and tactical levels

Internal & External Environment

❑ External Environment:

- The global/local market; the industry; and the competitive, financial and political environments
- The legal and regulatory environment
- Social and cultural conditions
- External stakeholders

Risk, Likelihood and Impact

IMPACT

VERY HIGH (Extreme)	LOW	MEDIUM	HIGH	VERY HIGH	VERY HIGH
HIGH (Major)	LOW	MEDIUM	HIGH	HIGH	VERY HIGH
MEDIUM (Moderate)	LOW	MEDIUM	MEDIUM	HIGH	HIGH
LOW (Minor)	LOW	LOW	MEDIUM	MEDIUM	MEDIUM
VERY LOW (Insignificant)	VERY LOW	LOW	LOW	LOW	LOW
	VERY LOW (Rare)	LOW (Unlikely)	MEDIUM (Possible)	HIGH (Likely)	ERY HIGH (Almost Certain)

LIKELIHOOD

Risk, Likelihood and Impact

- Likelihood

RATING	POTENTIAL FOR RISK TO OCCUR	PROBABILITY
VERY HIGH (Almost Certain)	Likely to occur several times a year	>90%
HIGH (Likely)	Likely to occur once a year	50%-90%
MEDIUM (Possible)	Possibly occur once every few years	20%-50%
LOW (Unlikely)	Maybe occur once in 5 years	10%-20%
VERY LOW (Rare)	Might occur once in 10 years	<10%

Risk Analysis Approaches

- **Qualitative analysis:**
  - Based on category assignment (Low, Medium, High)
  - Scales can be adjusted to suit circumstances
  - Can be used:
    - As an initial assessment
    - To consider nontangible aspects of risk(e.g reputation)
    - When there is a lack of adequate information

Analysis

Quantitative analysis

- Assigned numerical values
    - Based on statistical probabilities and monetary values
- Quality depends on accuracy and validity
- Consequences may be expressed in terms of:
    - Monetary
    - Technical
    - Operational
    - Human impact criteria

Activity

- Using risk analysis, determine the relative value of the following:

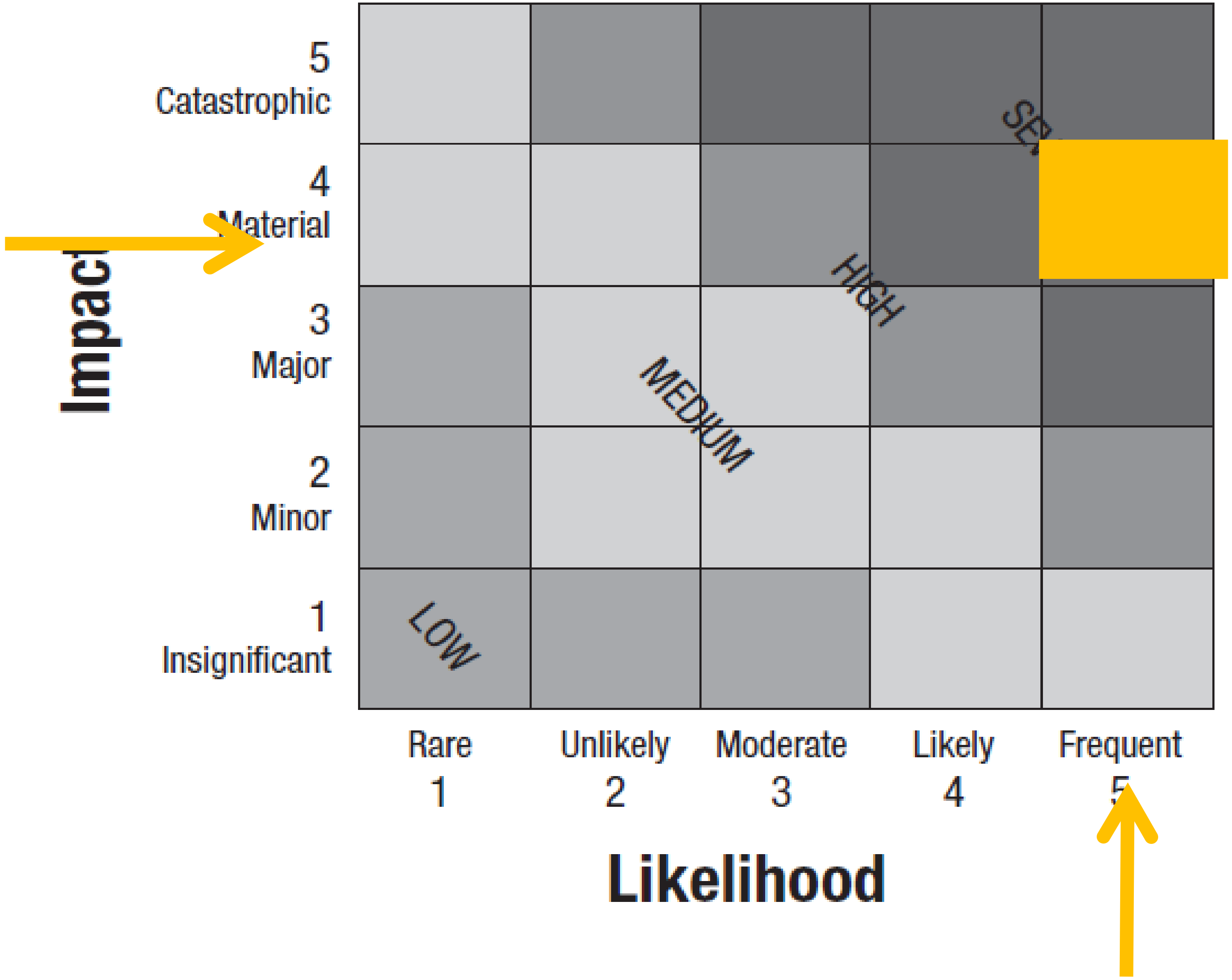
1. Lack of Regular Software Updates on Key Servers : The IT department in a medium-sized company has been understaffed for the last six months. As a result, critical security patches and software updates on several key production servers (hosting customer data and core business applications) have been frequently delayed or skipped entirely.
2. Reputational risk if a product line fails: The product development team has indicated that the market is ready for this particular product, but the infrastructure needed to launch the product is new to the organization and has been rushed into production to meet the desired launch date.
3. Noncompliance with new local regulation: Local government has passed a new law mandating businesses operating within the jurisdiction to update HVAC systems to more energy-efficient models. The cost of upgrading the existing system would be US $500,000, whereas the annual fine for noncompliance would be $10,000.

Activity

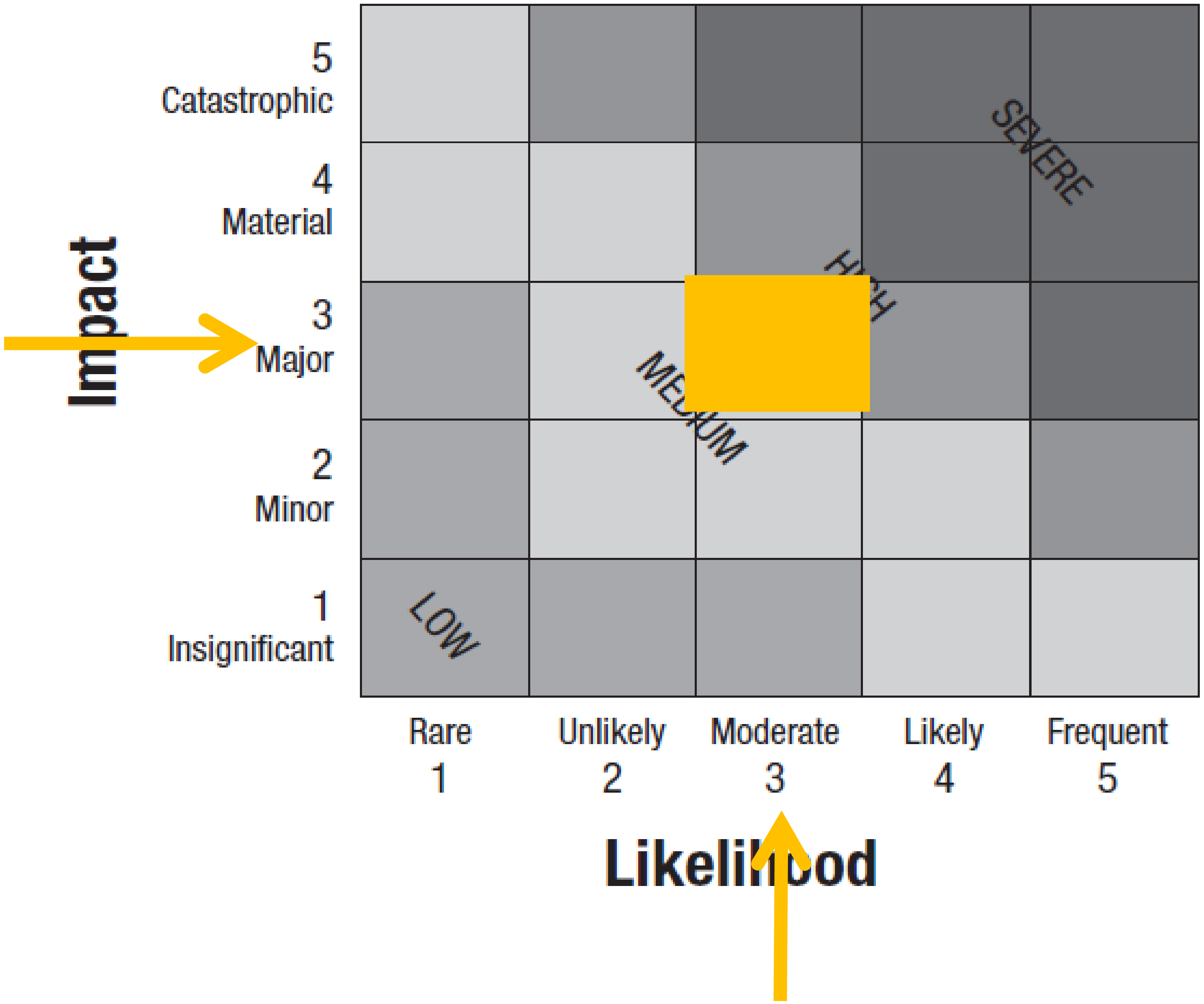
- ❑ Using semi quantitative analysis, determine the relative value of the following:

    4. Email quarantine system is outdated: The company’s email quarantine system is outdated, and messages are not being filtered as successfully as they had been in the past.

Activity: Scenario 1



Activity: Scenario 2



Impact

5 Catastrophic

4 Material

3 Major

2 Minor

1 Insignificant

Rare 1

Unlikely 2

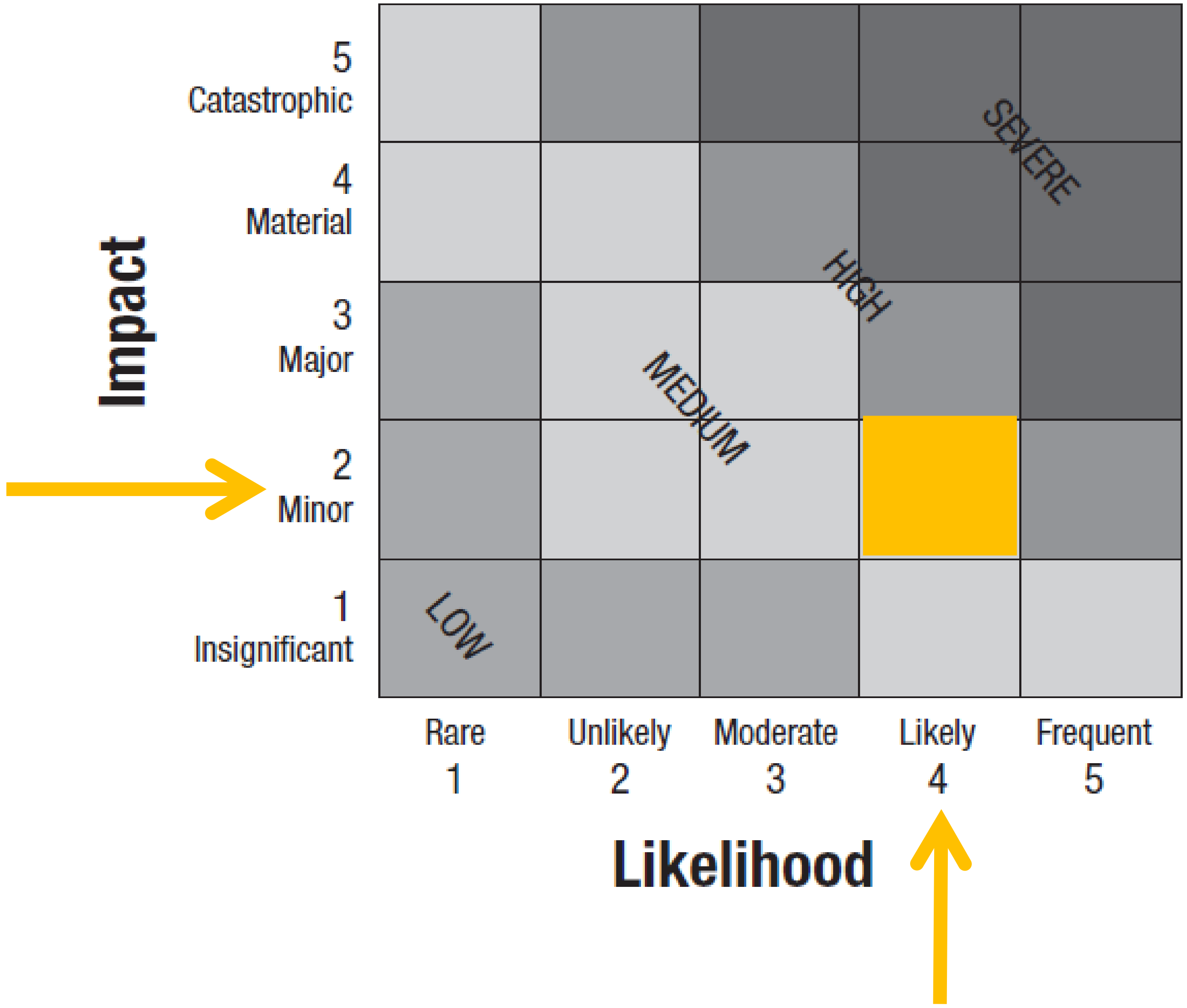
Moderate 3

Likely 4

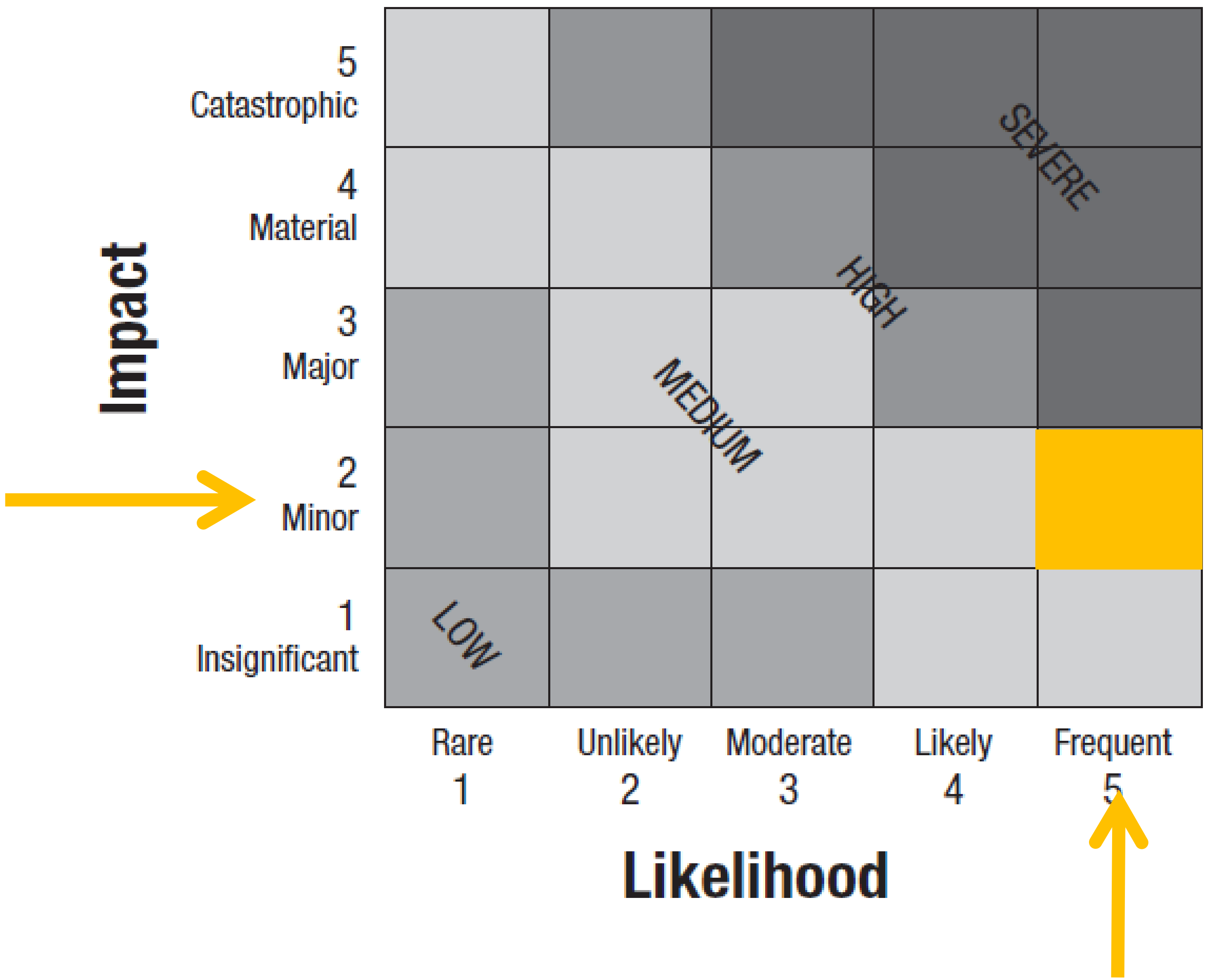
Frequent 5

Likelihood

Activity: Scenario 3



Activity: Scenario 4



The Risk Register

- Maintains the organization’s overall risk profile
- Includes:
  - Summary of the risk based on threat type and associated event or actor
  - Category and classification of the risk
  - Risk owner
- Also documents risk treatment choices

2.2 Vulnerability & Control Deficiency Analysis

- Vulnerability is referred to as weakness and vulnerability arises when control is not efficient, we need to calculate the degree of weakness.
- Sources of Vulnerabilities:
  - National Vulnerability Database at nvdnist.gov
  - Common Weakness Enumeration at nvd.nist.gov/cwe.cfju
  - Common Vulnerabilities and Exposures at cve.initre.org
  - Exploit Database at expioit-db.com
  - The Community Driven Vulnerability Database at vulndb.org
  - Vulnerability Database Catalog at www.first.org/globol/sigs/vrdx/vdb-catalog
  - Packet Storm Security atpacketstorinsecurity.com
  - Rapid7's Vulnerability and Exploit Database at rapid7.com/db
  - CXSecurity Free Vulnerability Database at cxsecurity.com/exploit/
  - Vulnerability Lab at viduerability-lab.com
  - Oday.today at https://Odcry. today'
  - Harmonized Threat and Risk Assessment at www. cse-cst.gc. ca
  - Contingency Planning and Management at coiitiiigeiicyplaiiiiing.com
  - Open Web Application Security Project (OWASP) at www.owasp.org

Vulnerability Categories

It may be useful to consider vulnerabilities in the following categories

- Network vulnerabilities, Physical access, Applications and publicly accessible services, Utilities, Supply chain, Processes, Equipment, Cloud computing, IoT, BYOD etc.
- Audits, security reviews, vulnerability scans and penetration tests are among the approaches that are usually helpful in identifying vulnerabilities.
- Some typical examples of vulnerabilities include:
    - Defective software, Improperly configured hardware/software, Inadequate or inconsistent compliance enforcement, Poor network design (i.e.. flat networks), Uncontrolled, unmonitored or defective processes, Inadequate governance or management, Insufficient staffing levels, Lack of knowledge to support users or operations, Lack of security functionality, Lack of proper hygiene and maintenance, Poor choice of passwords, Transmission of unprotected communications, Lack of redundancy or management communications

2.2.1 Security Baselines

- Security baselines can help manage risk implications
  - Has many benefits:
    - Standardizes the minimum amount of security measures
    - Provides a convenient point of reference for measurement
  - May be built by:
    - Observation of current controls
    - Using published third-party standards

Security Baseline

- Selecting relevant metrics among the numerous available choices can be achieved by using a set of criteria. Effective metrics for risk management, including controls for evaluation, can be selected based on the best ranking of the following characteristics:
  - Specific—Based on a clearly understood goal; clear and concise
  - Measurable—Able to be measured; quantifiable (objective), not subjective
  - Attainable—Realistic; based on important goals and values
  - Relevant—Directly related to a specific activity or goal
  - Timely—Grounded in a specific time frame
  - Meaningful—Understood by the recipients
  - Accurate—Reasonably accurate
  - Cost-effective—Not too expensive to acquire or maintain
  - Repeatable—Able to be acquired reliably over time
  - Predictive—Indicative of outcomes
  - Actionable—Clear to the recipient what action to take

2.2.1 Security Baseline

CIS®

OpenSCAP

Compliance Manager

ALERT LOGIC™

2.2.2 Event Effecting Security Baseline

- A number of factors may change the risk, probability or impact equation, necessitating that baseline security be changed.
- Baseline security is determined by the collective ability of controls to protect the enterprise’s information assets.
- Examples:
  - Change Controls
  - Emerging Threats
  - Shadow IT
  - Zero day

2.3 Risk Analysis, Evaluation and Assessment

- Security baselines can help manage risk implications

2.3.1 Risk Management Context

- Important criteria to be considered are:
  - ***Impact***—The kinds of consequences that will be considered
  - ***Likelihood***—The probability of a negatively impacting event occurring
  - ***Cost-benefits analysis*** —To determine the best approach for mitigation versus transferring impact of a risk event
  - ***Risk appetite/risk tolerance*** —The rules that determine whether the risk level is such that further treatment activities are required

Thanks a lot