Section 3: Week 8: Corporate Risk Management Plan

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

July 26, 2020

North Central University

# Corporate Risk Management Plans

NCU Financial (NCU-F) provides banking and investment services through its online portal and physical branch locations. These points of presence encounter risks from a litany of maliciousness and negligent sources that can impact its service’s confidentiality, integrity, and availability. When these situations occur, it results in economic loss, damage to the brand, and litigation. Mitigating these concerns requires a risk management plan that identifies prioritized lists of vulnerabilities and implements strategies to limit the blast radius. This plan must include solutions that span people, processes, and products across the business value chain. Through a combination of reactive and proactive systems, the organization can prepare for both known and unknown scenarios and rise to the challenges at hand.

# Section I: State of the Organization

## Corporate Management of Systems

## Threats Every Organization Faces

## Organizational Chart

## Network Diagrams

# Section II: Objectives of Risk Management Plan

## Risk Statement

## People

## Processes

## Products

# Section III: Business Impact Analysis

# Section IV: Plan of Action and Milestones

# Section V: Risk Reduction for Mobile Device Management

# Section VI: Tooling Recommendations

# Section VII: Response and Risk Management

## Privacy and Risk from Cloud

## Incident Response Process

## Vulnerability Assessments

# Section VIII: Disaster Recovery

## Remote Locations

## Inventory Management

## Backup and Recovery

## Remote Site Fail-Over

# Section IX: Plan Verification

## Implementing Drills

## Assessing Drills

# Section X: Dissemination

## Plan Distribution

## Awareness Training

## Formation of Emergency Committee Personnel