Assess Discovery Risks

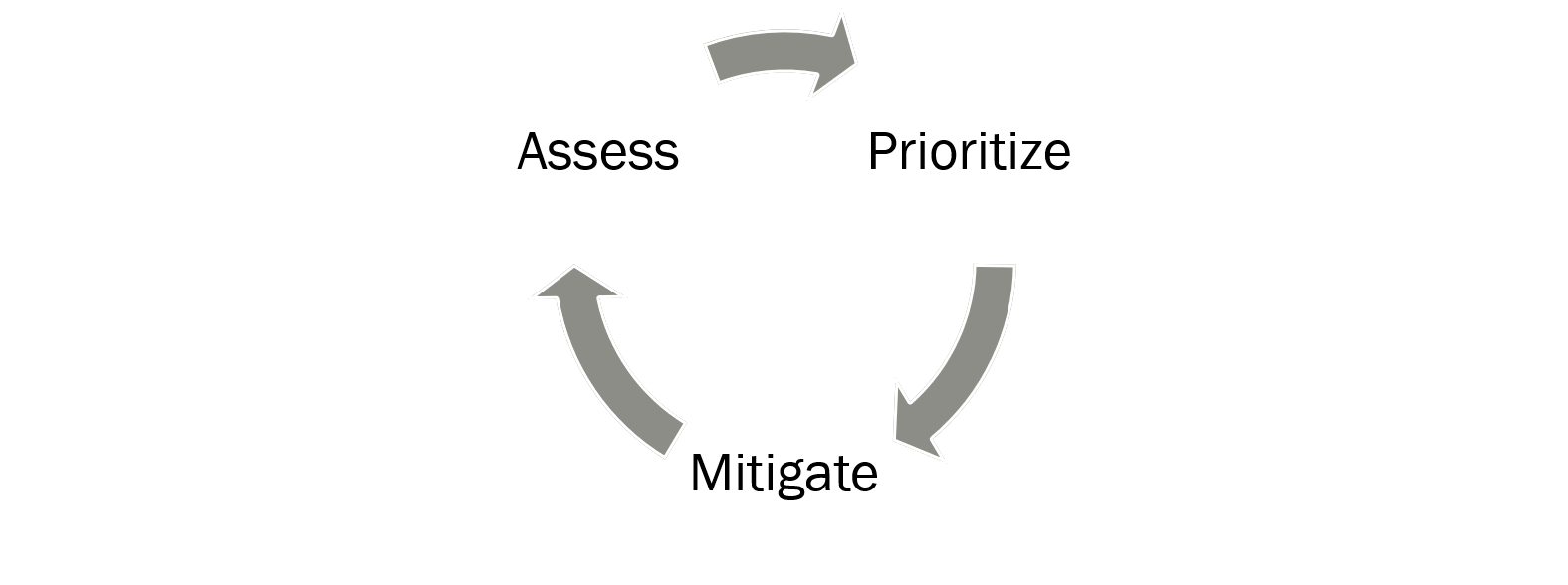
Nate Bachmeier

TIM7030- Managing Risk, Security, & Privacy in Information Systems

June 7, 2020

# Introduction

Figure 1: RMP Cycle



The core objective of NCU Financial (NCUF) is to deliver on its mission of world-class banking services. Meeting that expectation requires a corporate strategy that minimizes risks where possible, through mitigation or transference strategies. When the business chooses to remove a vulnerability, that decision requires resources and detracts from the core mission. The corporate risk management program (RMP) needs to answer both ‘when and how’ to address these threats by operating on a feedback loop of assessing, prioritizing, and mitigating risks.

# Requirements of Risk Assessment

Security assessments perform an audit of the people, processes, and products that are involved in a business workflow. This analysis needs to assess the controls at integration points and whether they are appropriate protections for the resources. Threat modeling is a formal process the enumerates these interactions and considers different spoofing, tampering, repudiation, disclosure, and elevation (STRIDE) attacks (Hennig, 2018).

# Primary Risks

CyberSecurity refers to a collection of mechanisms and processes that constrain risk to business systems by ensuring they meet performance and consistency expectations, even under erroneous conditions (Mickens, 2018). These erroneous conditions arise due to both malicious and negligent scenarios, degrading the confidentiality, integrity, and availability of our service offerings.

Nearly half of security incidents come from negligence, a quarter from external actors, and the remainder from technical glitches (Valiente, 2017). These statistics highlight the criticality of starting with controls that limit the blast radius of human errors. NCUF is always one lousy SQL command away from executing a disaster recovery process.

External actors attack the organization with vulnerability scanners, phishing scams, denial of service (DoS), and malware (Lee, Moon, & Park, 2017). These strategies tend to be highly automated, with costs disproportional skewed toward the defender.

The misconfiguration of service policy can result in security incidents like outages or device compromise. Administrating network topologies are highly complex dynamic environments. Without automation, failures will eventually creep in.

# Regulatory Requirements

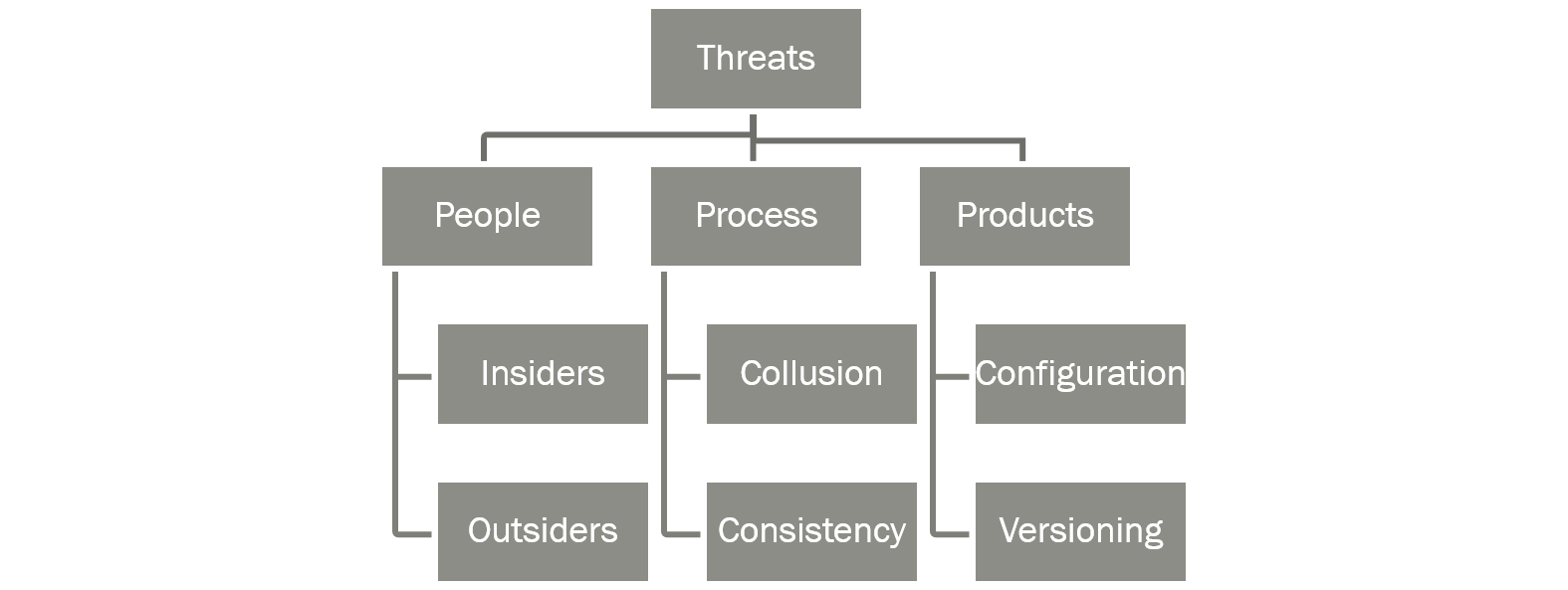
Financial institutions need to maintain the confidentiality, integrity, and availability of customer data. When these expectations are not maintained, then it results in economic loss and public embarrassment for NCUF. Various regulatory boards have established regulatory requirements to create a baseline of policy expectations.

Table 1: Regulations

|  |  |
| --- | --- |
| Program | Impact |
| Sarbanes Oxley Act (2002) | Requires audit and control systems |
| Payment Card Ind. Data Security Std (PCI) | Requires encryption and storage norms of financial data |
| Gen Data Protection Regulation Act (GDPR) | Requires European customer data to reside in the EU |

# Taxonomy of Risk

Figure 2: Taxonomy



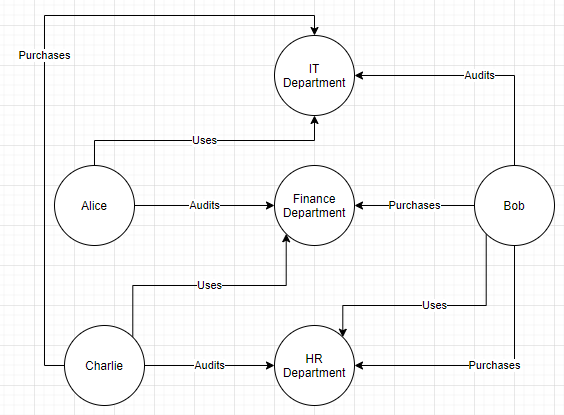
A taxonomy represents a hierarchical system for entity classification. NCUF can use this approach to group related items together and then prioritize which the buckets to tackle first. It would be prohibitively expensive to mitigate all business risks entirely. Vulnerabilities exist at the intersection of system susceptibility, threat accessibility, and actor capability (Baskerville, Rowe, & Wolff, 2018). Often removing one of these facets is more economical than the other.

# Collusion and Segregating of Duties (SoD)

The objective of SoD is to remove single points of failure from the organizational hierarchy. For instance, if an employee can purchase equipment and audit the inventory, then they could be tempted to make false invoices and embezzle the funds. NCUF minimizes this scenario by assigning these roles to different employees. However, there is also a risk that these different team members join forces, through collusion, to sidestep the protections. The business can only hire a finite staff.

One potential solution is to convert the problem into a game of Sodoku. In Sodoku, there are NxM cells, with each and row containing a value exactly once. Similarly, role assignments can cross validate such as Figure 3. Alice is a manager in IT that audits the finance. She has little incentive to collude with the primary users Charlie because Bob their interactions and needs to be consulted for purchases. Meanwhile, Bob is a manager in the HR department and will be audited by Charlie.

Figure 3: Minimizing Collusion & SoD



# Misconfiguration and Compromise