Risk Management

Content

1) What is Risk?

2) What is Threat?

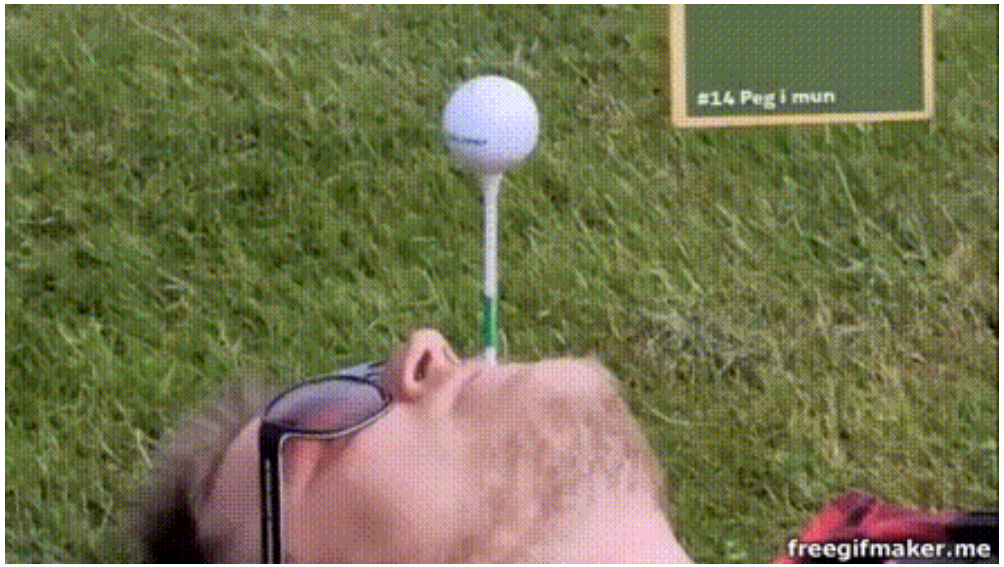
3) What is Vulnerability?

4) Risk Analysis

5) Enterprise Risk Management Model

6) Risk Management Framework

What is Risk?



"Risk is the probability of a negative (harmful) event occurring as well as the potential of scale of that harm."

What is Threat?

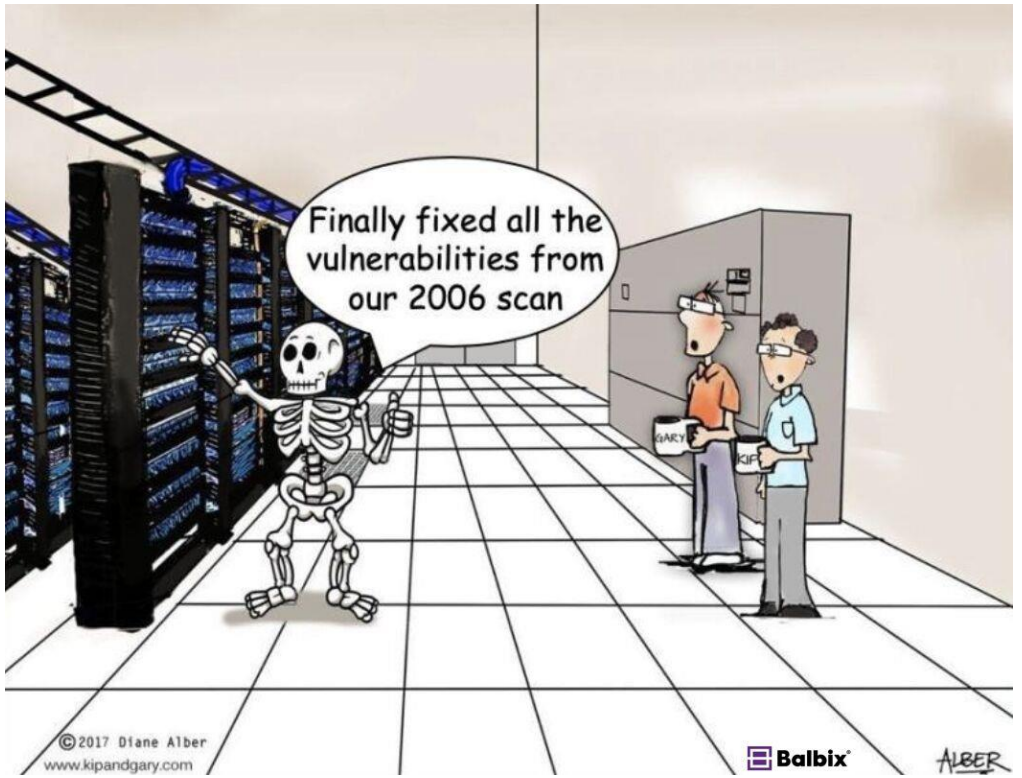
"An expression of intention to inflict evil injury or damage"

"Attacks against key security services Confidentiality, integrity, availability"

Examples of Threats

- T01 Access (Unauthorized to System - logical)
- T02 Access (Unauthorized to Area - physical)
- T03 Airborne Particles (Dust)
- T04 Air Conditioning Failure
- T05 Application Program Change (Unauthorized)
- T06 Bomb Threat
- T07 Chemical Spill
- T08 Civil Disturbance
- T09 Communications Failure
- T10 Data Alteration (Error)
- T11 Data Alteration (Deliberate)
- T12 Data Destruction (Error)
- T13 Data Destruction (Deliberate)
- T14 Data Disclosure (Unauthorized)
- T15 Disgruntled Employee
- T16 Earthquakes
- T17 Errors (All Types)
- T18 Electro-Magnetic Interference
- T19 Emanations Detection
- T20 Explosion (Internal)
- T21 Fire, Catastrophic
- T22 Fire, Major
- T23 Fire, Minor
- T24 Floods/Water Damage
- T25 Fraud/Embezzlement
- T26 Hardware Failure/Malfunction
- T27 Hurricanes
- T28 Injury/Illness (Personal)
- T29 Lightning Storm
- T30 Liquid Leaking (Any)
- T31 Loss of Data/Software
- T32 Marking of Data/Media Improperly
- T33 Misuse of Computer/Resource
- T34 Nuclear Mishap
- T35 Operating System Penetration/Alteration
- T36 Operator Error
- T37 Power Fluctuation (Brown/Transients)
- T38 Power Loss
- T39 Programming Error/Bug
- T40 Sabotage
- T41 Static Electricity
- T42 Storms (Snow/Ice/Wind)
- T43 System Software Alteration
- T44 Terrorist Actions
- T45 Theft (Data/Hardware/Software)
- T46 Tornado
- T47 Tsunami (Pacific area only)
- T48 Vandalism
- T49 Virus/Worm (Computer)
- T50 Volcanic Eruption

What is Vulnerability ?



"A vulnerability is a flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by a threat."

Examples of Vulnerability

•Physical

- •V01 Susceptible to unauthorized building access
- •V02 Computer Room susceptible to unauthorized access
- •V03 Media Library susceptible to unauthorized access
- •V04 Inadequate visitor control procedures
- •(and 36 more)

•Administrative

- •V41 Lack of management support for security
- •V42 No separation of duties policy
- •V43 Inadequate/no computer security plan policy
- •V47 Inadequate/no emergency action plan
- •(and 7 more)

•Personnel

- •V56 Inadequate personnel screening
- •V57 Personnel not adequately trained in job
- •...

•Software

- •V62 Inadequate/missing audit trail capability
- •V63 Audit trail log not reviewed weekly
- •V64 Inadequate control over application/program changes

Communications

- *•V87 Inadequate communications system*
- *•V88 Lack of encryption*
- *•V89 Potential for disruptions*
- *•...*

•Hardware

- *•V92 Lack of hardware inventory*
- *•V93 Inadequate monitoring of maintenance*

personnel

- *•V94 No preventive maintenance program*
- *•…*
- *•V100 Susceptible to electronic emanations*

Risk Analysis Assessment Management

- A **risk analysis** involves identifying the most probable threats to an organization and analyzing the related vulnerabilities of the organization to these threats.

- A **risk assessment** involves evaluating existing security and controls and assessing their adequacy relative to the potential threats of the organization.

- **Risk management** is the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analyzing, evaluating, treating, monitoring and communicating risk.

Basic Risk Analysis Structure

- An analytic discipline with three parts:
  - Risk assessment: determine what the risks are
  - Risk management: evaluating alternatives for mitigating the risk
  - Risk communication: presenting this material in an understandable way to decision makers and/or the public

- Evaluate:
  - Value of computing and information assets
  - Vulnerabilities of the system
  - Threats from inside and outside
  - Risk priorities

Basic Risk Analysis Structure

- Examine:
  - Availability of security countermeasures
  - Effectiveness of countermeasures
  - Costs (installation, operation, etc.) of countermeasures
- Implement and Monitor
- **Benefits of Risk Analysis:**
  - Assurance that greatest risks have been identified and addressed
  - Increased understanding of risks
  - Mechanism for reaching consensus
  - Support for needed controls
  - Means for communicating results

What is Control?

- Mechanisms or procedures for mitigating vulnerabilities
  - Prevent
  - Detect
  - Recover
- Understand cost and coverage of control.
- Controls follow vulnerability and threat analysis.

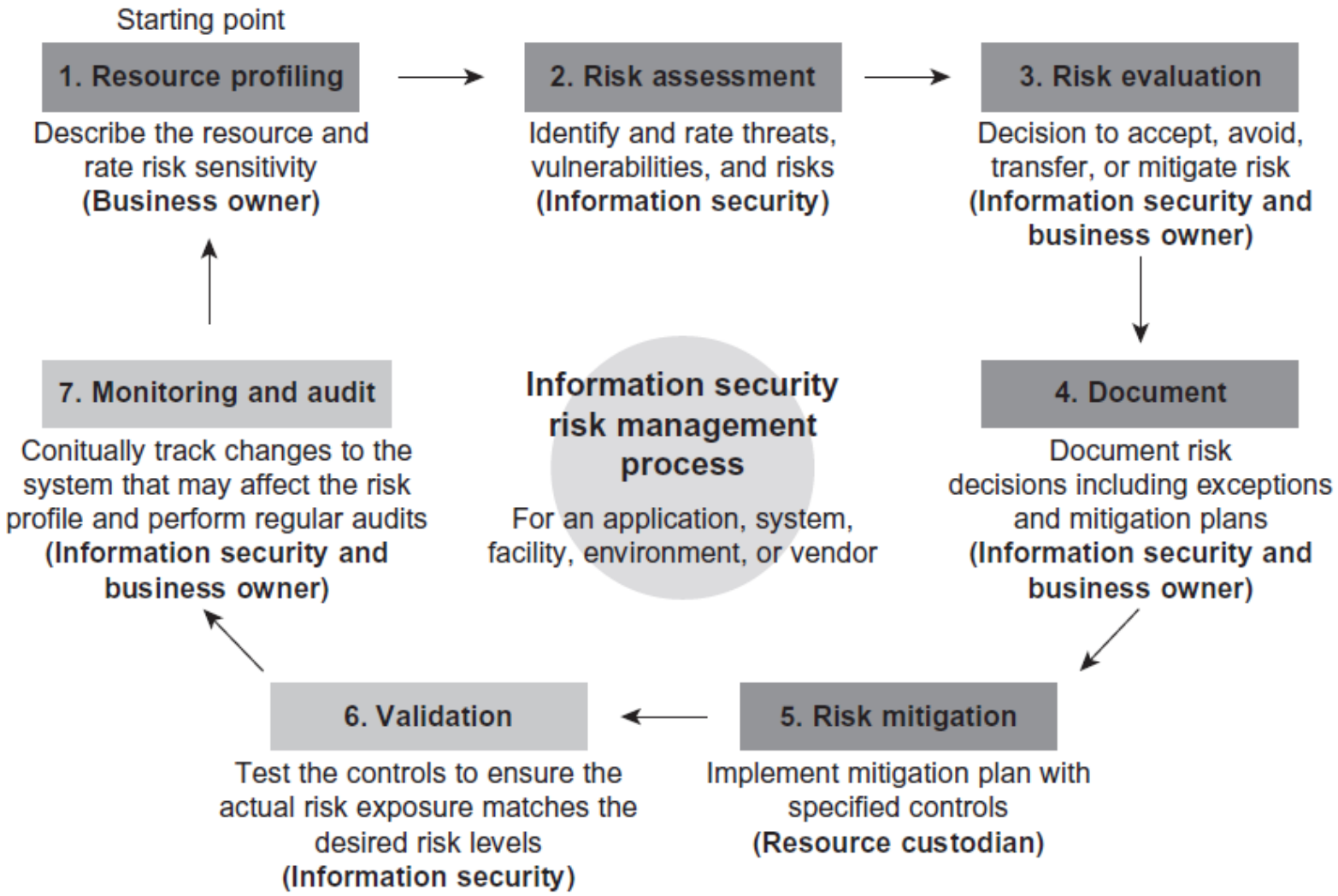
Examples of Control

- C01 Access control devices - physical
- C02 Access control lists - physical
- C03 Access control - software
- C04 Assign ADP security and assistant in writing
- C05 Install-/review audit trails
- C06 Conduct risk analysis
- C07Develop backup plan
- C08 Develop emergency action plan
- C09 Develop disaster recovery plan
- ...
- C21 Install walls from true floor to true ceiling
- C22 Develop visitor sip-in/escort procedures
- C23 Investigate backgrounds of new employees
- C24 Restrict numbers of privileged users
- C25 Develop separation of duties policy
- C26 Require use of unique passwords for logon
- C27 Make password changes mandatory
- C28 Encrypt password file
- C29 Encrypt data/files
- C30 Hardware/software training for personnel
- C31Prohibit outside software on system
- ...
- C47 Develop software life cycle development program
- C48 Conduct hardware/software inventory
- C49 Designate critical programs/files
- C50 Lock PCs/terminals to desks
- C51 Update communications system/hardware
- C52 Monitor maintenance personnel
- C53 Shield equipment from electromagnetic interference/emanations
- C54Identify terminals

What is Risk Management ?

- "A process for identifying, prioritizing and managing risk to an acceptable level within the organization."
- There are two strategies for Risk Management:
  - Reactive: A process that responds to security events as they occur.
  - Proactive: A process that reduces the risk of new vulnerabilities in your organization.

Risk Management Process



Types of Risk Analysis

- **Qualitative:**
- Ideally, we would map out every possible threat and outcome, do lengthy research to calculate a precise likelihood of occurrence, and perform hands-on testing of every compensating control for effectiveness.

- But, unfortunately, this just isn't practical. You need a quick, yet accurate and consistent, methodology to separate the critical risks from the ones you just have to live with.

- This is qualitative analysis. It will never be as precise as a quantitative approach, but it can be structured and flexible at the same time.

Types of Risk Analysis

❑**Qualitative :**

Table 6.11 Qualitative Severity Scale, 4-Level

Level	Description
Low	May be a deviation from recommended practice or an emerging standard. May lack a security governance process or activity, but have no direct exposure.
Moderate	May indirectly contribute to unauthorized activity or just have no known attack vector. May result in a degradation of service and/or a noticeable decrease in service performance.
High	May allow limited access to or control of the application, system, or communication, including only certain data and functionality. May result in a short disruption of service and/or denial of service for part of the user community.
Critical	May allow full access to or control of the application, system, or communication, including all data and functionality. May result in a prolonged outage affecting all users of the service.

Types of Risk Analysis

❑Qualitative:

Table 6.12 Qualitative Likelihood Scale, 5-Level

Level	Description
Negligible	The threat source is part of a small and trusted group, controls prevent exploitation without physical access to the target, significant inside knowledge is necessary, or purely theoretical.
Low	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.
Moderate	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
High	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Very High	Exposure is apparent through casual use or with publicly available information, and the weakness is accessible publicly on the Internet.

Types of Risk Analysis

❑**Qualitative:** Risk Matrix

		Severity			
		Critical	**High**	**Moderate**	**Low**
Likelihood	**Very high**	Critical	Critical	High	Moderate
	High	Critical	Critical	High	Low
	Moderate	High	High	Moderate	Low
	Low	Moderate	Moderate	Low	Low
	Negligible	Low	Low	Low	Low

Types of Risk Analysis

- **Quantitative:**
- Most commonly, you will see professionals in the security field using a qualitative approach to rating risk exposures because we just don't have enough easily accessible historical data to calculate the probabilities and magnitudes of risks like an insurance actuary or financial analyst would.
- Many quantitative models have been proposed over the years with very complex equations for calculating risk, but this relies heavily on having both accurate historical data about previous breaches and a lot of time to devote to the analysis. For example, a textbook quantitative model is the calculation of the Annualized Loss Expectancy (ALE).

Types of Risk Analysis

- **Quantitative:**

- 1. Identify and value assets
- 2. Determine vulnerabilities and impact
- 3. Estimate likelihood of exploitation
- 4. Compute Annual Loss Exposure (ALE)
- 5. Survey applicable controls and their costs
- 6. Project annual savings from control
- 7. Assigns real numbers to costs of safeguards and damage
- 8. Probability of event occurring
- 9. Can be unreliable/inaccurate

Types of Risk Analysis

- **Quantitative:**

- Risk = Risk impact x Risk Probability
  - Loss of car: risk impact is cost to replace car, e.g. $10,000
  - Probability of car loss: 0.10
  - Risk = 10,000 x 0.10 = 1,000

- Generally measured per year
  - Annual Loss Exposure (ALE)

Types of Risk Analysis

- **Quantitative:**

- **Step 1: Identify Scope**
  - Bound the problem

- **Step 2: Assemble team**
  - Include subject matter experts, management in charge of implementing, users

- **Step 3: Identify Threats**
  - Pick from lists of known threats
  - Brainstorm new threats
  - Mixing threats and vulnerabilities here…

Types of Risk Analysis

- **Quantitative:**

- **Step 4: Threat prioritization**
- Prioritize threats for each asset
  - Likelihood of occurrence
- Define a fixed threat rating
  - E.g., Low(1) … High(5)
- Associate a rating with each threat
- Approximation to the risk probability in quantitative approach

Types of Risk Analysis

- **Quantitative:**

- **Step-5: Loss Impact**
- With each threat determine loss impact
- Define a fixed ranking
  - E.g., Low(1) … High(5)
- Used to prioritize damage to asset from threat

- **Step-6: Total Impact**
  - Sum of threat priority and impact priority

Threat	Threat Priority	Impact Priority	Risk Factor
Fire	3	5	8
Water	2	5	7
Theft	2	3	5

Types of Risk Analysis

❑Quantitative:

❑ Step-7: Identify Controls/Safeguards

- ❑Potentially come into the analysis with an initial set of possible controls
- ❑Associate controls with each threat
- ❑Starting with high priority risks

❑ Step-8:

- ❑Do cost benefits and coverage analysis

❑Step-9:

- ❑Rank controls

Threat	Risk Factor	Possible Safeguard	Safeguard cost
Fire	8	Fire supression system	$15,000.00
Tornado	8	Business Continuity Plan	$75,000.00
Water Damage	7	Business Continuity Plan	$75,000.00

Types of Risk Analysis

- **Quantitative:**

- **Step 10: Communicate Results**

- Most risk analysis projects result in a written report
  - Generally not read
  - Make a good executive summary
  - Beneficial to track decisions.

- Real communication done in meetings and presentations

Types of Risk Analysis

	Benefits	Drawbacks
Quantitative	• Risks prioritized by financial impact; assets prioritized by their financial values • Results facilitate management of risk by return on security investment • Results can be expressed in management-specific terminology	• Impact values assigned to risks are based upon subjective opinions of the participants • Very time-consuming • Can be extremely costly
Qualitative	• Enables visibility and understanding of risk ranking • Easier to reach consensus • Not necessary to quantify threat frequency • Not necessary to determine financial values of assets	• Insufficient granularity between important risks • Difficult to justify investing in control as there is no basis for a cost-benefit analysis • Results dependent upon the quality of the risk management team that is created

Enterprise Risk Management Model

- Risk Identification: What can go wrong? List all possible events that could occur in a subsystem if there are no controls. Once risks are identified, combine like risks according to the following key areas impacted by the risks: people, mission, physical assets, financial assets, and customer/stakeholder trust.

- Risk Analysis: What is the likelihood and impact? Rate risks according to probability and impact.

- Requirements Identification: What is in place to prevent it? List all controls that would exist without subsystem specific controls.

Enterprise Risk Management Model

- Controls Identification: What else is needed to control the risk? Where there is a significant or extreme risk rating, list gaps between existing risks and existing controls.

- Risk Registry: What documentation is needed so that the logic and conclusions are clear? Create a register that documents the results of the risk evaluation, including the events, probabilities, impacts, and risk management strategy.

Enterprise Risk Management Model

- For each subsystem a group of senior level staff and subject matter experts complete the following

- **1.Risk Identification:** What can go wrong? What events can have an impact on people, mission, physical assets, financial assets, and customer/stakeholder trust? A risk can also be a missed opportunity for improving effectiveness and efficiency.

- **2.Risk Analysis:** Look at the subsystem in the context of existing external controls. If there were no specific controls what is the probability and impact of specific risks?

Enterprise Risk Management Model

- **3. Requirements Identification:** What is in place to prevent it? List all controls that would exist without subsystem specific controls.

- **4. Controls Identification:** What else is needed to control the risk? Where there is a significant or extreme risk rating, list gaps between existing risks and existing external controls . Defer to existing external controls and standards whenever possible.

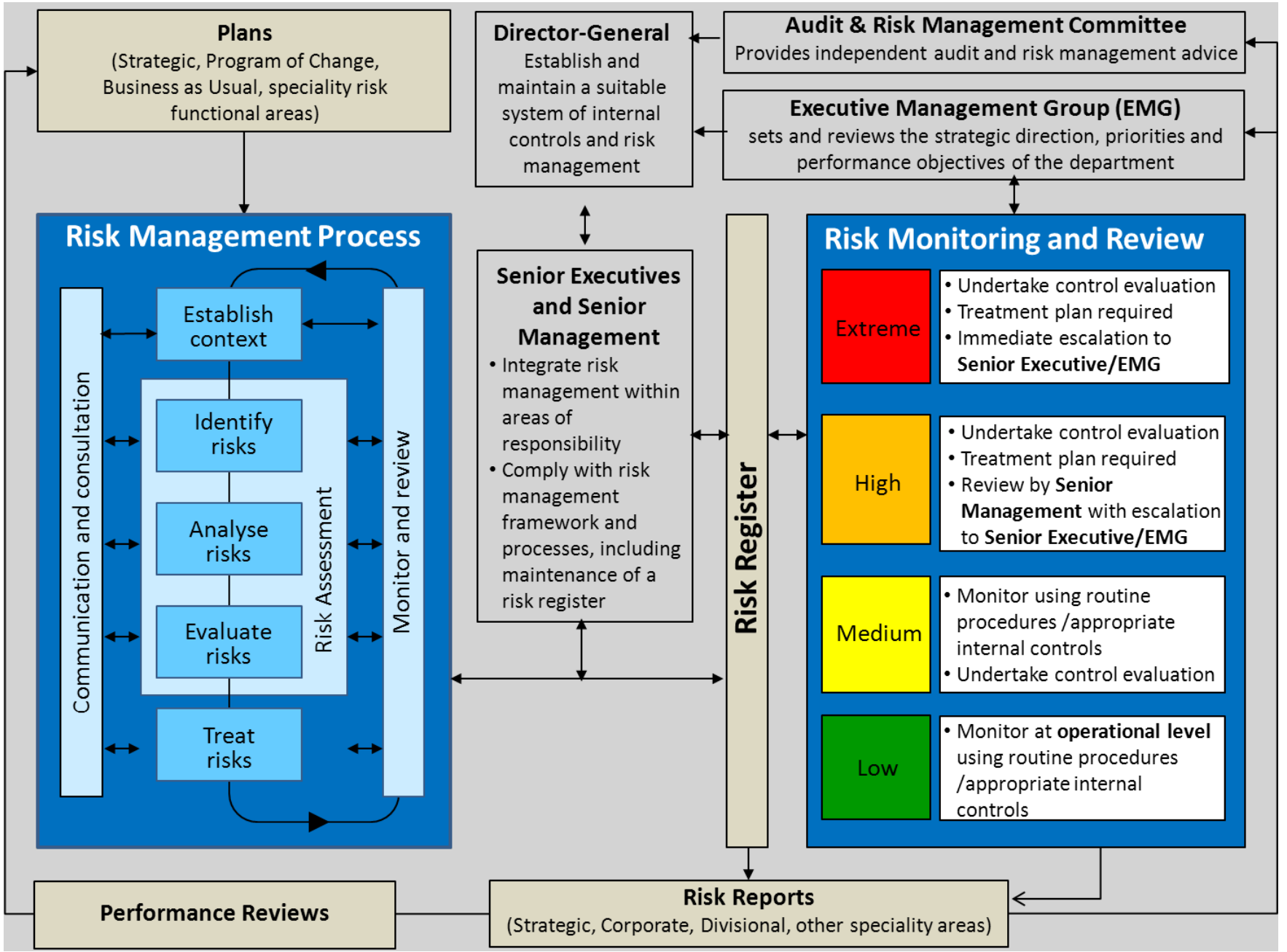
- **5. Risk Registry:**
  - Clearly document the analysis of identified risks, existing controls, and proposed controls to address any serious gap between existing controls and risk.
  - Risk Mitigation Options Acceptance, Monitoring, Mitigation, and Avoidance
  - Evaluate the costs of various mitigation techniques compare the cost/benefit of the risk

Enterprise Risk Management Model

❑5. Risk Registry:

Risk/ Opportunity	Risk Level	Potential Cost/Benefit	External Control(s)	Proposed Mitigation Technique	Internal Control (if needed)
Identify specific risks and their risk level	Minor, Moderate, Significant and Extreme – based on the probability and impact chart.	Give a rough estimate of the magnitude of the cost/benefit of the risk/opportunity without specific controls.	List all external controls that help address the risks and opportunity identified.	Based on any gap between the risk/opportunity and existing controls, what strategy should adopt?	List all internal controls needed to effectively and efficiently address gaps between risks and external controls.

Risk Management Framework



References

[1] Wheeler, E. (2011). Security risk management: Building an information security risk management program from the Ground Up. Elsevier.

[2] Weiss, M., & Solomon, M. G. (2015). Auditing IT infrastructures for compliance. Jones & Bartlett Publishers.

Truth, Transparency and Tactics Are the Characteristics of a good Auditor