CYBER 503x
Cybersecurity Risk Management

Unit 2: Risk Management 1

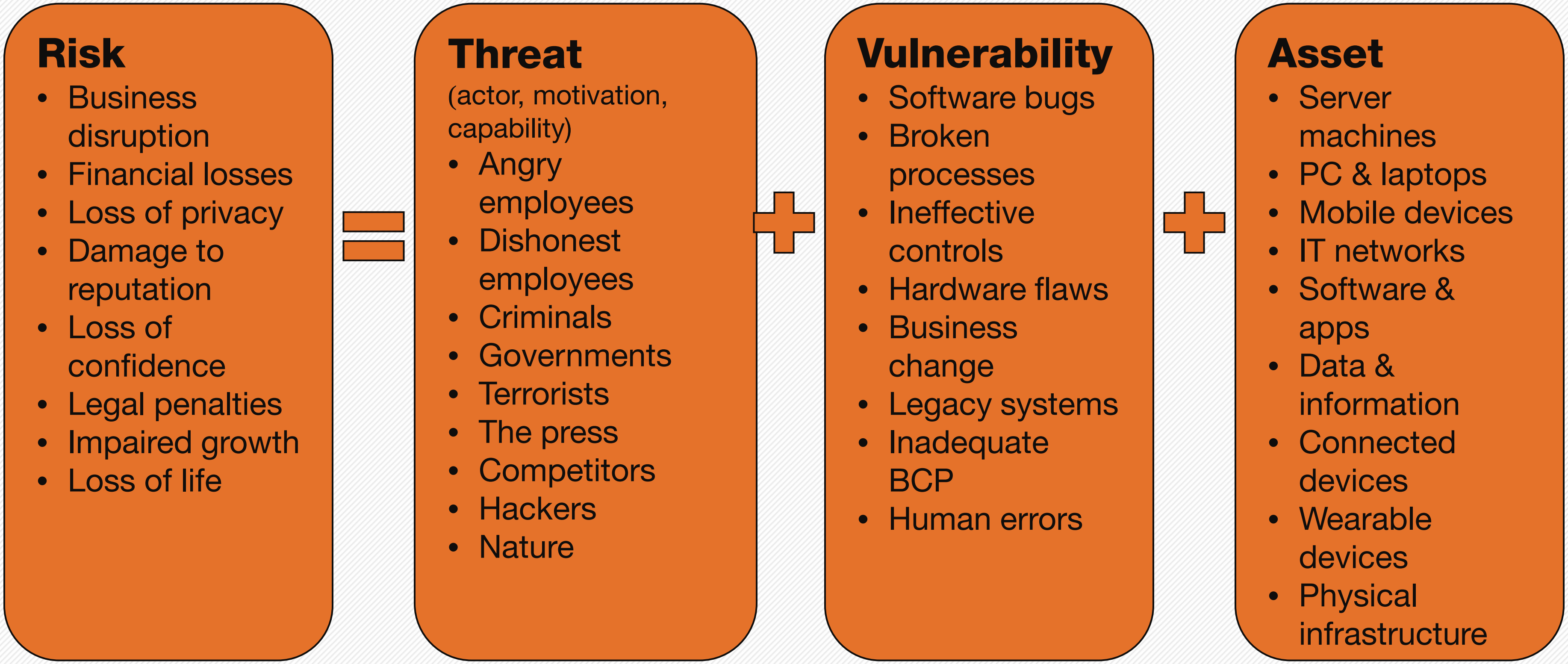
R·I·T

The Origins of Risk Management

- The Shift in philosophy beyond “to buy insurance”:
  - The introduction of “Operations Research” and “Management Science”
  - Emphasis on cost-benefit analysis, expected value, and a scientific approach
    - to decision-making under uncertainty;
  - A shift from descriptive to normative decision theory
- Risk management as a multi-disciplinary subject grew out of a merger of applications in the military and aerospace programs, financial theory, and insurance.

What is Risk?

- Risk is a threat that exploits some vulnerability that could cause harm to an asset.



Risk

- Business disruption
- Financial losses
- Loss of privacy
- Damage to reputation
- Loss of confidence
- Legal penalties
- Impaired growth
- Loss of life

=

Threat

(actor, motivation, capability)

- Angry employees
- Dishonest employees
- Criminals
- Governments
- Terrorists
- The press
- Competitors
- Hackers
- Nature

+

Vulnerability

- Software bugs
- Broken processes
- Ineffective controls
- Hardware flaws
- Business change
- Legacy systems
- Inadequate BCP
- Human errors

+

Asset

- Server machines
- PC & laptops
- Mobile devices
- IT networks
- Software & apps
- Data & information
- Connected devices
- Wearable devices
- Physical infrastructure

Bald Tire Scenario

photo credit: Dennis Yang (flickr.com)

(1)

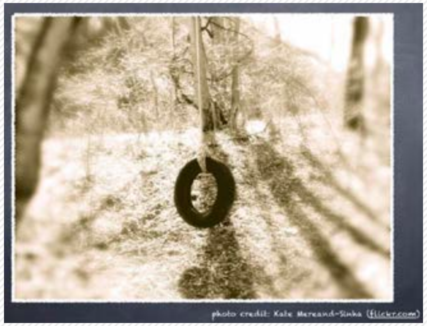


photo credit: Kate Mereand-Sinha (flickr.com)

(2)

photo credit: Tom Beck (flickr.com)

(3)

photo credit: dfinnecy (flickr.com)

(4)

Asset: *“Bald Tire”*

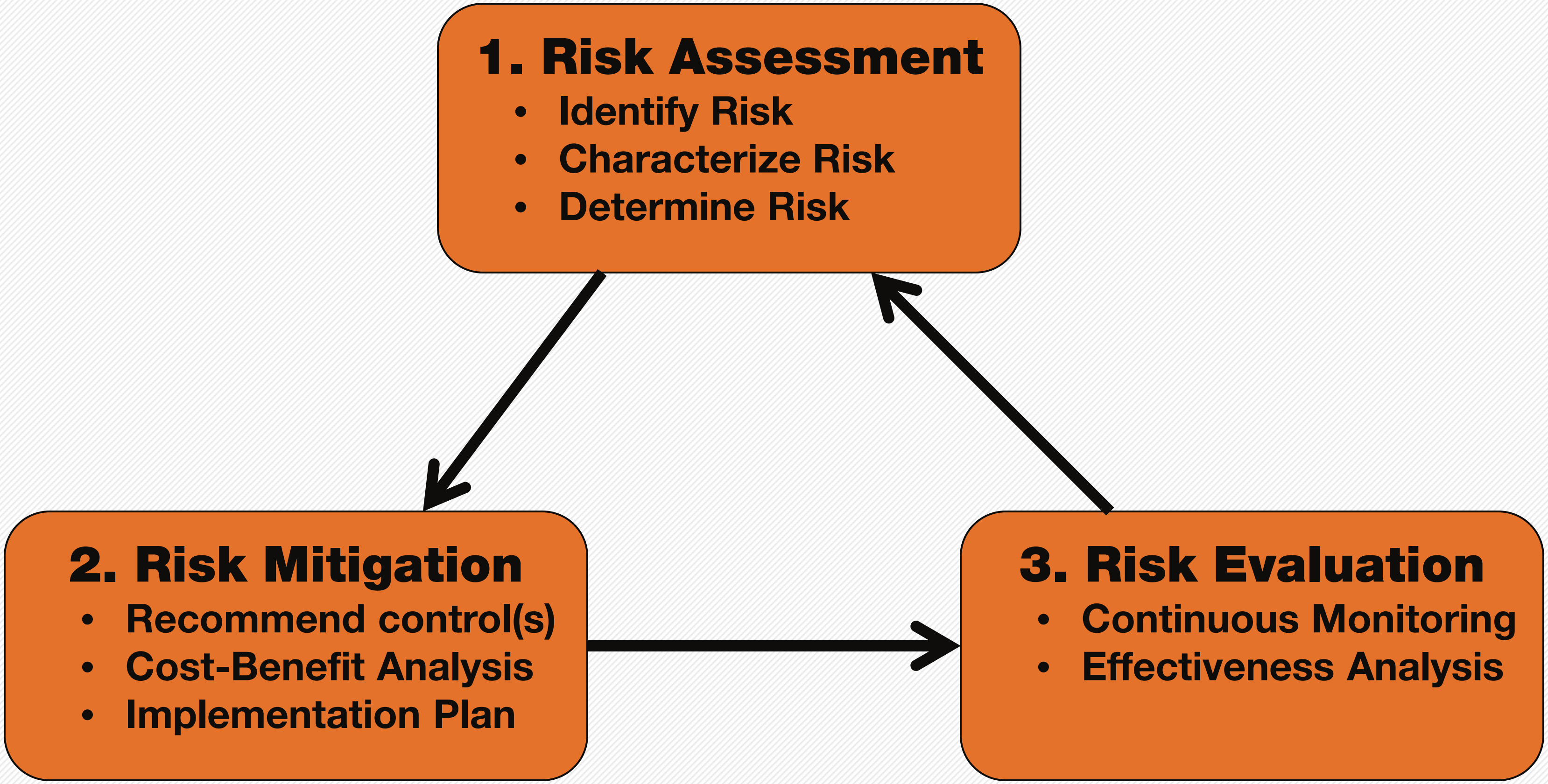
Threat: *the earth and the gravity*

Vulnerability: *frayed rope, cliff, sharp rocks*

Risk: a derived value and has *a likelihood and a magnitude component*

https://www.slideshare.net/pjbeyer/risk-explained-in-5-minutes-or-less

Risk Management Lifecycle



1. Risk Assessment

- Identify Risk
- Characterize Risk
- Determine Risk

2. Risk Mitigation

- Recommend control(s)
- Cost-Benefit Analysis
- Implementation Plan

3. Risk Evaluation

- Continuous Monitoring
- Effectiveness Analysis

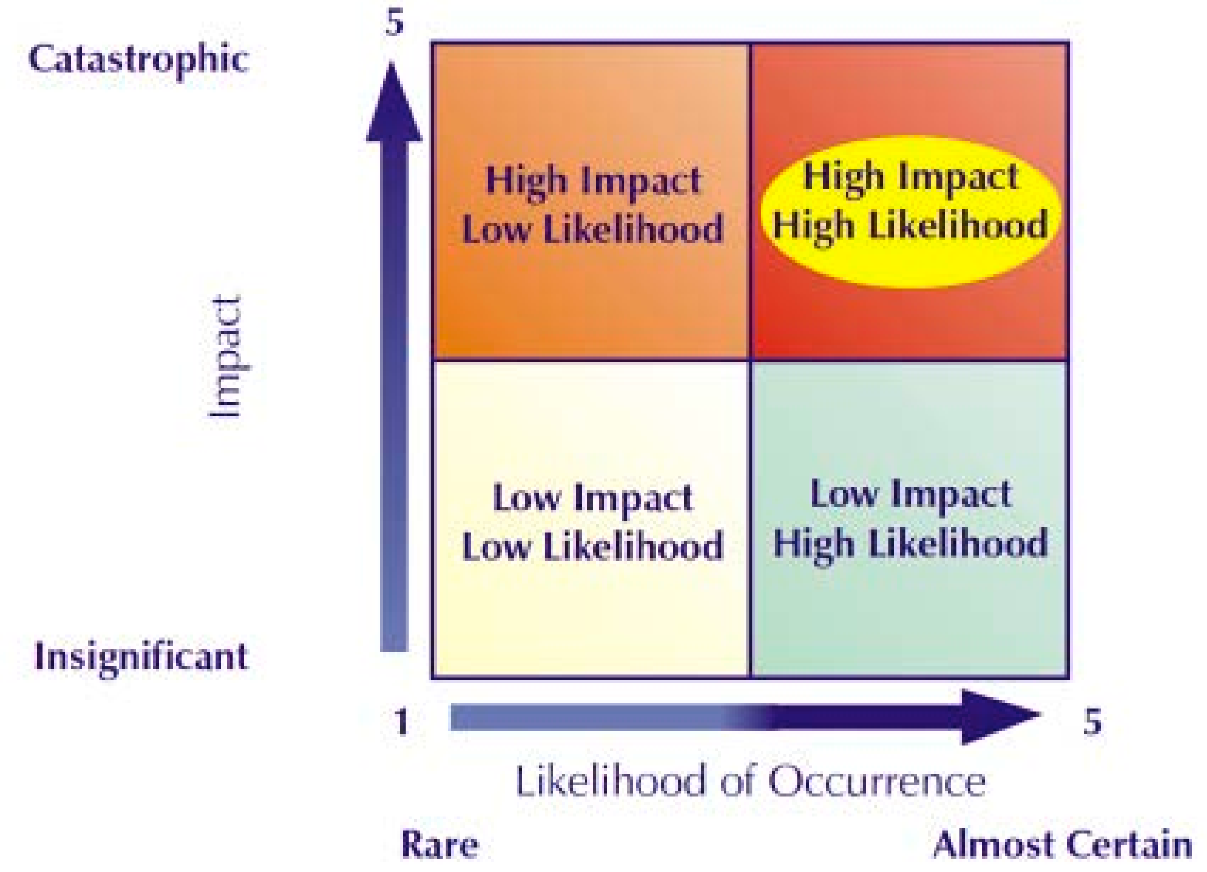
Risk Management Approaches

- Reactive Approach: focus on respond
  - Incident response process
- Proactive Approach: focus on prevent and prepare
  - Quantitative risk assessment
  - Qualitative risk assessment

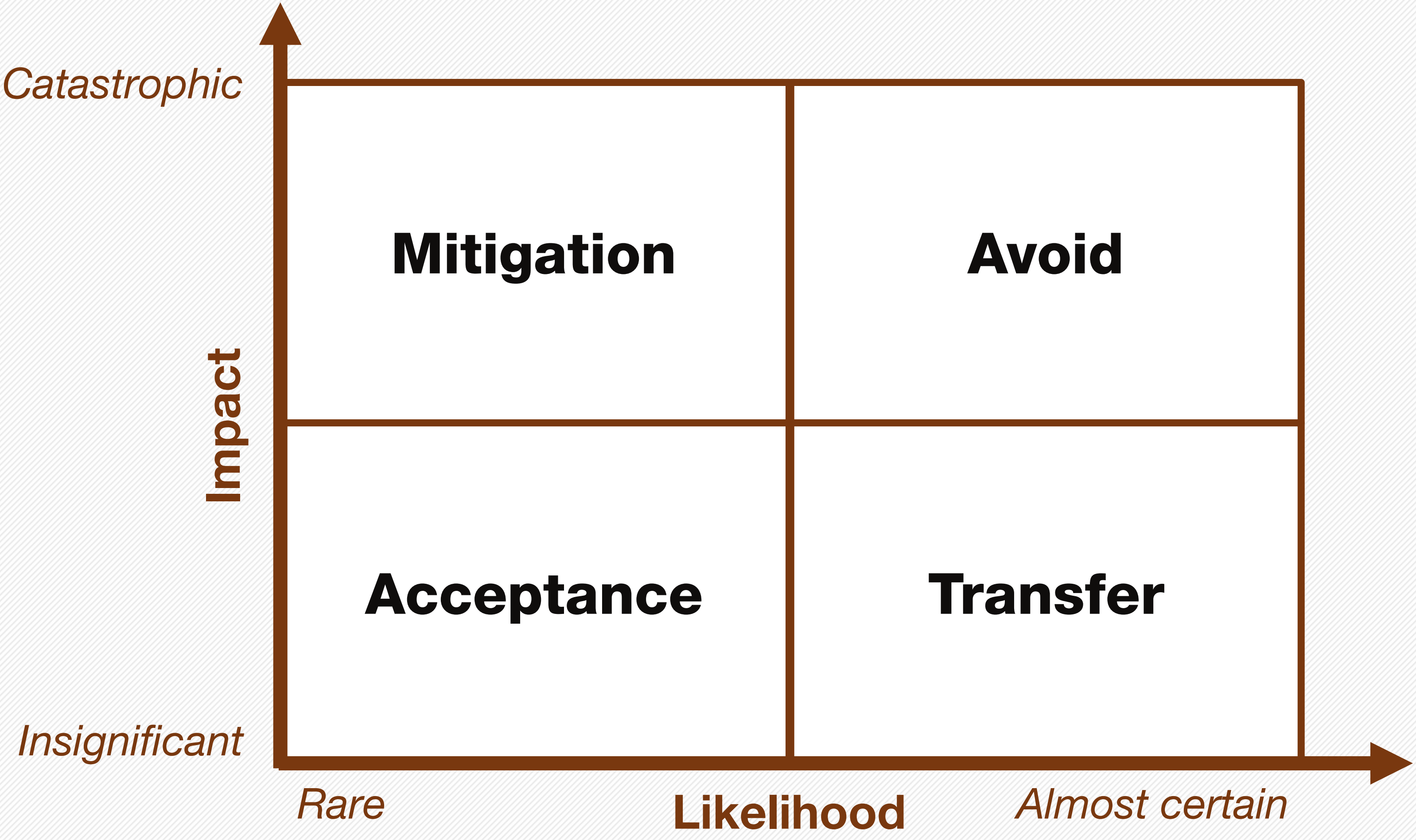
Risk Characterization Methods

- Quantitative risk assessment
  - Leverage quantitative methodologies used by financial institutions and insurance companies
    - Point risk estimate
    - Probability distributions
- Qualitative risk assessment
  - Calculate relative value based on subjective expert knowledge
    - The conventional “Risk Matrix” approach

The Risk Matrix



How is Risk Managed?



Catastrophic

Impact

Insignificant

Mitigation

Avoid

Acceptance

Transfer

Rare

Likelihood

Almost certain

Common Methodologies & Tools

- NIST RMF
- OCTAVE
- FRAP
- COBRA
- Risk Watch
- FAIR

NIST Risk Management Framework

- Step 1: System Characterization
- Step 2: Threat Identification
- Step 3: Vulnerability Identification
- Step 4: Control Analysis
- Step 5: Likelihood Determination
- Step 6: Impact Analysis
- Step 7: Risk Determination
- Step 8: Control Recommendations
- Step 9: Results Documentation

OCTAVE by CMU/SEI

- Workshop-based not tool-based
- Three Phases
  1. Knowledge gather from senior managers on critical assets, threats and protection strategies
  2. Knowledge gather from operational area managers
  3. Knowledge gather from staff
- The outputs
  - Protection Strategy
  - Mitigation Plan
  - Action List

FRAP

- By Thomas Peltier, with a focus on cost-effective risk management techniques
- Formal *qualitative* risk analysis methodologies using
  - Vulnerability Analysis
  - Hazard Impact Analysis
  - Threat Analysis
  - Facilitator + small group of SME through discussions & questionnaires
- Faster and Simpler - requires pre-screening systems
- Integrates with BIA (Business Impact Analysis)

COBRA

- Consultative, Objective and Bi-functional Risk Analysis, created by C&A Systems Security in 1991
- Four primary knowledge bases:
  1. IT Security (or default)
  2. Operational Risk
  3. ‘Quick Risk’ or ‘high level risk’
  4. e- Security
- Two main products
  1. Risk Consultant
  2. ISO Compliance

Risk Watch

- A Software Tool that uses an expert knowledge database
  - walk user through risk assessment
  - Generate reports
- It includes statistical analysis to support quantitative risk assessment, e.g. ROI
- Product Portfolio
  - SecureWatch
  - CyberWatch
  - ComplianceWatch (e.g. HIPPA, Banking, PCI, Nuclear Cybersecurity compliances)

FAIR

- “Measuring and Managing Information Risk: A FAIR Approach” by Dr. Jack Freund and Jack Jones
- A quantitative risk analysis tool and methodology
  - Meaningful measurements for risk factors
  - Not about a checklist and formulas, but about critical thinking
  - Risk can be effectively measured to reduce the management uncertainty about risk
- Shift from a compliance-based to a risk-based approach to InfoSec Risk and IT Risk

Other Related Frameworks & Standards

- COBIT by ISACA
  - RISK IT: includes all types of operational risk in IT, e.g. business continuity

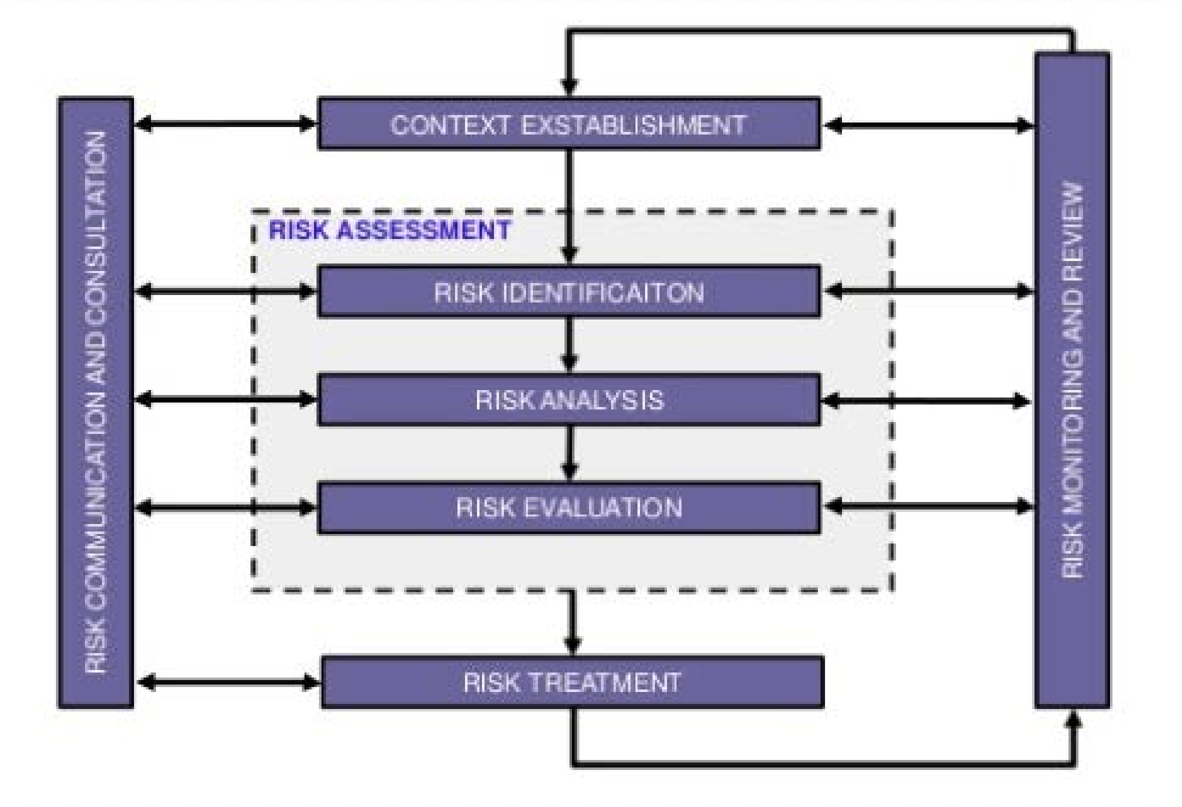
- ISO 27001 and 27002
  - ISO 27005:2008

ISACA's COBIT

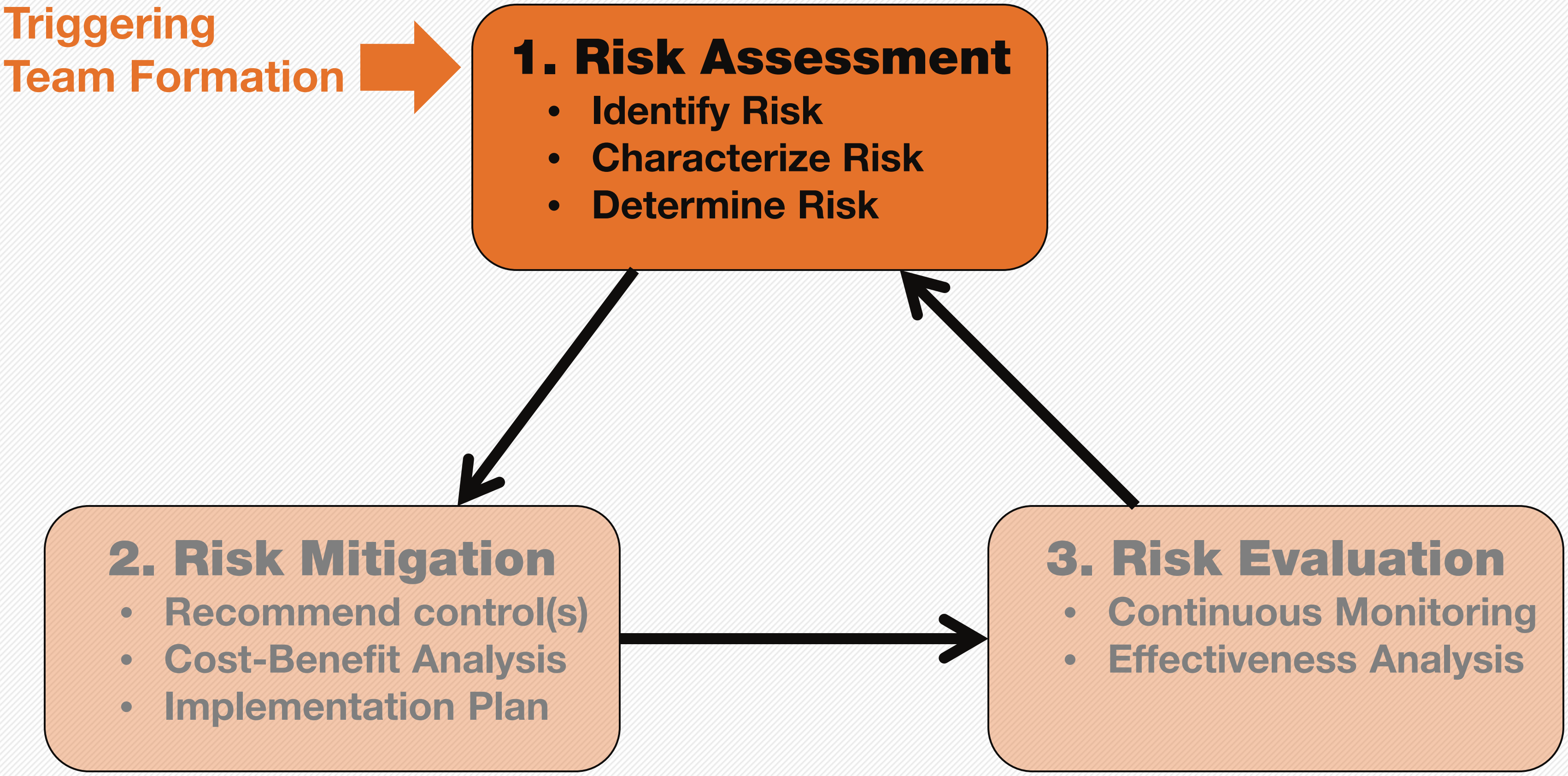
- Control Objectives for Information and related Technology
- COBIT supports IT governance by providing a framework to ensure that
  - IT is aligned with the business
  - IT enables the business and maximizes benefits
  - IT resources are used responsibly
  - IT risks are managed appropriately
- Design to support
  - Executive and management boards
  - Business and IT management
  - Governance, assurance, control and security professionals

Other Related Frameworks & Standards

- ISO 27001 and 27002
  - ISO 27005:2008 – 27005 solely concentrates on security



Risk Assessment



Risk Assessment:
Step 0: Scope, Asset & Team

- Begin with identifying the sponsor, to define what is to be accomplished.
  - What questions to be answered?
  - Business operations or processes: e.g. eCommerce, supply chain management
  - Business application: e.g. payroll processing, human resource management
  - Information asset: e.g. customer data, credit card information
  - Physical asset: e.g. server, data center, sub-network, corporate LAN
- Data gathering approach
  - Questionnaire or Data gathering template
  - Workshop and brainstorming

Information Asset Classification

- Asset Classes
  - High business impact (HBI)
    - Authentication credential, highly sensitive business materials, financial profiles, medical profiles, personally identifiable information, assets subjected to specific regulatory requirements
  - Moderate business impact (MBI)
    - Internal business information (e.g. employee directory, network infrastructure designs, information on internal Web sites)
  - Low business impact (LBI)
    - Organization structure, public cryptographic keys, product brochures, white papers, obsolete business information, read access to publicly accessible web pages.
- Additional References for Information asset classification:
  - NIST Special Publication 800-60 workshops, “Mapping Types of Information and Information Systems to Security Categories”
  - Federal Information Processing Standards (FIPS) publication 199, “Security Categorization of Federal Information and Information Systems)”

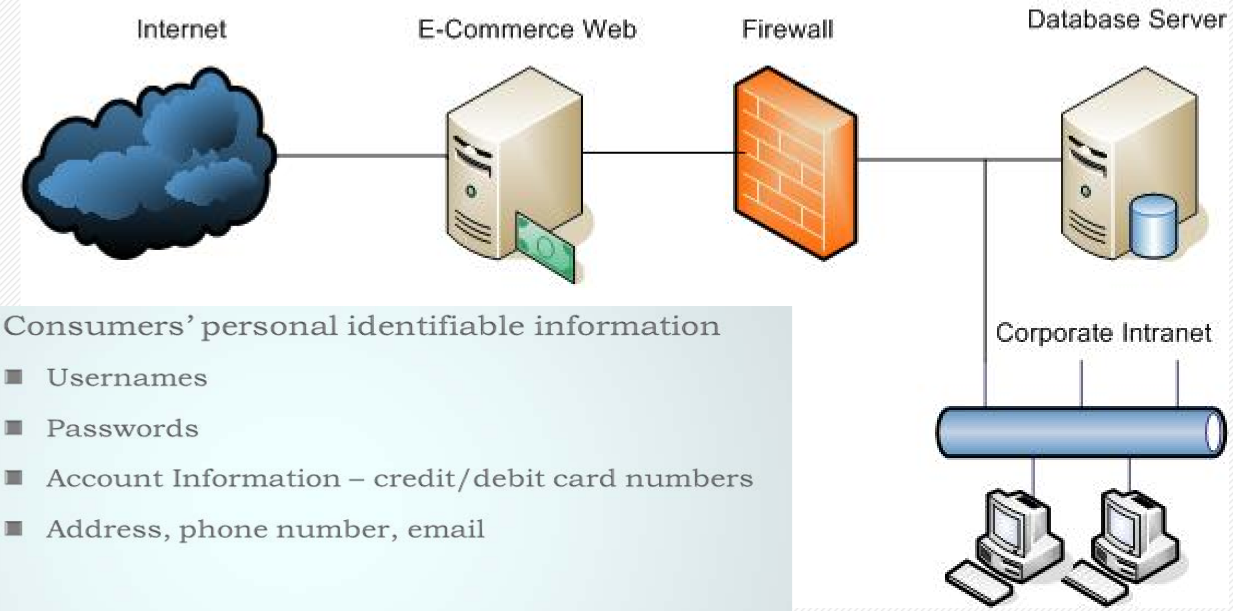
Deliverable for Step 0

- Reach agreement with owners on what the assessment is to review and all relevant parameters
- Assessment scope statement
- Asset specifications and classifications
- Team members with defined roles and responsibility

Risk Management Program Team: Key Roles & Responsibilities

Role	Responsibility
Senior Management	- Incorporate results of the risk management program into the decision making process - Resource allocation & capability development
Information Security Professional	- Responsible for organization security program, including risk management - Held liable if internal controls are not adequate - Determines the probability of impact on business assets
System & Information Owners	- Determine the value of information asset - Ensure the proper controls are in place to address integrity, confidentiality, and availability - Key role in "asset classification policy" - Has authority and responsibility for making cost-benefit decisions
Information Technology Engineering & Operations	- Design & implement technical solutions and estimate engineering costs - Design & implement operational components of solution and estimate operating costs

Example: eCommerce Operation Risk Assessment Scope and Asset



- Consumers’ personal identifiable information
  - Usernames
  - Passwords
  - Account Information – credit/debit card numbers
  - Address, phone number, email
- Information in transit
  - Making a purchase on the website

Asset Classifications

Assets	Confidentiality	Integrity	Availability
User names	LBI	**HBI**	**HBI**
Passwords	**HBI**	**HBI**	**HBI**
Credit/Debit Card Info	**HBI**	**HBI**	**HBI**
Address, phone, email	LBI	MBI	LBI
Purchase transaction (in transit)	LBI	**HBI**	MBI

Risk Assessment:
Step 1: Threat Identification

- **Threat:** The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.
  - Threat Sources (or Actor)
  - Threat Occurrence Rates – L
  - Threat Impact:

    ALE = V x L (V: value of an asset, ALE: Annual Loss Exposure)
- *Example:* You have a $3 million data center located in a flood area. A major flood that would destroy the data center occurs once every 100 years.
  - Value = $3 million
  - Likelihood L = 0.01
  - ALE = $3 million x 0.01 = $30,000

Actors, Motivators, and Threats

Actor	Motivation	Threat
External hacker (Script-kiddies)	Curiosity Ego	System hacking Spoofing
Internal hacker	Financial gain Disenchantment	Fraud Poor documentation
Cybercriminal	Profit Ideology	DDoS, Phishing, Ransomware Credit card fraud, cyber stalking
Nation-State Hacker	Power Revenge	Critical infrastructure attacks Multi-stage, multi-vector attacks
Poorly trained employee	Unintentional errors	Corruption of data Malicious code introduced
Cracker	Monetary gain Unauthorized data alteration	Social engineering System intrusion Impersonation

New Threat Landscape

- Nature of threats changing
- Today’s attacks sophisticated and successful
- Network perimeter dissolving
- Existing detection techniques failing:
  - Coordinated Persistent Threat Actors
  - Dynamic, polymorphic malware
  - Multi-vector attacks
  - Multi-stage attacks

Threat Intelligence

- What is it?
  - Threat Intelligence is the knowledge extracted from relevant data and information that helps you identify threats and make informed decisions.
- Intelligence Typologies
  - **Operational Intelligence:** produced entirely by computers, e.g. automatic detection of DDoS
  - **Strategic Intelligence:** produced by human analysts

Risk Assessment: Step 3: Vulnerability Identification

- The use of vulnerability sources (e.g. previous risk assessment documents, audit reports, system test and evaluation reports)
  - NIST I-CAT vulnerability database (http://icat.nist.gov)
  - National Vulnerability Database (NVD – http://nvd.nist.gov)
  - Common Vulnerability and Exposures (CVE – http://cve.mitre.org)
  - Commercial computer incident/emergency response teams and post lists (e.g. SecurityFocus.com forum mailings)
- System security testing (proactive methods)
  - Automated vulnerability scanning tools
  - Security test and evaluation
  - Penetration testing
- Development of security requirements checklist
  - Management (e.g. Continuity of support, incident response capability, assignment of responsibilities, risk assessment, etc.)
  - Operational (e.g. facility protection, workstation, laptops, external data distribution and labeling)
  - Technical (e.g. cryptography, discretionary access control, identification and authentication, intrusion detection, system audit, etc.)

Risk Assessment:
Step 3: Vulnerability Identification

Vulnerability	Threat-Source	Threat Action
Terminated employees' system ID are not removed from the system	Terminated employees	Dialing into the company's network and accessing company proprietary data.
Company firewall allows inbound telnet, and guest ID is enabled on XYZ server.	Unauthorized users (e.g. hackers, computer criminals, terrorists)	Using telnet to XYZ server ad browsing system files with the guest ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied.	Unauthorized users	Obtaining unauthorized access to sensitive system files based on known system vulnerability.