SEC-202: Secure Start-Up

Lecture 4 – Governance, Risk, and Compliance (GRC)

Translating "Tech" into "Business Risk" and "Law." This lecture moves away from firewalls and code to focus on rules, strategy, and proving security to the world.

Instructed By:

Dr. Charnon Pattiyanon

Assistant Director of IT and Instructor
CMKL University

Artificial Intelligence and Computer Engineering (AICE) Program

Class Agenda

- Defining GRC
- The Documentation Hierarchy
- Risk Assessment
- The Risk Register
- Treating Risk (The 4 Ts)
- Key Compliance Frameworks
- Privacy Regulations (GDPR & CCPA)
- Vulnerability Management Lifecycle
- Exception Management (Risk Waivers)
- Vendor Risk Management (Third-Party Risk)
- Audits (Internal vs. External)

Defining GRC

- **Governance (The Strategy):**
  - How the organization is directed and controlled.
  - Ensures security aligns with business goals (e.g., "We are a security-first bank").

- **Risk (The Uncertainty):**
  - Identifying, analyzing, and responding to potential threats.
  - Quantifying "What could go wrong?"

- **Compliance (The Rules):**
  - Adherence to external laws (GDPR), regulations (HIPAA), and contracts.
  - Golden Rule: "Compliance is not Security." (You can be compliant and still get hacked).

The Documentation Hierarchy

- **Policy (The "Why"):**
  - High-level intent set by senior leadership.
  - Mandatory.
  - Example: "All company devices must be encrypted."
- **Standard (The "What"):**
  - Specific technical requirements or metrics.
  - Mandatory.
  - Example: "Encryption must use AES-256 with a TPM chip."
- **Procedure (The "How"):**
  - Step-by-step instructions (SOPs).
  - Example:
    "1. Open Settings. 2. Click Security. 3. Enable BitLocker."
- **Guideline:**
  - Recommended best practices.
  - Optional.

Risk Assessment Methodologies

Qualitative Assessment

- Uses descriptive scales: **Low** / **Medium** / **High**.
- **Pros:** Quick, easy to communicate to non-technical staff.
- **Cons:** Subjective.
  (My "High" risk might be your "Medium").

Qualitative Assessment

- Uses numerical financial data: **Annual Loss Expectancy (ALE)**

Single Loss Expectancy

$$ALE = SLE \times ARO$$

Annual Rate of Occurence

- **Pros:** Helps justify budgets (ROI).
- **Cons:** Hard to get accurate data for cyber events.

Generalization of the Risk Definition

- **Risk** is commonly measured as **a pair** of **the probability of occurrence of an event**, and **the outcomes or consequences** associated with the event's occurrence.

$$\boldsymbol{Risk} = \{(p_1, c_1), (p_2, c_2), \dots, (p_n, c_n)\}$$

where p_i= occurrence probability of an outcome or event i,
and c_i= occurrence consequences or outcome of the event i.

Risk is also measured as the **product** of **likelihood** of occurrence and the **impact** severity of occurrence of the event:

$$\boldsymbol{RISK}\left(\frac{Consequence}{Time}\right) = \boldsymbol{LIKELIHOOD}\left(\frac{Event}{Time}\right) \times \boldsymbol{IMPACT}\left(\frac{Consequence}{Event}\right)$$

- A generalized expression for risk is given as:

$$\boldsymbol{Risk} = \{(l_1, o_1, u_1, cs_1, po_1), (l_2, o_2, u_2, cs_2, po_2), \dots, (l_n, o_n, u_n, cs_n, po_n)\}$$

where
- l_i = occurrence likelihood of the event i,
- o_i = occurrence outcome of the event i,
- u_i = utility or significance of the occurrence event i,
- cs_i= causal scenarios of the event i, and
- po_i= population affected by the outcome of the event i.

Generalization of the Risk Definition

- Since risk can be assessed in terms of the likelihood of occurrence, probabilistic algebra can be applied to summarize and quantify the overall risk level.
- The **occurrence probability (p)** of **an outcome (o)** can be decomposed into **an occurrence probability of an event or threat (t)**, and **the outcome-occurrence probability given the occurrence of the event ($o|t$)**.
- The **occurrence probability of an outcome** can be expressed as follows:

$$Pr(o) = Pr(t)\, Pr(o|t)$$

Identifying Risk – The Risk Register

- **The "Source of Truth":** A central database (or spreadsheet) tracking all known security risks.

ID	Risk description	Risk category	Risk assessment			Risk response type	Risk response description	Risk response cost	Risk owner	Status
			Likelihood	Impact	Exposure rating					
R.1	[Web application] is using a deprecated and unsecure protocol. If exploited, this vulnerability could allow a hacker to decrypt web app traffic.	System and Information Integrity	Moderate	Moderate	Moderate	Mitigate	Upgrade [web application]'s authentication protocol. Have all the tools necessary to perform this upgrade.	$0	[Engineer]	Open
R.2										
R.3										

Prioritizing Risk – The Risk Matrix

- Risk can be presented and assessed using matrices for preliminary screening by **subjectively estimating probabilities and consequences in a qualitative manner**.
- A risk matrix is a two-dimensional presentation of likelihood and consequences using qualitative metrics for both dimensions.

Likelihood Categories

Category	Description	Annual Probability Range
A	Likely	> 0.1 (1 in 10)
B	Unlikely	≥ 0.01 (1 in 100), but < 0.1
C	Very Unlikely	≥ 0.001 (1 in 1,000), but < 0.01
D	Doubtful	≥ 0.0001 (1 in 10,000), but < 0.001
E	Highly Unlikely	≥ 0.00001 (1 in 100,000), but < 0.0001
F	Extremely Unlikely	< 0.00001 (1 in 100,000)

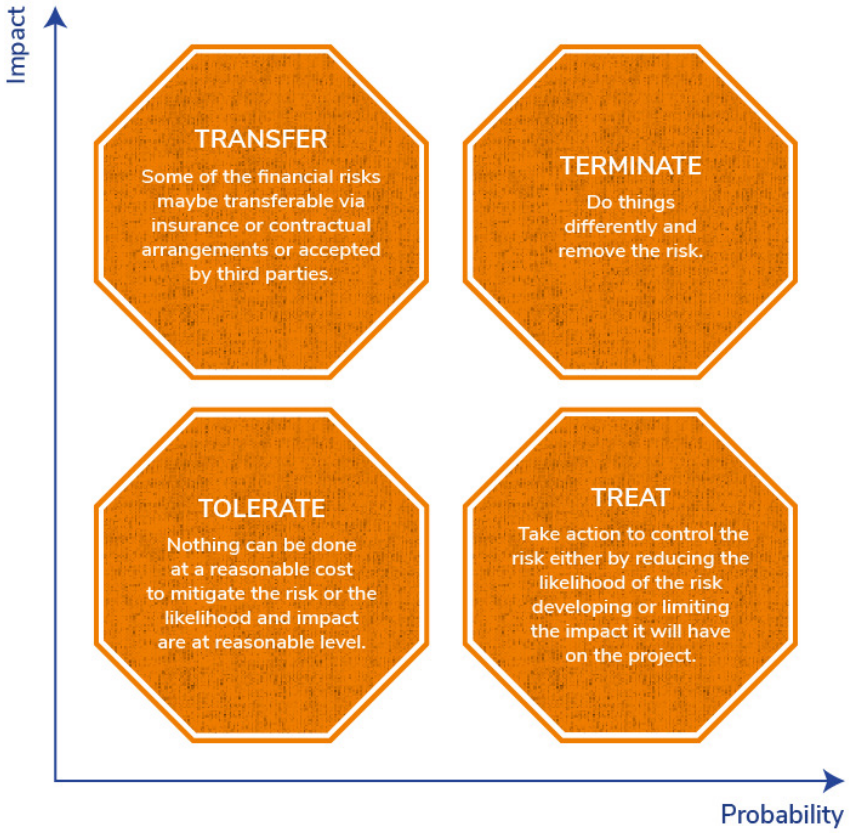
Consequence Categories

Category	Description	Examples
I	Catastrophic	Large number of fatalities, and/or major long-term environmental impact
II	Major	Fatalities, and/or major short-term environmental impact
III	Serious	Serious injuries, and/or significant environmental impact.
IV	Significant	Minor injuries, and/or short-term environmental impact.
V	Minor	First aid injuries only, and/or minimal environmental impact
VI	None	No significant consequence.

Prioritizing Risk – The Risk Matrix

Probability Category							
	A	L	M	M	H	H	H
	B	L	L	M	M	H	H
	C	L	L	L	M	M	H
	D	L	L	L	L	M	M
	E	L	L	L	L	L	M
	F	L	L	L	L	L	L
		VI	V	IV	III	II	I
		Consequence Category					

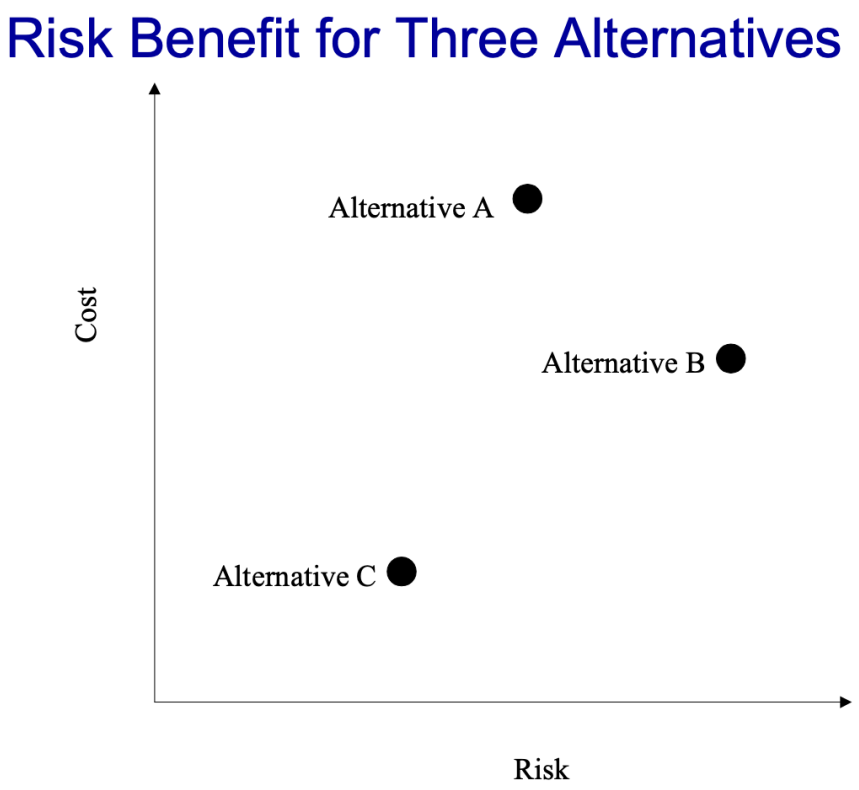
Treating Risk (The 4 Ts)



- **1. Treat (Mitigate):**
  - Implement controls to reduce Likelihood or Impact.
  - **Example:** Installing a Firewall reduces the likelihood of a hack.
- **2. Transfer:**
  - Shift the financial burden to a third party.
  - **Example:** Buying Cyber Insurance or outsourcing to a managed vendor.
- **3. Tolerate (Accept):**
  - Acknowledge the risk but do nothing.
  - **Condition:** The cost of the fix > The potential loss.
  - **Requirement:** Must be formally signed off by an executive.
- **4. Terminate (Avoid):**
  - Stop the risky activity entirely.
  - **Example:**
    "We will stop selling products in that country to avoid their privacy laws."

Decision Analysis based on Risk Factors

- **Decision Analysis:** Cost-Benefit Analysis
  - Risk managers commonly weigh various factors including cost and risk.
  - The analysis of three different alternatives is shown graphically in the figure (right).
  - The graph shows that alternative (C) is the best choice since the level of risk and cost is less than alternatives (A) and (B).
  - However, if the only alternatives were A and B, the decision would be more difficult.



Key Compliance Frameworks

SOC2 vs ISO 27001

	SOC 2	ISO 27001
Definition	A set of audit reports that show the level of conformity to a set of defined criteria	A Standard that establishes requirements for an Information Security Management System
Global Reach	U.S. Standard	International Standard
Certifying Body	Completed by a licensed CPA Firm	Completed by an accredited ISO 27001 certification body
Duration	6-12 months initial attestation, annual re-attestation required	6-24months initial certification, valid for 3 years, annual audit required
Industry	Can be applied to service organizations from any industry, most commonly technology based	Designed to be used by organizations or any size or industry
Difficulty to achieve	Moderate	High
What is if for?	Provides evidence that security for systems in scope meet basic trust principles and criteria	Provides system for identifying, minimizing and managing security threats to information assets

SOC 2 vs PCI DSS

	SOC 2	PCI DSS
Scope	System or product	Only what touches, transmits, or protects credit card data
Data Protection	Sensitive data	Credit card data
Audited by	CPA	QSA or self-assessment
Audience	End Customers	Credit Card Providers (VISA, MC, etc)
Requirements	Controls that address criteria	Specific requirements

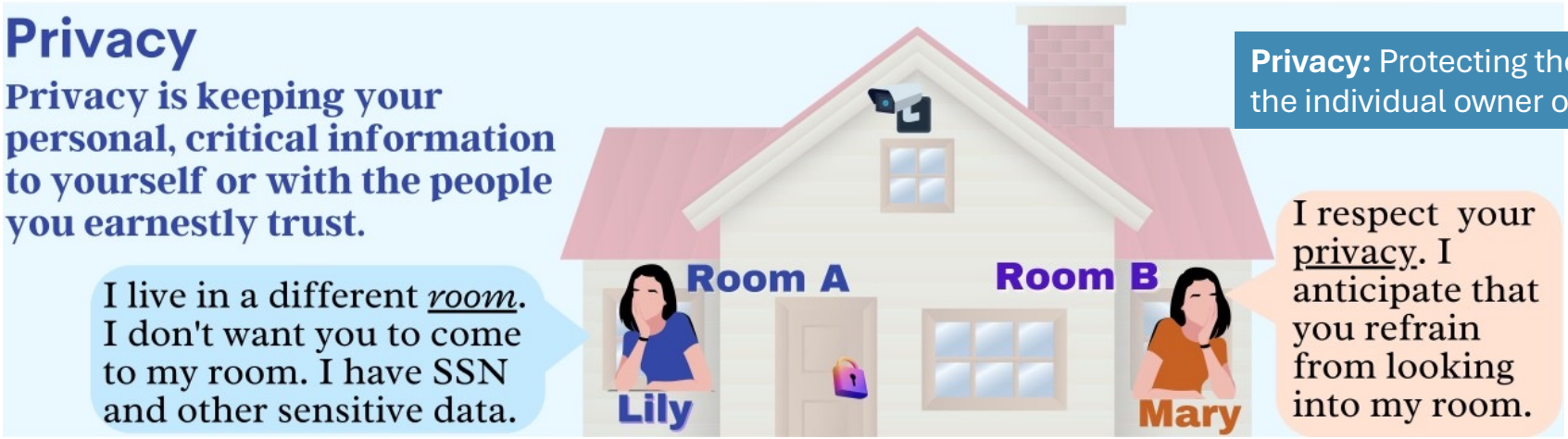
SOC 2 (Service Organization Control):
Audience: B2B SaaS customers.
Focus: Trust Principles (Security, Availability, Confidentiality).
Type I (Snapshot) vs. **Type II** (Over a period of time like 6-12 months).

ISO 27001:
Audience: International customers.
Focus: Building a complete Information Security Management System (ISMS).

PCI DSS:
Audience: Payment Card Industry.
Focus: Protecting credit card numbers.
Very prescriptive.

Privacy Regulations (GDPR & CCPA)

Security: Protecting data from unauthorized access.

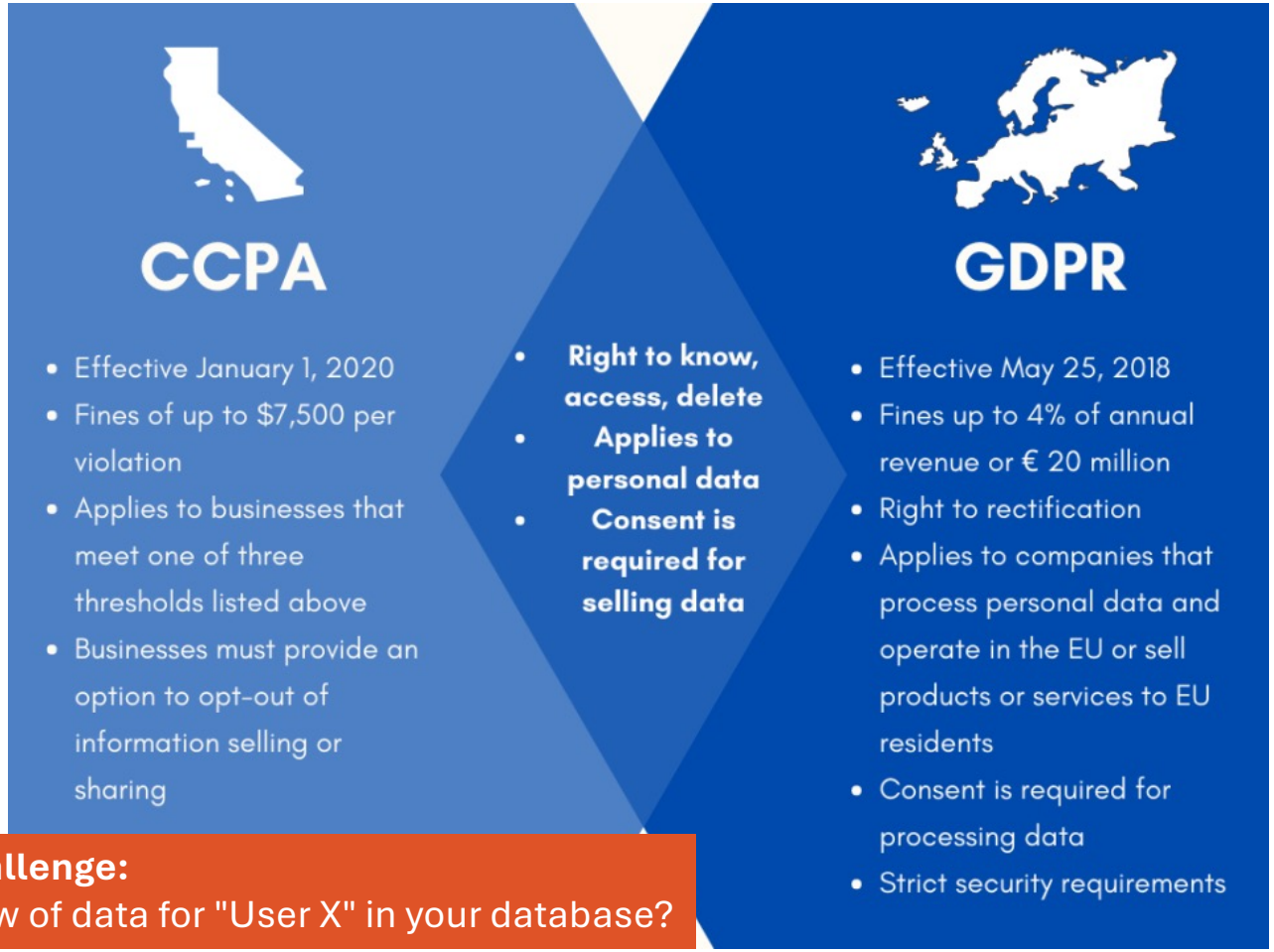


Privacy: Protecting the rights of the individual owner of that data

Privacy Regulations (GDPR & CCPA)

CCPA/CPRA (California):

Gives US consumers similar rights to access and delete data.



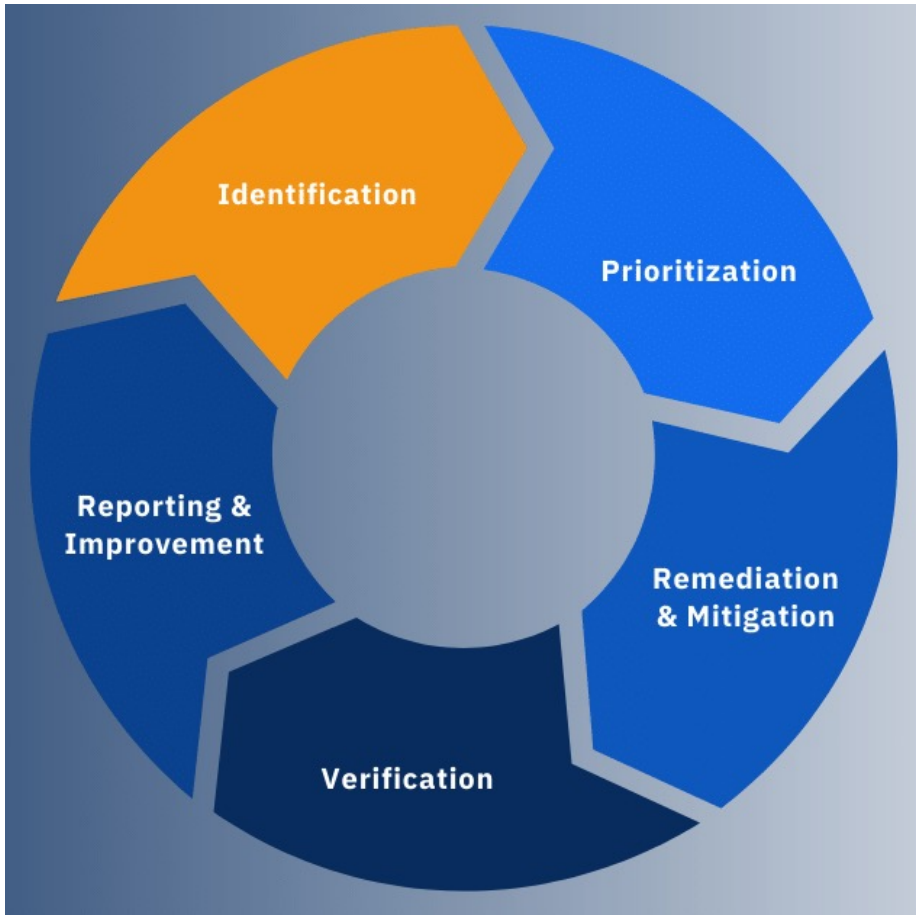
GDPR (Europe):

Right to be Forgotten: You must be able to delete all of a user's data upon request.

Breach Notification: You must report breaches within 72 hours.

The Operational Challenge:
Can you find every row of data for "User X" in your database?

Vulnerability Management Lifecycle

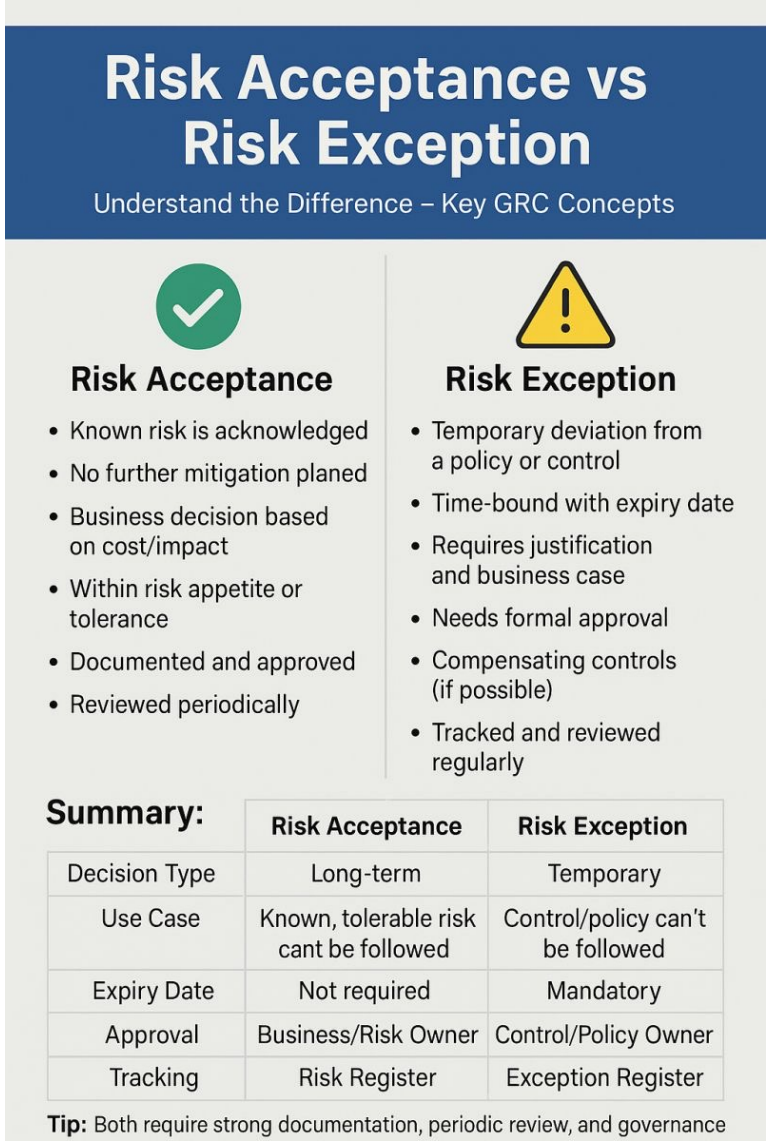


- **The Cycle:**
  - **Scan/Identification:** Automated tools (Nessus, Qualys) find CVEs.
  - **Prioritize:** Filter the noise. Focus on **Exploitable** bugs (CISA KEV List).
  - **Remediate:** Apply the patch or config change.
  - **Verify:** Rescan to prove it is fixed.

- **SLA (Service Level Agreement):**
  - The internal law for patching speed.
  - *Critical:* 48 Hours.
  - *High:* 14 Days.
  - *Medium:* 30 Days.

Exception Management (Risk Waiver)

- **The Reality:** Sometimes you cannot patch.
  - Scenario: A legacy server runs critical software that breaks if updated.
- **The Process:**
  1. **Request:** Engineer submits a waiver request.
  2. **Compensating Control:** "We can't patch it, so we will remove its internet access (Air Gap)."
  3. **Approval:** Security leadership approves the waiver for a set time (e.g., 6 months).
  4. **Review:** Waiver expires and must be re-evaluated.



Vendor Risk Management (Third-Party Risk)

- **Vendor Risk Management (VRM)** is the strategic, ongoing process of identifying, assessing, and mitigating risks—cybersecurity, operational, legal, and reputational—posed by third-party vendors, suppliers, and service providers.
- It covers the full vendor lifecycle, from initial due diligence and onboarding to continuous monitoring and offboarding.
- **Key Aspects of Vendor Risk Management:**
  - **Purpose:** To prevent financial loss, operational disruptions, and damage to reputation caused by third-party vulnerabilities.
  - **Key Risk Areas:** Cybersecurity threats (data breaches), compliance failures (GDPR, HIPAA, etc.), financial instability of the vendor, and operational failure.
  - **Lifecycle Stages:** The process involves vendor onboarding, risk assessment/scoring, contracting, continuous monitoring, and termination.

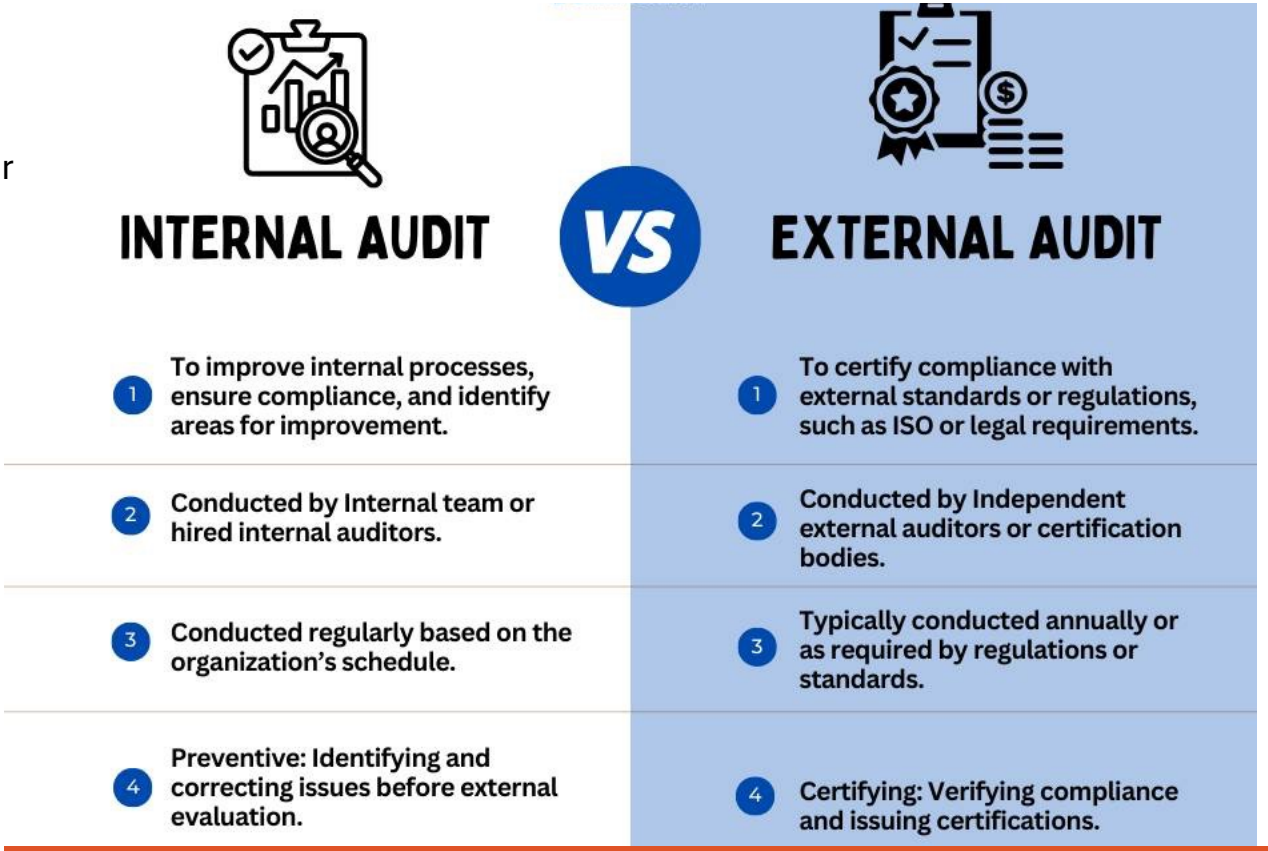
Vendor Risk Management (Third-Party Risk)

Vendor Risk Management (Third-Party Risk)

- **Best Practices:**
  - **Tiering Vendors:** Categorizing vendors based on the risk they pose (e.g., high-risk if they have sensitive data access).
  - **Continuous Monitoring:** Using automated tools to track vendor security postures in real-time.
    - Using tools (e.g., SecurityScorecard, BitSight) to watch vendor hygiene in real-time.
  - **Due Diligence:** Thoroughly vetting vendors before engagement, including reviewing their security certifications (e.g., SOC 2) and business continuity plans.

Audits (Internal vs. External)

- **Internal Audit:**
  - Performed by your own team or consultants.
  - **Goal:** Preparation. Find the gaps before the real auditor does.



- **External Audit:**
  - Performed by a CPA firm (for SOC 2) or Registrar (for ISO).
  - **Goal:** Certification.

Evidence Collection:
- "If it isn't documented, it didn't happen."
- Auditors need screenshots, ticket exports, and logs to prove you followed your own policies.

Key Takeaways

- **Governance** aligns security with business goals.
- **Risk Registers** are the primary tool for tracking and reporting threats to leadership.
- **Compliance Frameworks** (SOC 2) are essential for sales/trust, but they are just a baseline.
- **Privacy Laws** (GDPR) turn data deletion into a mandatory technical requirement.
- **Key Takeaway:** GRC is the language used to translate "technical headaches" into "business decisions."

End of the Lecture

Please do not hesitate to ask any questions to free your curiosity,

If you have any further questions after the class, please contact me via email (charnon@cmkl.ac.th).