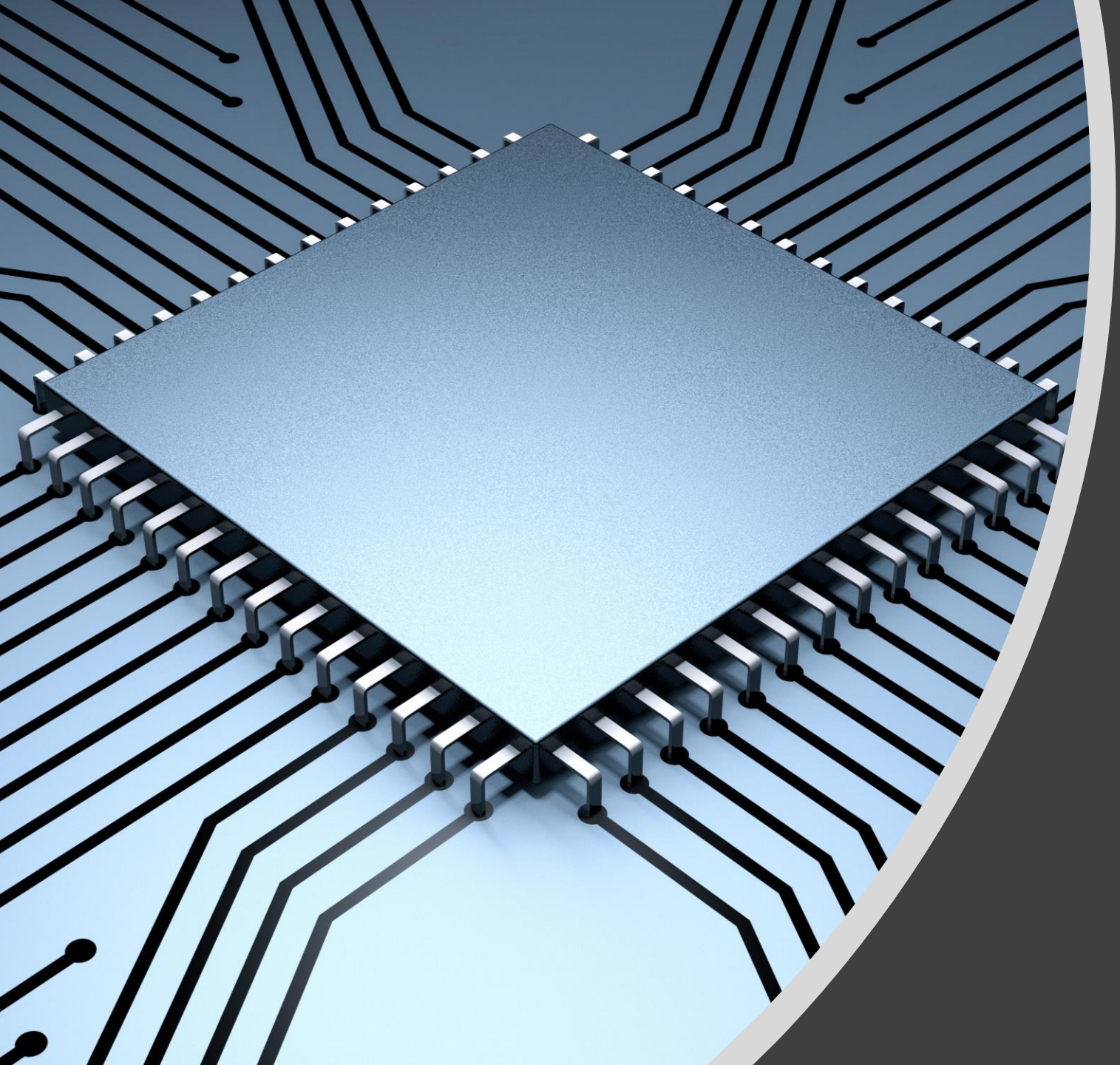


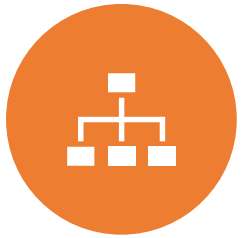
Risk Management and Organization Resilience of City of Aurora

CYB 3300 Course Project

By: Troy warner

Fall 2022

Table of Contents



ORGANIZATION – CITY OF AURORA

GOAL

RMF FRAMEWORK

PREPARE

CATEGORIZATION

Organization – City of Aurora

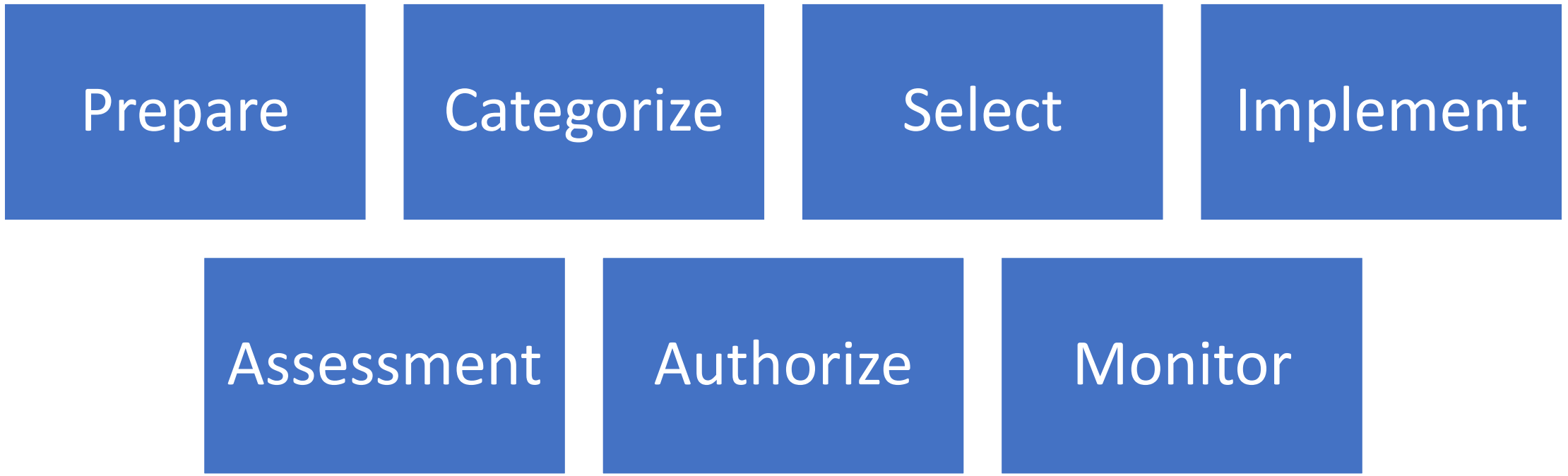
The City of Aurora is in charge of critical systems that deal with infrastructure and resources that are important to the residents of the city. The safety of the resident can depend on the security of systems under their control

City of Aurora Cybersecurity Goal

Create a plan using RMF to secure the systems of the city

Build a resilient network of systems that allows the city to keep operations going even in the case of an attack

RMF Framework



Prepare

- Prepare the organization to manage security and privacy risks

Categorize

- Categorize the system and information processed, stored and transmitted based on an impact analysis

Select

- Choose controls to be put in place on systems

Implement

Assessment

Authorize

Monitor

Step One: Prepare

System	Tasks	Outcomes
Risk Management Roles	The Head of Public works will be in charge of creating goals that form from the risk management strategy. The head of IT will be the one executing the plan and putting the controls in place.	The outcome is a clear goal created from the top of the organization and systems with controls so an assessment can be completed
Risk Management Strategies	The city of Aurora will focus heavily on protecting critical systems that could seriously hurt people. They also want to protect important personal data that they hold	The outcome is a strong plan in place to protect the city's most critical system
Risk Assessment	A team of pen testers comes in and runs tests to find vulnerabilities in the organization.	The outcome is a series of vulnerabilities discovered.

Step Two: Categorize

System	Tasks	Outcomes
Water Treatment Controller	Description	This system controls the water treatment process. It determines what gets added to the water to make it safe and clean. Processes include decontamination, treatment and storage.
	Categorization: High Risk and Critical	Security Category: (confidentiality, High), (integrity, High), (availability, Low) High Risk This system is critical as It runs the processes that make the town's water clean and safe. A mission of City of Aurora is to make sure their residents receive drinkable water that will not harm them. It is also a top priority in the City's risk management strategy which makes the value of this system extremely high. It becomes even more critical as a water treatment system is a valuable target for hackers
	Security Categorization Review and Approval	The head of public works will review the categorization that was made by the town's risk managers and will approve it as he knows the importance of protecting such a vital system

Step Two: Categorize

System	Tasks	Outcomes
Payroll Systems	Description	This system holds important data on the local government workers in the town so it can send out paychecks. Some of the data includes; social security numbers, bank account numbers, and billing addresses.
	Categorization: High Risk and Critical	Security Category: (confidentiality, High), (integrity, High), (availability, Low) High Risk The payroll system holds critical financial data on employees of the town. Protecting this data is important as it keeps business functions moving. The categorization does meet the goal of wanting to protect important personal data that the town holds
	Security Categorization Review and Approval	The CFO will review this categorization as he deals with all thing finance in the town.

City of Aurora		Outcomes	
Selection	Policy: No Remote Access Software on	Firewall	Intrusion Prevention System
Tailoring	High risk machines will be barred from having remote access software to prevent breaches	A sound firewall will be put in place and tailored to only allow necessary ports to be open and block unwanted connections	An intrusion system will monitor all systems on the network to ensure no unwanted user has unauthorized access to high risk systems
Allocation	This policy will only be applied to systems categorized as high risk	All systems will be connected to the firewall	This control will be allocated to the entire network

Controls	Implementation
Firewall	The city will hire a contractor to set up a firewall with all the recommended baseline controls from the firewall provider and tailor it by blocking all ports that the water system controller does not need
Access Control	Only authorized users will be given the password to the system, and cameras will be put in place to ensure no unauthorized users attempt to access it. There will also be announcement so that all unauthorized users are aware they are not to access it. A lock will also be placed onto the room where the system is
Remote Software Policy	The base user of the system will not have permissions to download anything. Only the IT administrator will have access to an admin account that can download software. The IT administrator will have specific instructions to never download remote access software.