Risk Management Framework

By: Jocelyn Perez

Goal of Report

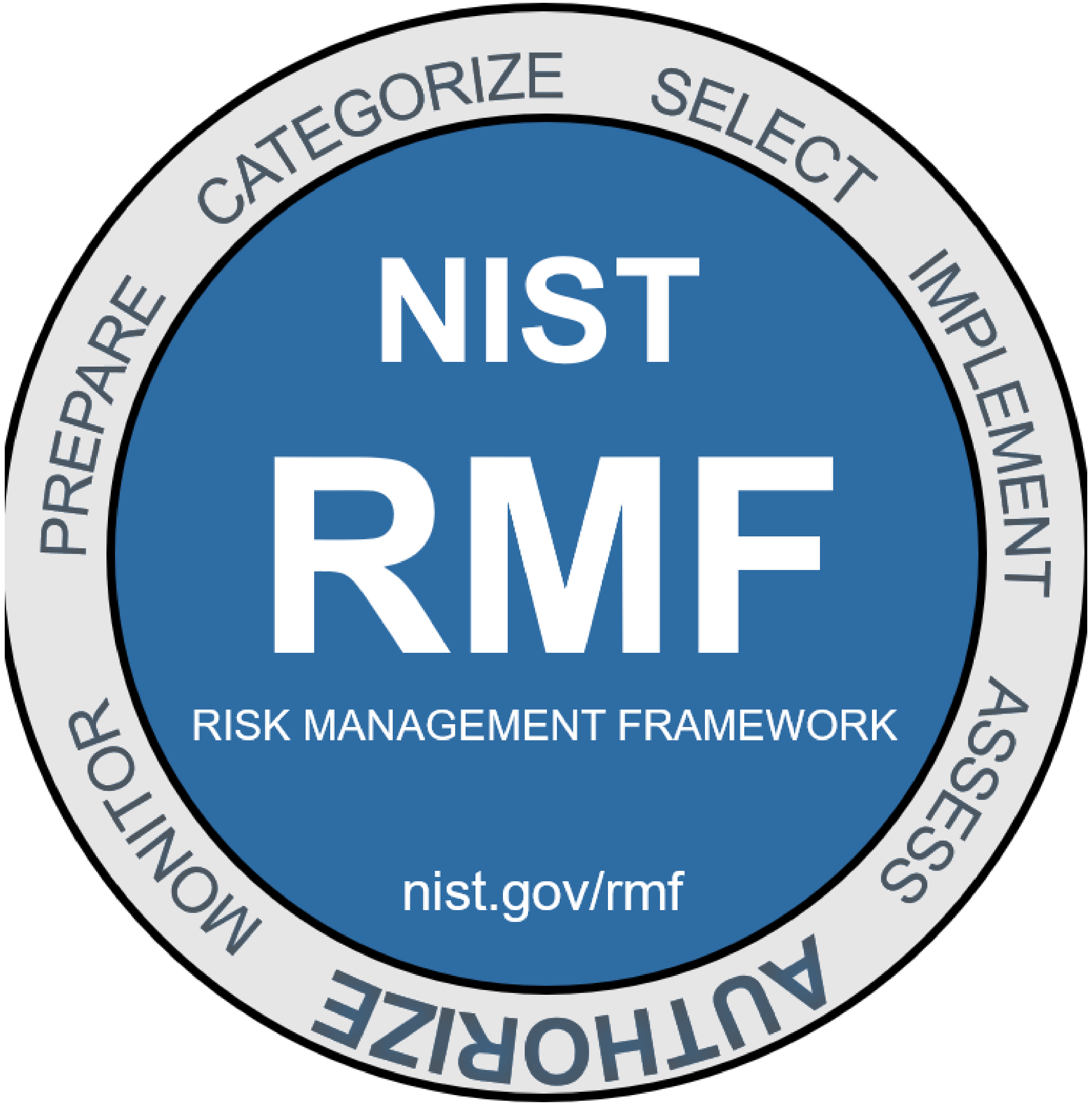
- Using the Risk Management Framework for Aurora University's Financial system by highlighting on possible risks and finding resiliency for future risks.

Table of Content

Organization – Aurora University

Private University that holds in-person and online classes for students. Has an active Financial System that stores and manages student information.

Located in Aurora, Illinois



Risk Management Framework

- We will follow the NIST RMF model to implement a strategy for the financial system within Aurora University.

Financial System

01

Holds
all financial information for all students new and past.

02

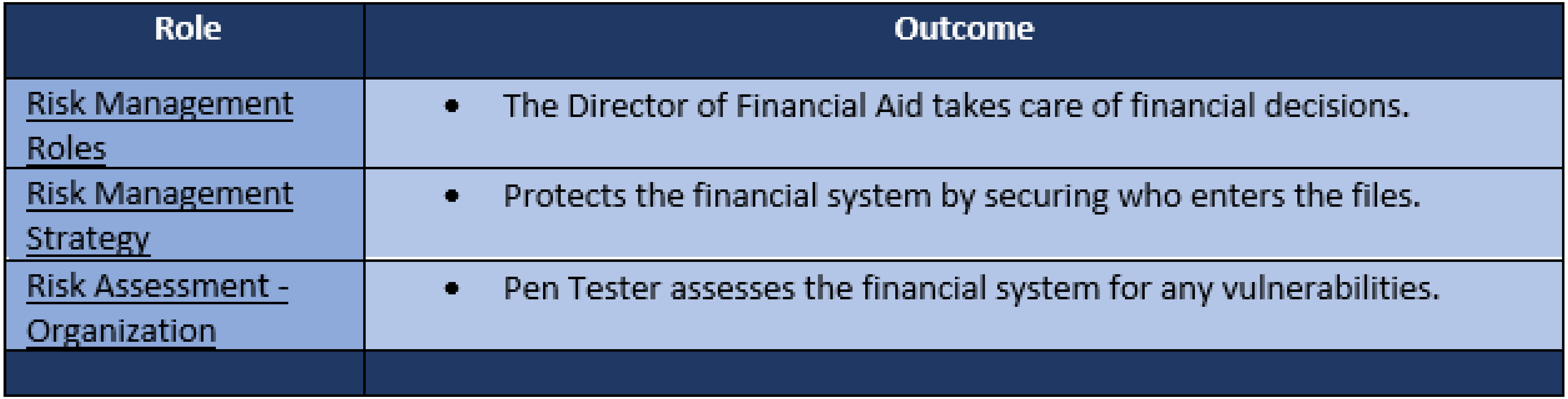
Threat: Information accessed without permission.

03

The Director of Financial Aid takes care of financial decisions.

Prepare

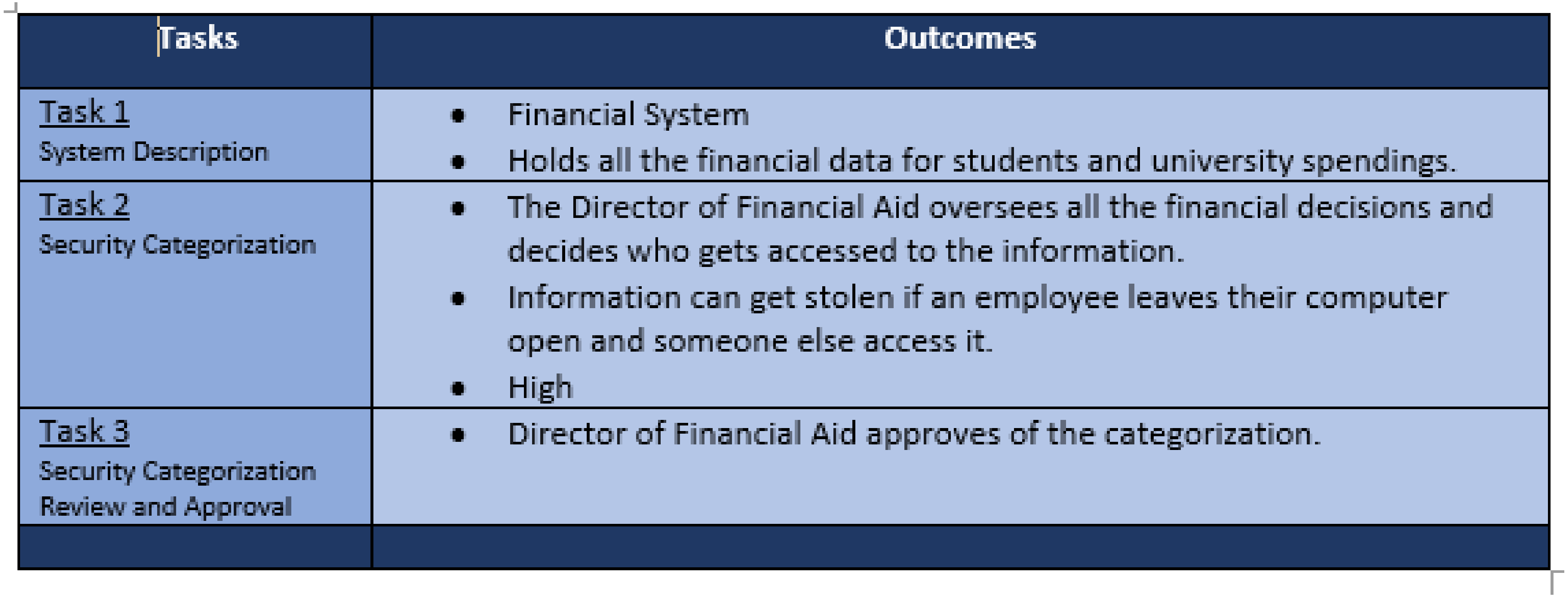
- The purpose of the Prepare step is to carry out essential activities at the organization, mission and business process, and information system levels of the organization to help prepare the organization to manage its security and privacy risks using the Risk Management Framework.



Role	Outcome
Risk Management Roles	• The Director of Financial Aid takes care of financial decisions.
Risk Management Strategy	• Protects the financial system by securing who enters the files.
Risk Assessment - Organization	• Pen Tester assesses the financial system for any vulnerabilities.

Categorize

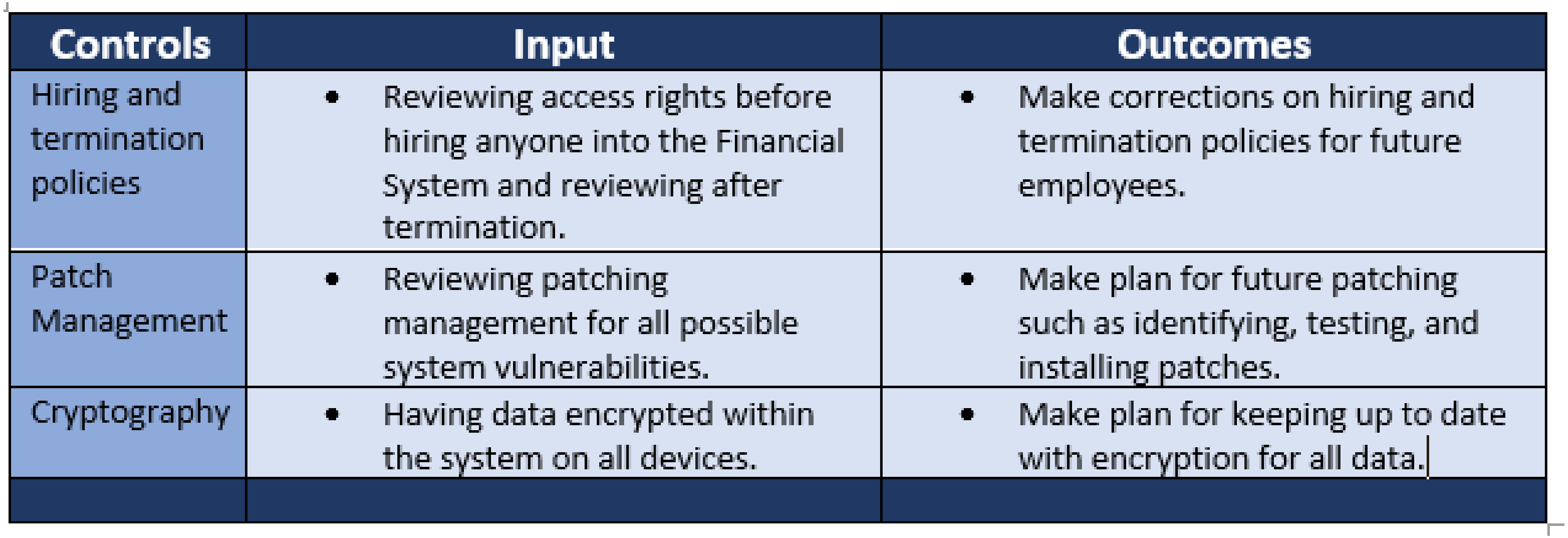
- To inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems.



Tasks	Outcomes
Task 1 System Description	• Financial System • Holds all the financial data for students and university spendings.
Task 2 Security Categorization	• The Director of Financial Aid oversees all the financial decisions and decides who gets accessed to the information. • Information can get stolen if an employee leaves their computer open and someone else access it. • High
Task 3 Security Categorization Review and Approval	• Director of Financial Aid approves of the categorization.

Select

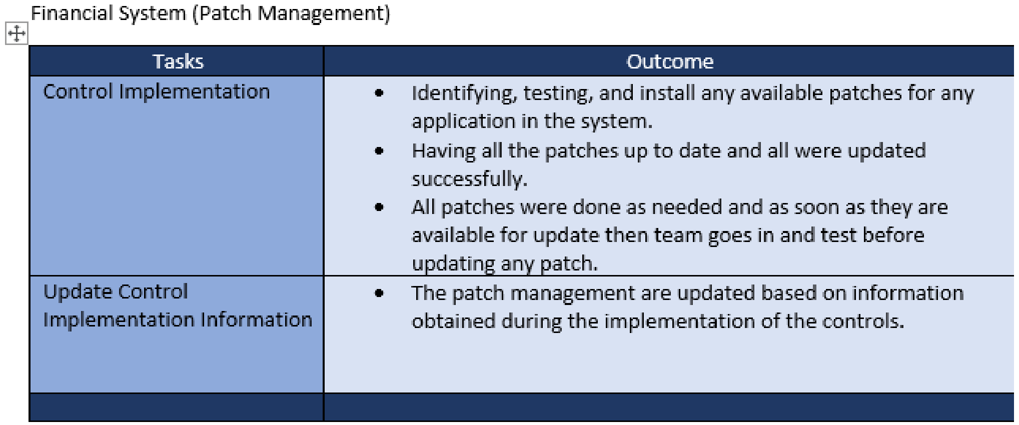
- Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.



Controls	Input	Outcomes
Hiring and termination policies	• Reviewing access rights before hiring anyone into the Financial System and reviewing after termination.	• Make corrections on hiring and termination policies for future employees.
Patch Management	• Reviewing patching management for all possible system vulnerabilities.	• Make plan for future patching such as identifying, testing, and installing patches.
Cryptography	• Having data encrypted within the system on all devices.	• Make plan for keeping up to date with encryption for all data.

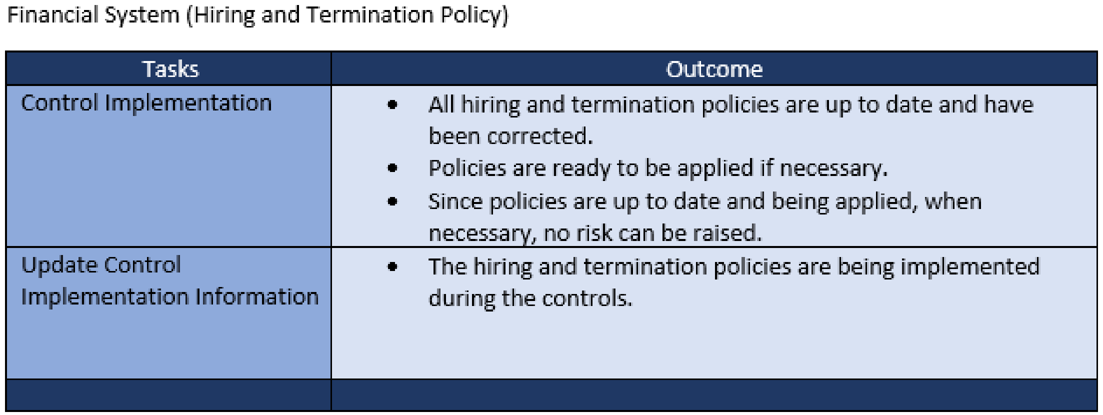
Implement

- To implement the controls in the security and privacy plans, putting in place the controls to work.



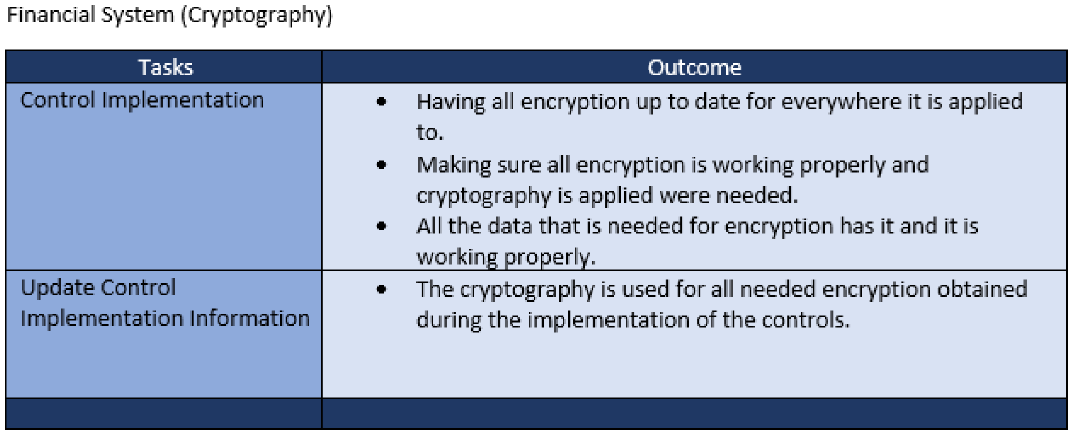
Financial System (Patch Management)

Tasks	Outcome
Control Implementation	• Identifying, testing, and install any available patches for any application in the system. • Having all the patches up to date and all were updated successfully. • All patches were done as needed and as soon as they are available for update then team goes in and test before updating any patch.
Update Control Implementation Information	• The patch management are updated based on information obtained during the implementation of the controls.



Financial System (Hiring and Termination Policy)

Tasks	Outcome
Control Implementation	• All hiring and termination policies are up to date and have been corrected. • Policies are ready to be applied if necessary. • Since policies are up to date and being applied, when necessary, no risk can be raised.
Update Control Implementation Information	• The hiring and termination policies are being implemented during the controls.



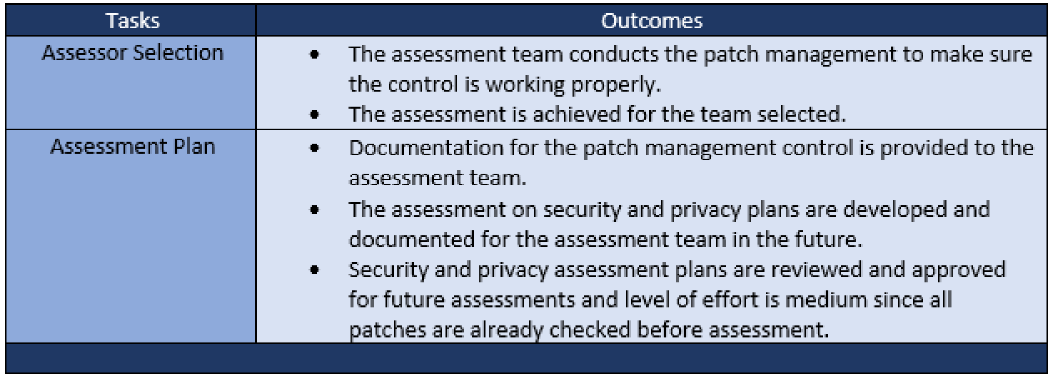
Financial System (Cryptography)

Tasks	Outcome
Control Implementation	• Having all encryption up to date for everywhere it is applied to. • Making sure all encryption is working properly and cryptography is applied were needed. • All the data that is needed for encryption has it and it is working properly.
Update Control Implementation Information	• The cryptography is used for all needed encryption obtained during the implementation of the controls.

Assess

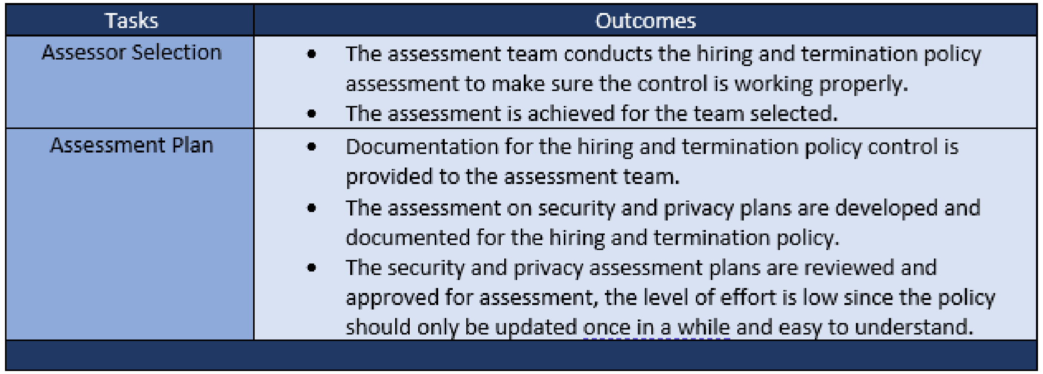
- The purpose of the Assess step is to determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meet the security and privacy requirements for the system and the organization.

Financial System (Patch Management)



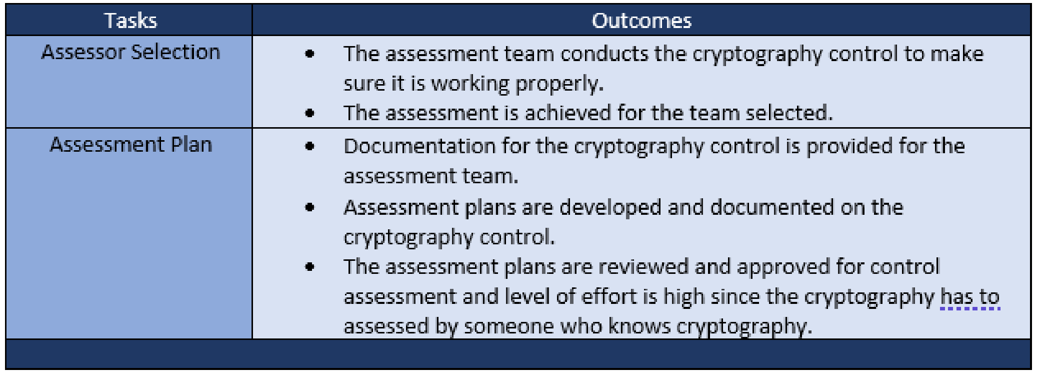
Tasks	Outcomes
Assessor Selection	• The assessment team conducts the patch management to make sure the control is working properly. • The assessment is achieved for the team selected.
Assessment Plan	• Documentation for the patch management control is provided to the assessment team. • The assessment on security and privacy plans are developed and documented for the assessment team in the future. • Security and privacy assessment plans are reviewed and approved for future assessments and level of effort is medium since all patches are already checked before assessment.

Financial System (Hiring and Termination Policy)



Tasks	Outcomes
Assessor Selection	• The assessment team conducts the hiring and termination policy assessment to make sure the control is working properly. • The assessment is achieved for the team selected.
Assessment Plan	• Documentation for the hiring and termination policy control is provided to the assessment team. • The assessment on security and privacy plans are developed and documented for the hiring and termination policy. • The security and privacy assessment plans are reviewed and approved for assessment, the level of effort is low since the policy should only be updated once in a while and easy to understand.

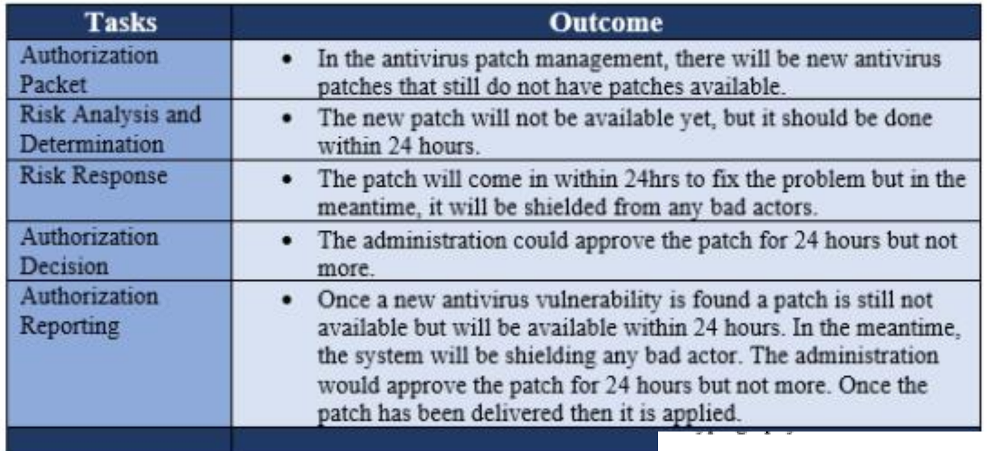
Financial System (Cryptography)



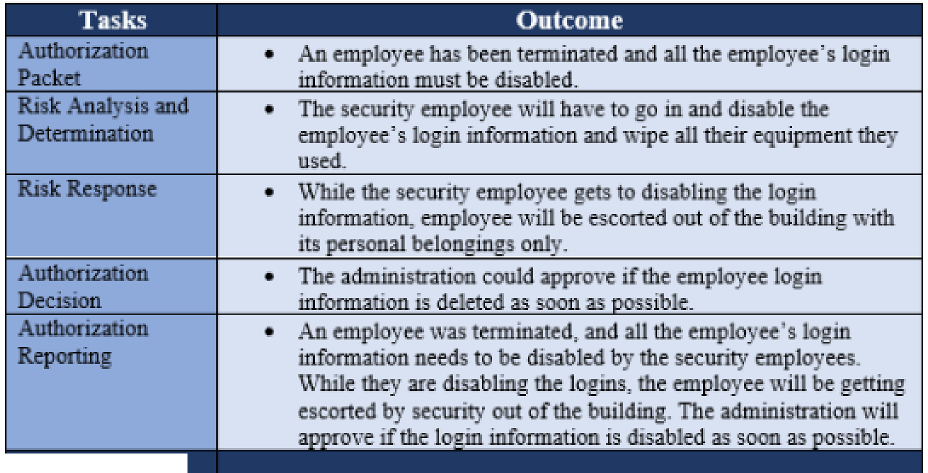
Tasks	Outcomes
Assessor Selection	• The assessment team conducts the cryptography control to make sure it is working properly. • The assessment is achieved for the team selected.
Assessment Plan	• Documentation for the cryptography control is provided for the assessment team. • Assessment plans are developed and documented on the cryptography control. • The assessment plans are reviewed and approved for control assessment and level of effort is high since the cryptography has to assessed by someone who knows cryptography.

Authorize

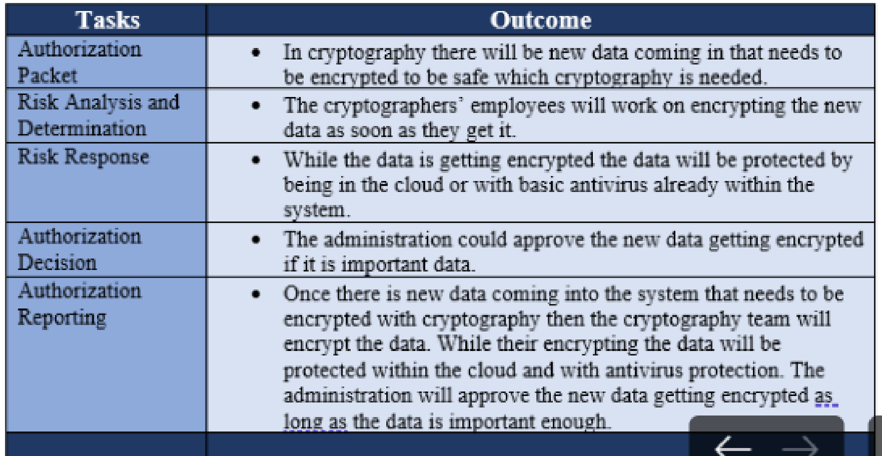
- To provide organizational accountability by requiring a senior management official to determine if the security and privacy risk.



Tasks	Outcome
Authorization Packet	• In the antivirus patch management, there will be new antivirus patches that still do not have patches available.
Risk Analysis and Determination	• The new patch will not be available yet, but it should be done within 24 hours.
Risk Response	• The patch will come in within 24hrs to fix the problem but in the meantime, it will be shielded from any bad actors.
Authorization Decision	• The administration could approve the patch for 24 hours but not more.
Authorization Reporting	• Once a new antivirus vulnerability is found a patch is still not available but will be available within 24 hours. In the meantime, the system will be shielding any bad actor. The administration would approve the patch for 24 hours but not more. Once the patch has been delivered then it is applied.



Tasks	Outcome
Authorization Packet	• An employee has been terminated and all the employee's login information must be disabled.
Risk Analysis and Determination	• The security employee will have to go in and disable the employee's login information and wipe all their equipment they used.
Risk Response	• While the security employee gets to disabling the login information, employee will be escorted out of the building with its personal belongings only.
Authorization Decision	• The administration could approve if the employee login information is deleted as soon as possible.
Authorization Reporting	• An employee was terminated, and all the employee's login information needs to be disabled by the security employees. While they are disabling the logins, the employee will be getting escorted by security out of the building. The administration will approve if the login information is disabled as soon as possible.

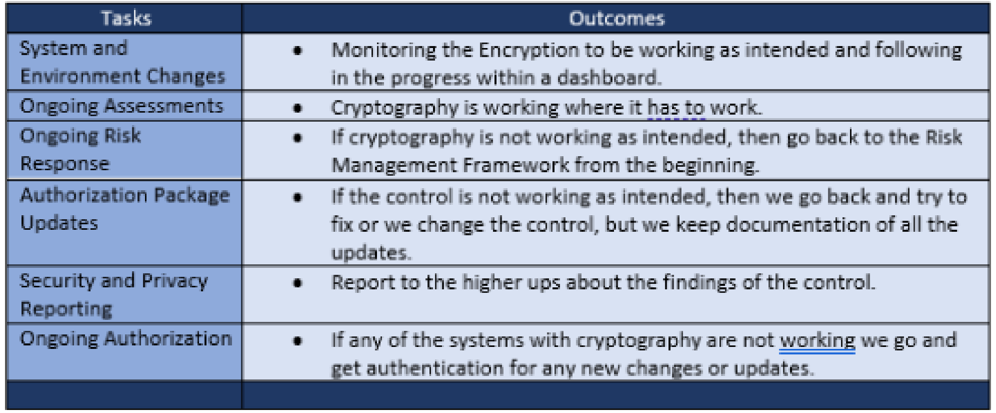


Tasks	Outcome
Authorization Packet	• In cryptography there will be new data coming in that needs to be encrypted to be safe which cryptography is needed.
Risk Analysis and Determination	• The cryptographers' employees will work on encrypting the new data as soon as they get it.
Risk Response	• While the data is getting encrypted the data will be protected by being in the cloud or with basic antivirus already within the system.
Authorization Decision	• The administration could approve the new data getting encrypted if it is important data.
Authorization Reporting	• Once there is new data coming into the system that needs to be encrypted with cryptography then the cryptography team will encrypt the data. While their encrypting the data will be protected within the cloud and with antivirus protection. The administration will approve the new data getting encrypted as long as the data is important enough.

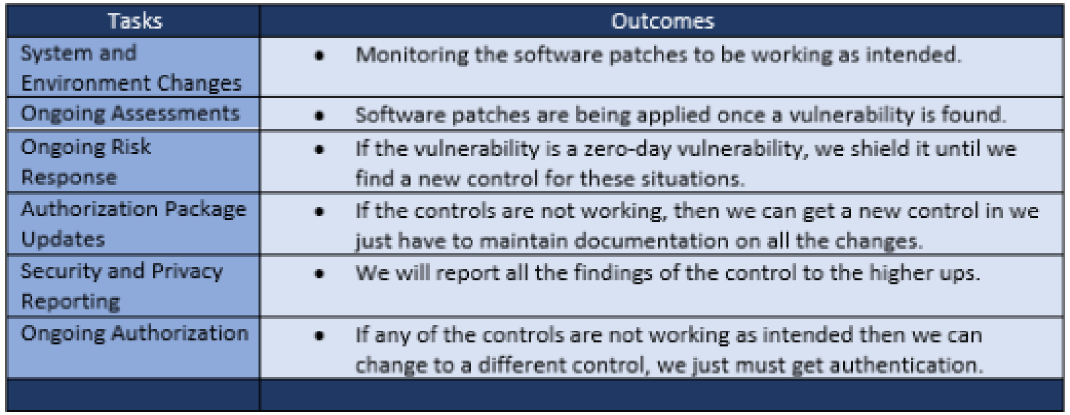
Monitor

- To look at the system all the time to find problems. Monitoring the control and doing its job.

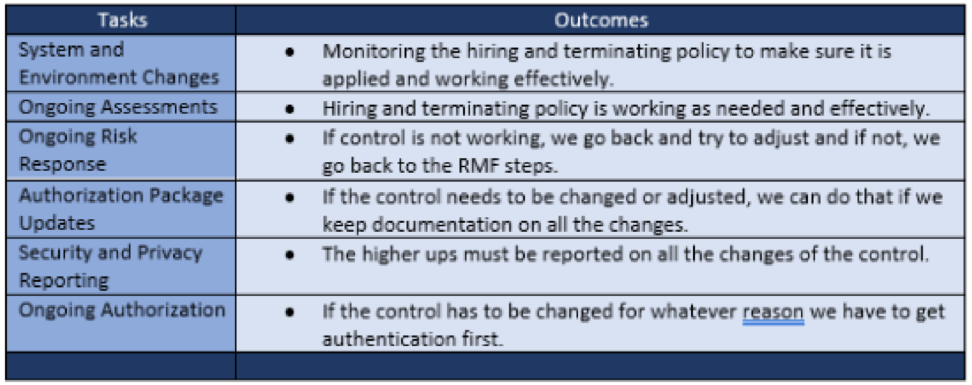
Cryptography



Tasks	Outcomes
System and Environment Changes	• Monitoring the Encryption to be working as intended and following in the progress within a dashboard.
Ongoing Assessments	• Cryptography is working where it has to work.
Ongoing Risk Response	• If cryptography is not working as intended, then go back to the Risk Management Framework from the beginning.
Authorization Package Updates	• If the control is not working as intended, then we go back and try to fix or we change the control, but we keep documentation of all the updates.
Security and Privacy Reporting	• Report to the higher ups about the findings of the control.
Ongoing Authorization	• If any of the systems with cryptography are not working we go and get authentication for any new changes or updates.



Tasks	Outcomes
System and Environment Changes	• Monitoring the software patches to be working as intended.
Ongoing Assessments	• Software patches are being applied once a vulnerability is found.
Ongoing Risk Response	• If the vulnerability is a zero-day vulnerability, we shield it until we find a new control for these situations.
Authorization Package Updates	• If the controls are not working, then we can get a new control in we just have to maintain documentation on all the changes.
Security and Privacy Reporting	• We will report all the findings of the control to the higher ups.
Ongoing Authorization	• If any of the controls are not working as intended then we can change to a different control, we just must get authentication.



Tasks	Outcomes
System and Environment Changes	• Monitoring the hiring and terminating policy to make sure it is applied and working effectively.
Ongoing Assessments	• Hiring and terminating policy is working as needed and effectively.
Ongoing Risk Response	• If control is not working, we go back and try to adjust and if not, we go back to the RMF steps.
Authorization Package Updates	• If the control needs to be changed or adjusted, we can do that if we keep documentation on all the changes.
Security and Privacy Reporting	• The higher ups must be reported on all the changes of the control.
Ongoing Authorization	• If the control has to be changed for whatever reason we have to get authentication first.

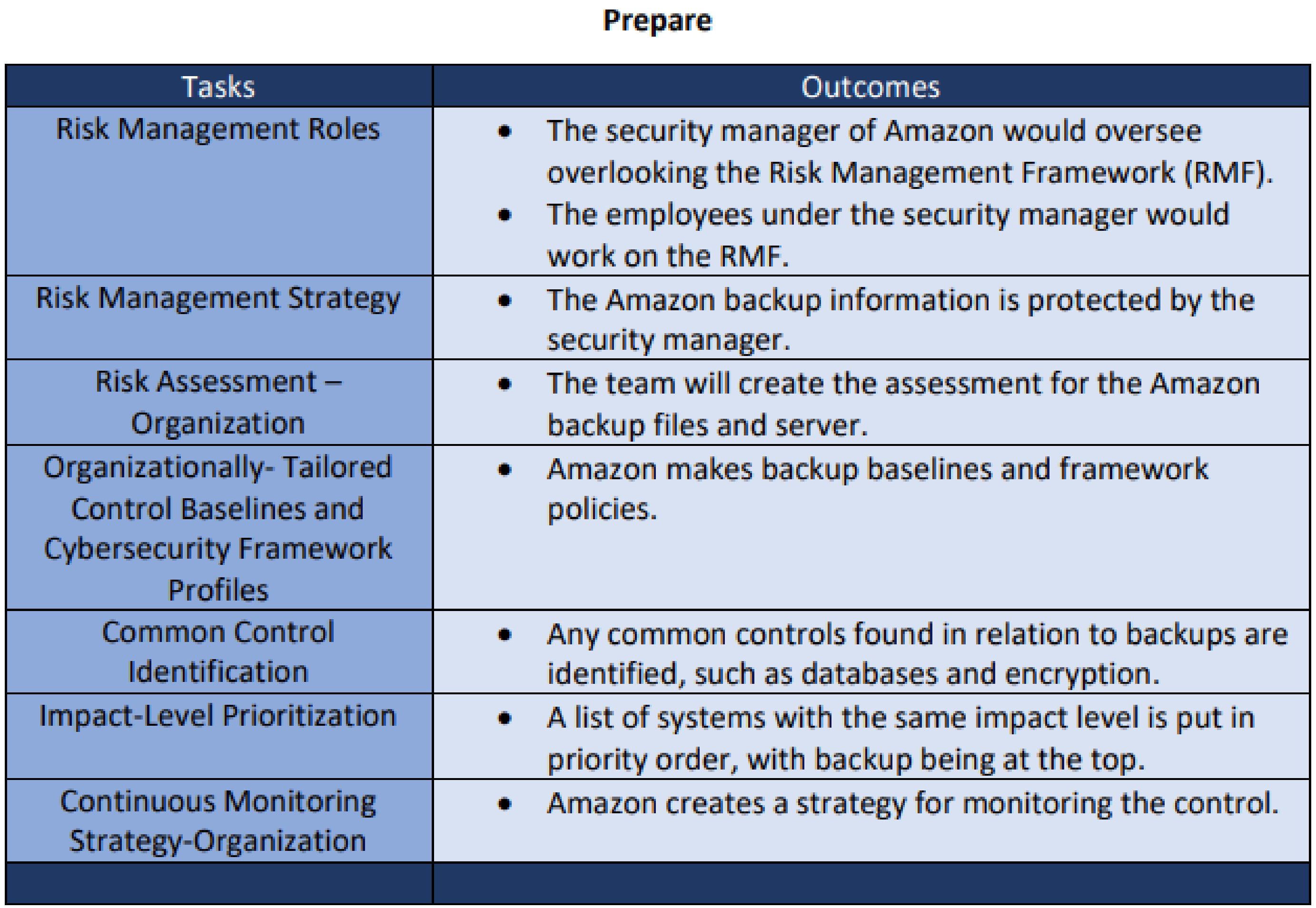
Data Protection Control

Control: Backup

System: Amazon

We will follow the RMF (Risk Management Framework) for this system following the backup control.

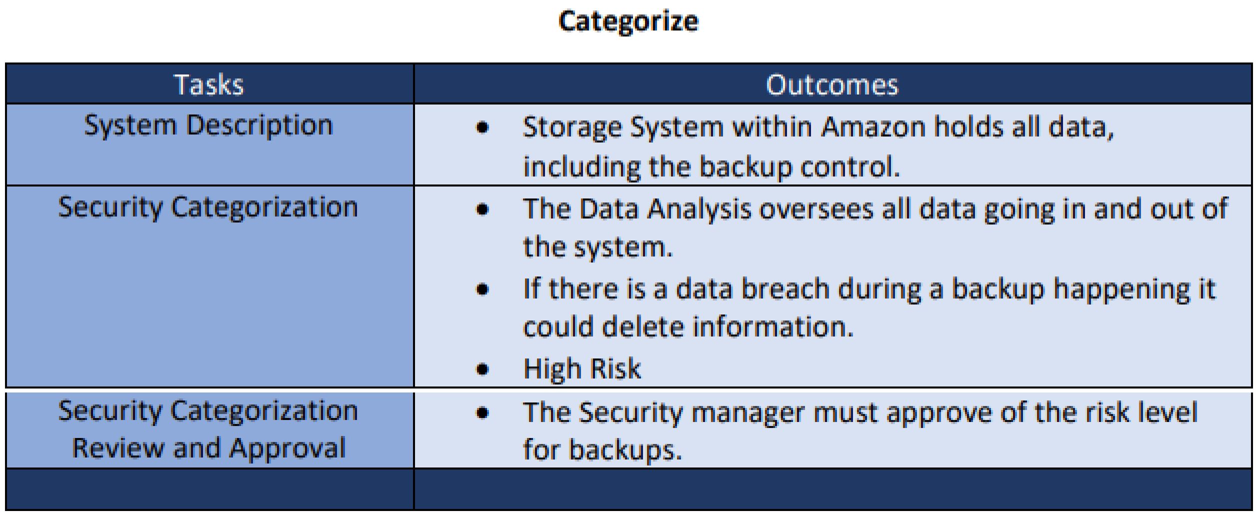
Prepare for Backup Control



Prepare

Tasks	Outcomes
Risk Management Roles	• The security manager of Amazon would oversee overlooking the Risk Management Framework (RMF). • The employees under the security manager would work on the RMF.
Risk Management Strategy	• The Amazon backup information is protected by the security manager.
Risk Assessment – Organization	• The team will create the assessment for the Amazon backup files and server.
Organizationally- Tailored Control Baselines and Cybersecurity Framework Profiles	• Amazon makes backup baselines and framework policies.
Common Control Identification	• Any common controls found in relation to backups are identified, such as databases and encryption.
Impact-Level Prioritization	• A list of systems with the same impact level is put in priority order, with backup being at the top.
Continuous Monitoring Strategy-Organization	• Amazon creates a strategy for monitoring the control.

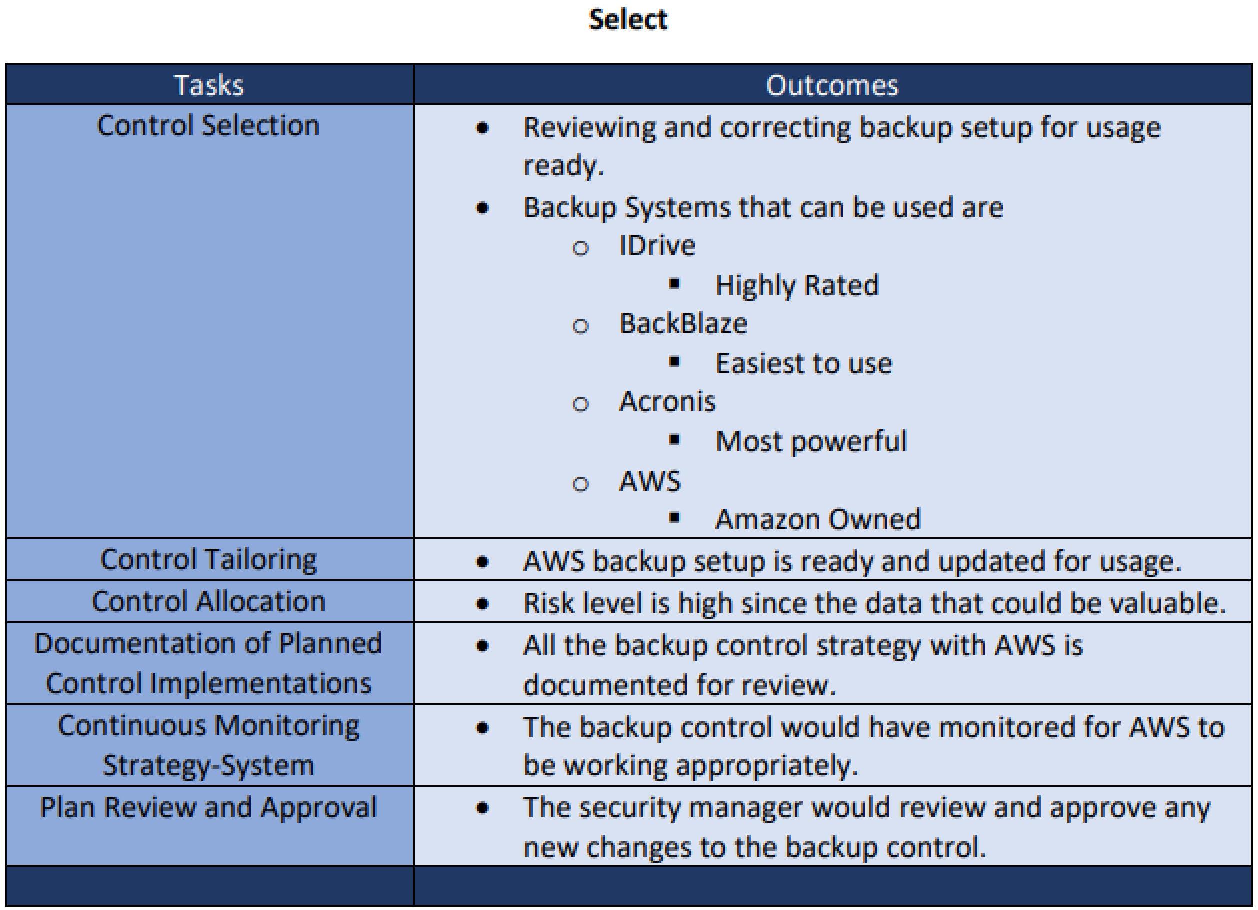
Categorize for Backup Control



Categorize

Tasks	Outcomes
System Description	• Storage System within Amazon holds all data, including the backup control.
Security Categorization	• The Data Analysis oversees all data going in and out of the system. • If there is a data breach during a backup happening it could delete information. • High Risk
Security Categorization Review and Approval	• The Security manager must approve of the risk level for backups.

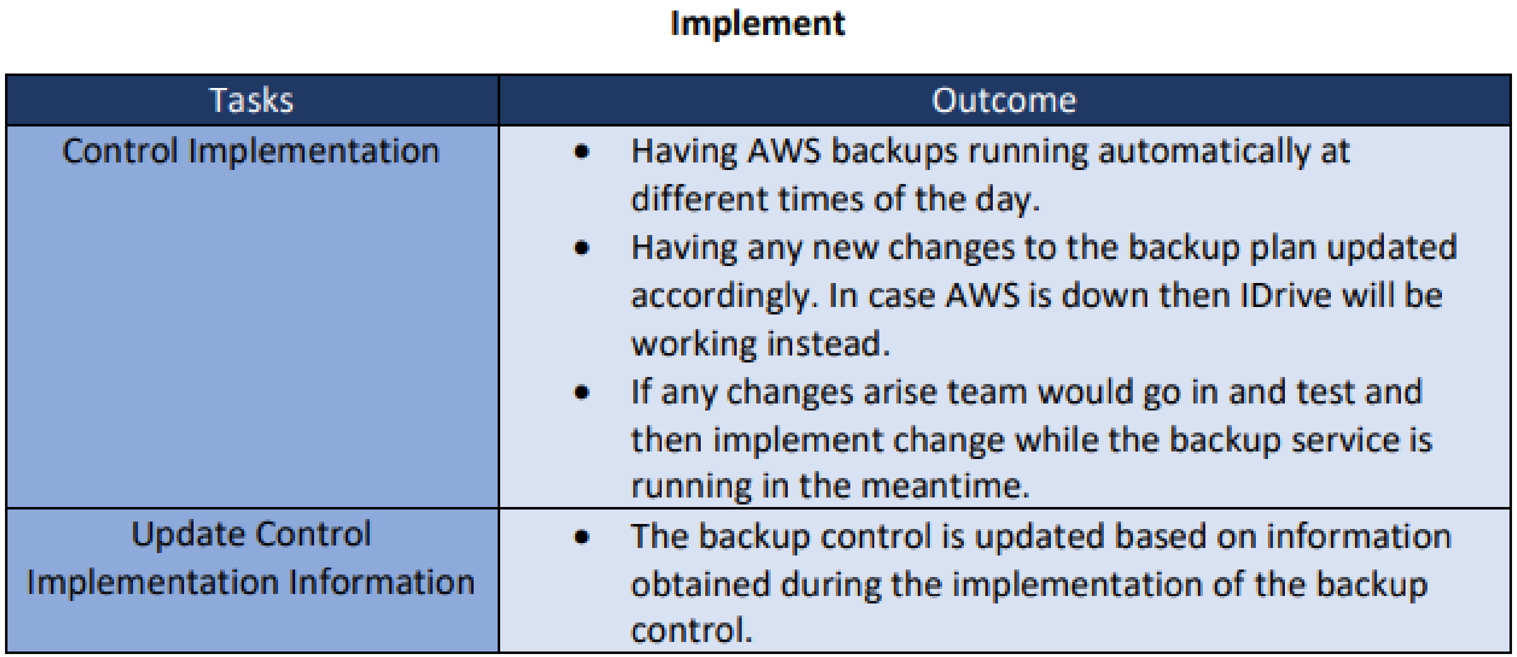
Select for Backup Control



Select

Tasks	Outcomes
Control Selection	- Reviewing and correcting backup setup for usage ready. - Backup Systems that can be used are ○ IDrive ▪ Highly Rated ○ BackBlaze ▪ Easiest to use ○ Acronis ▪ Most powerful ○ AWS ▪ Amazon Owned
Control Tailoring	- AWS backup setup is ready and updated for usage.
Control Allocation	- Risk level is high since the data that could be valuable.
Documentation of Planned Control Implementations	- All the backup control strategy with AWS is documented for review.
Continuous Monitoring Strategy-System	- The backup control would have monitored for AWS to be working appropriately.
Plan Review and Approval	- The security manager would review and approve any new changes to the backup control.

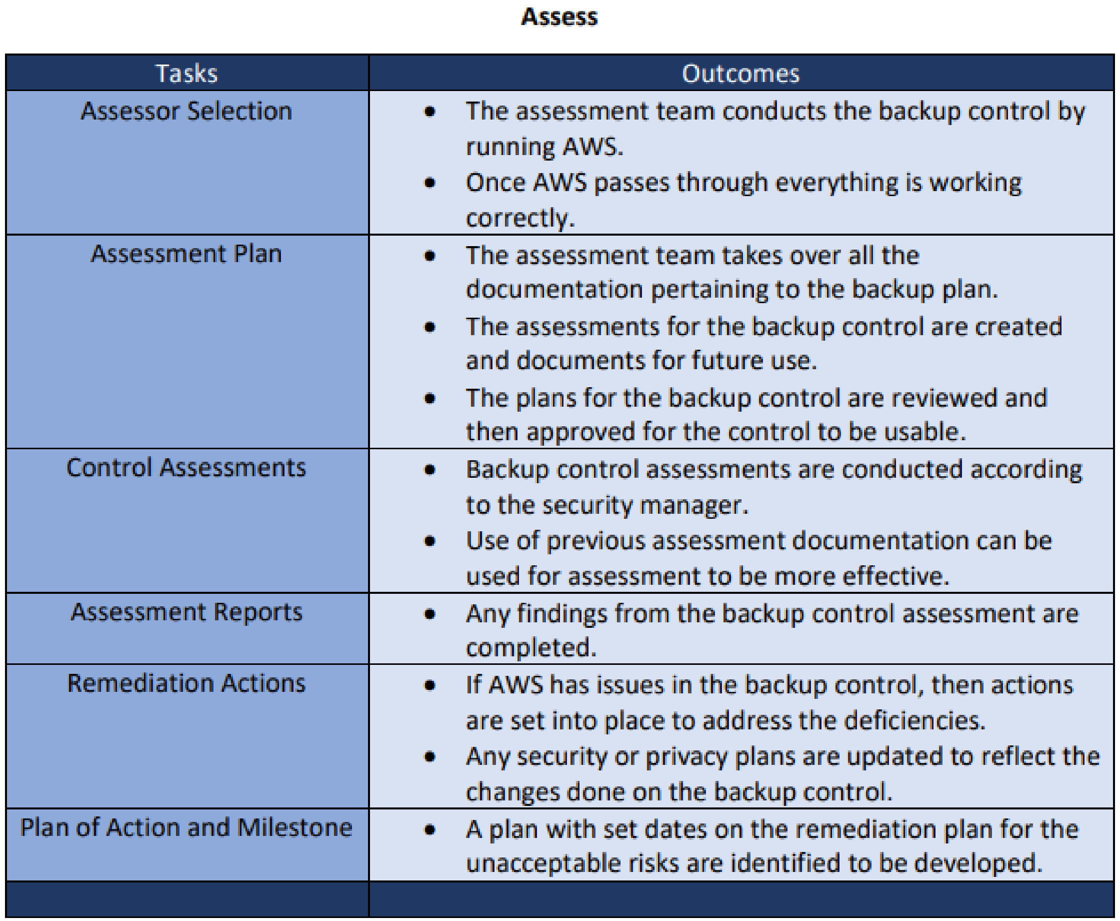
Implement for Backup Control



Implement

Tasks	Outcome
Control Implementation	• Having AWS backups running automatically at different times of the day. • Having any new changes to the backup plan updated accordingly. In case AWS is down then IDrive will be working instead. • If any changes arise team would go in and test and then implement change while the backup service is running in the meantime.
Update Control Implementation Information	• The backup control is updated based on information obtained during the implementation of the backup control.

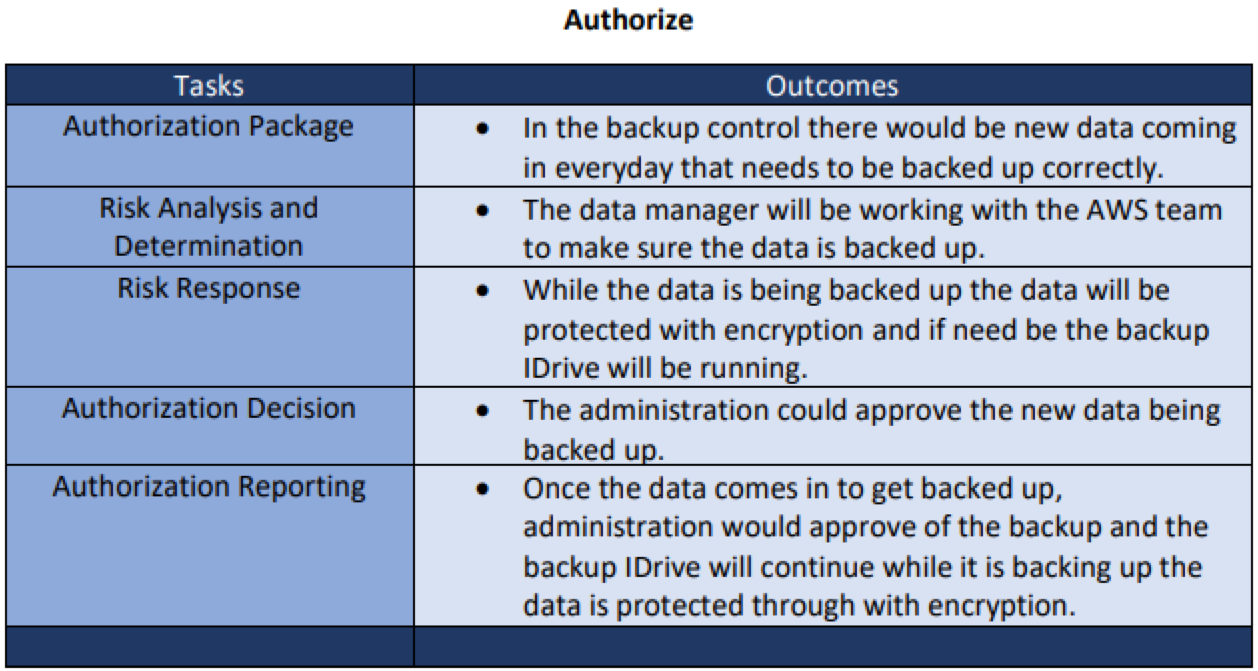
Assess for Backup Control



Assess

Tasks	Outcomes
Assessor Selection	- The assessment team conducts the backup control by running AWS. - Once AWS passes through everything is working correctly.
Assessment Plan	- The assessment team takes over all the documentation pertaining to the backup plan. - The assessments for the backup control are created and documents for future use. - The plans for the backup control are reviewed and then approved for the control to be usable.
Control Assessments	- Backup control assessments are conducted according to the security manager. - Use of previous assessment documentation can be used for assessment to be more effective.
Assessment Reports	- Any findings from the backup control assessment are completed.
Remediation Actions	- If AWS has issues in the backup control, then actions are set into place to address the deficiencies. - Any security or privacy plans are updated to reflect the changes done on the backup control.
Plan of Action and Milestone	- A plan with set dates on the remediation plan for the unacceptable risks are identified to be developed.

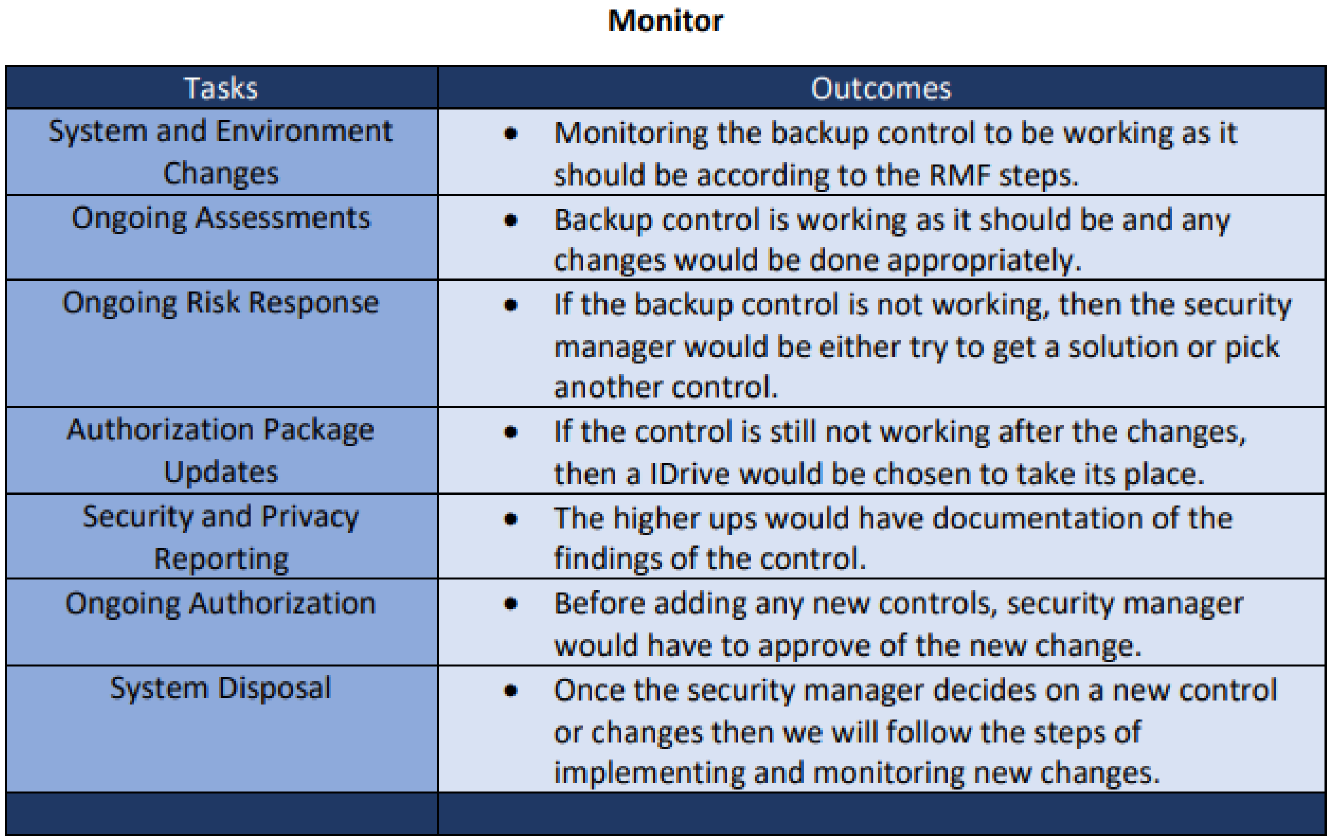
Authorize for Backup Control



Authorize

Tasks	Outcomes
Authorization Package	• In the backup control there would be new data coming in everyday that needs to be backed up correctly.
Risk Analysis and Determination	• The data manager will be working with the AWS team to make sure the data is backed up.
Risk Response	• While the data is being backed up the data will be protected with encryption and if need be the backup IDrive will be running.
Authorization Decision	• The administration could approve the new data being backed up.
Authorization Reporting	• Once the data comes in to get backed up, administration would approve of the backup and the backup IDrive will continue while it is backing up the data is protected through with encryption.

Monitor for Backup Control



Monitor

Tasks	Outcomes
System and Environment Changes	• Monitoring the backup control to be working as it should be according to the RMF steps.
Ongoing Assessments	• Backup control is working as it should be and any changes would be done appropriately.
Ongoing Risk Response	• If the backup control is not working, then the security manager would be either try to get a solution or pick another control.
Authorization Package Updates	• If the control is still not working after the changes, then a IDrive would be chosen to take its place.
Security and Privacy Reporting	• The higher ups would have documentation of the findings of the control.
Ongoing Authorization	• Before adding any new controls, security manager would have to approve of the new change.
System Disposal	• Once the security manager decides on a new control or changes then we will follow the steps of implementing and monitoring new changes.

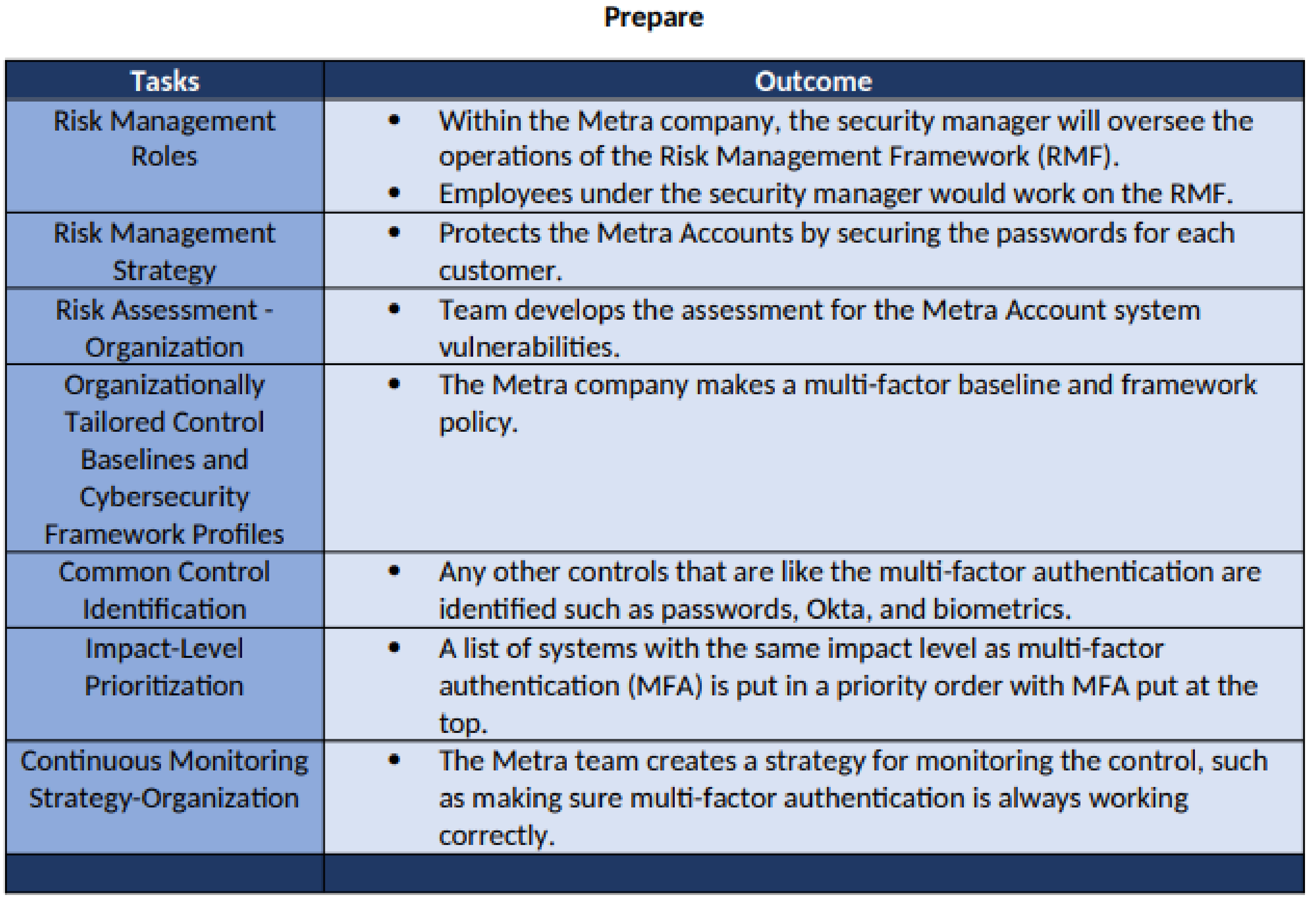
Security Technical Control

Control: Multi-Factor Authenticator

System: Metra

We will follow the RMF (Risk Management Framework) for this system with the control selected.

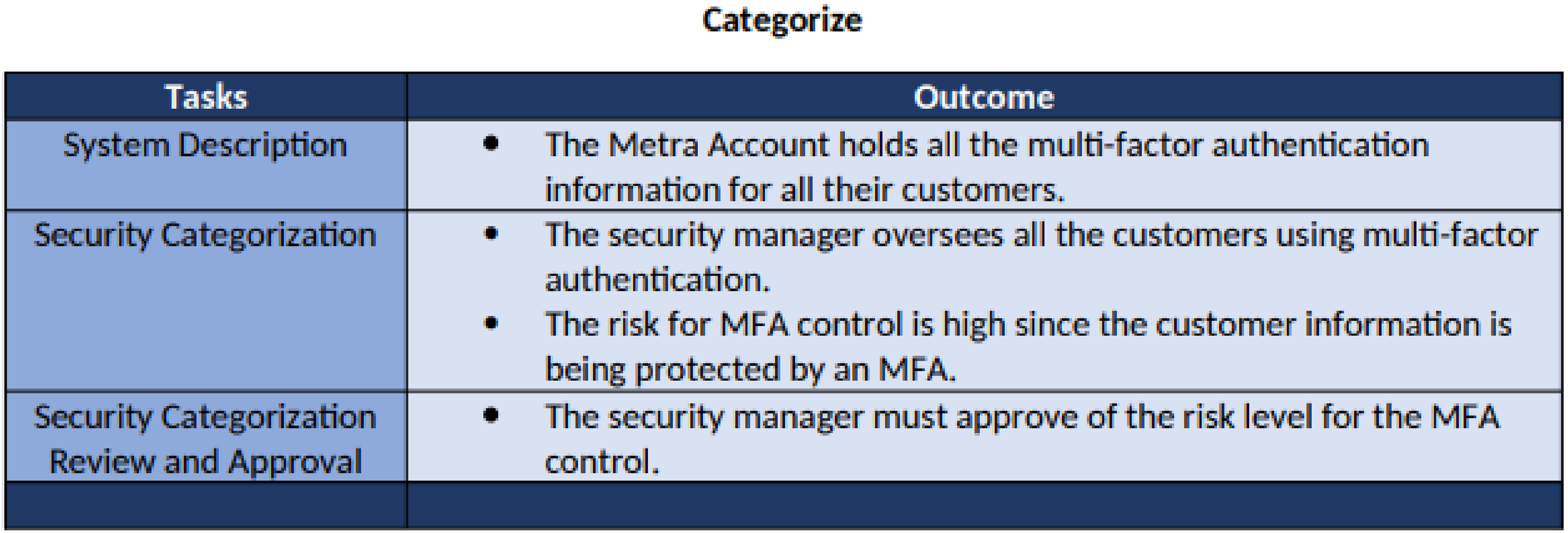
Prepare for Security Technical Control



Prepare

Tasks	Outcome
Risk Management Roles	- Within the Metra company, the security manager will oversee the operations of the Risk Management Framework (RMF). - Employees under the security manager would work on the RMF.
Risk Management Strategy	- Protects the Metra Accounts by securing the passwords for each customer.
Risk Assessment - Organization	- Team develops the assessment for the Metra Account system vulnerabilities.
Organizationally Tailored Control Baselines and Cybersecurity Framework Profiles	- The Metra company makes a multi-factor baseline and framework policy.
Common Control Identification	- Any other controls that are like the multi-factor authentication are identified such as passwords, Okta, and biometrics.
Impact-Level Prioritization	- A list of systems with the same impact level as multi-factor authentication (MFA) is put in a priority order with MFA put at the top.
Continuous Monitoring Strategy-Organization	- The Metra team creates a strategy for monitoring the control, such as making sure multi-factor authentication is always working correctly.

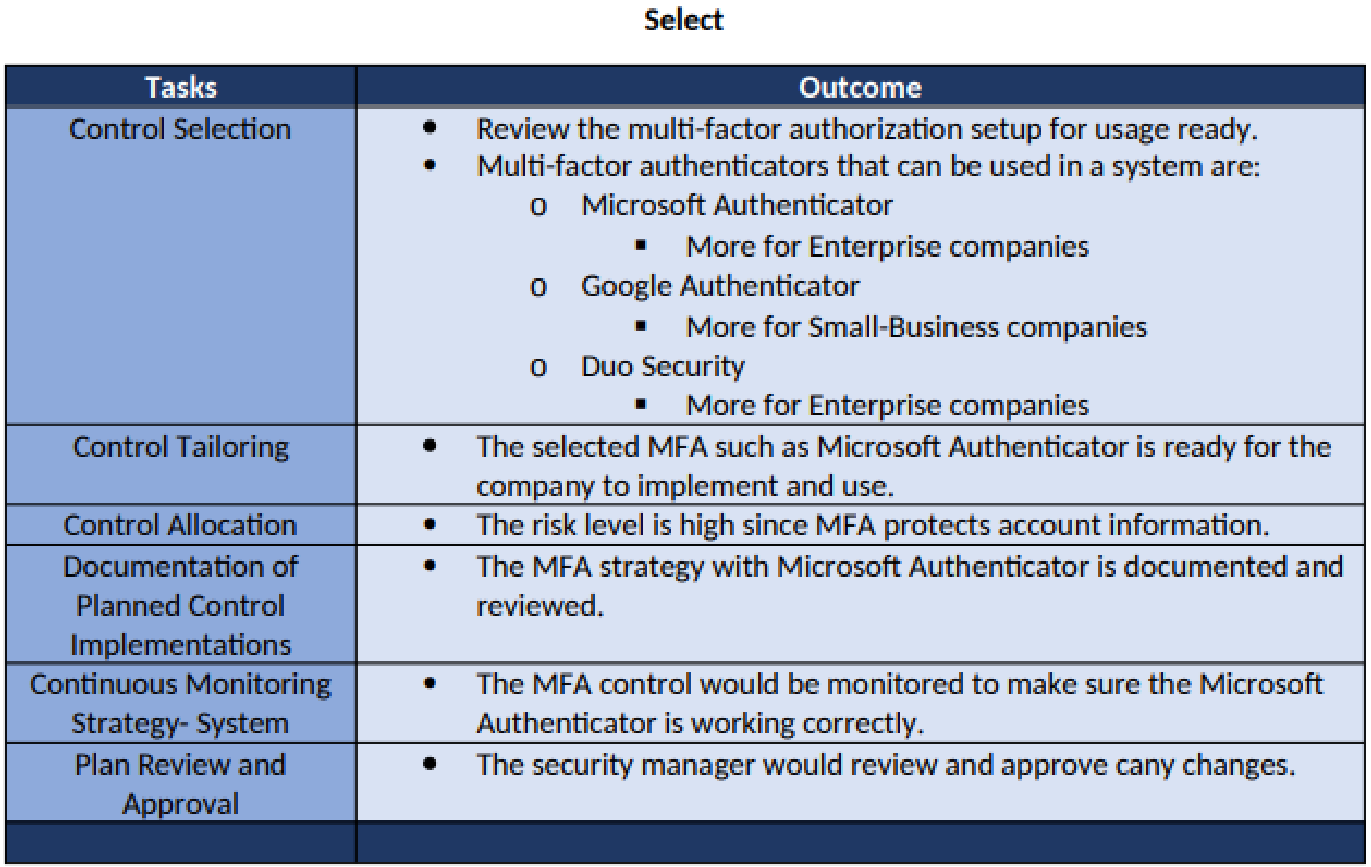
Categorize for Security Technical Control



Categorize

Tasks	Outcome
System Description	- The Metra Account holds all the multi-factor authentication information for all their customers.
Security Categorization	- The security manager oversees all the customers using multi-factor authentication. - The risk for MFA control is high since the customer information is being protected by an MFA.
Security Categorization Review and Approval	- The security manager must approve of the risk level for the MFA control.

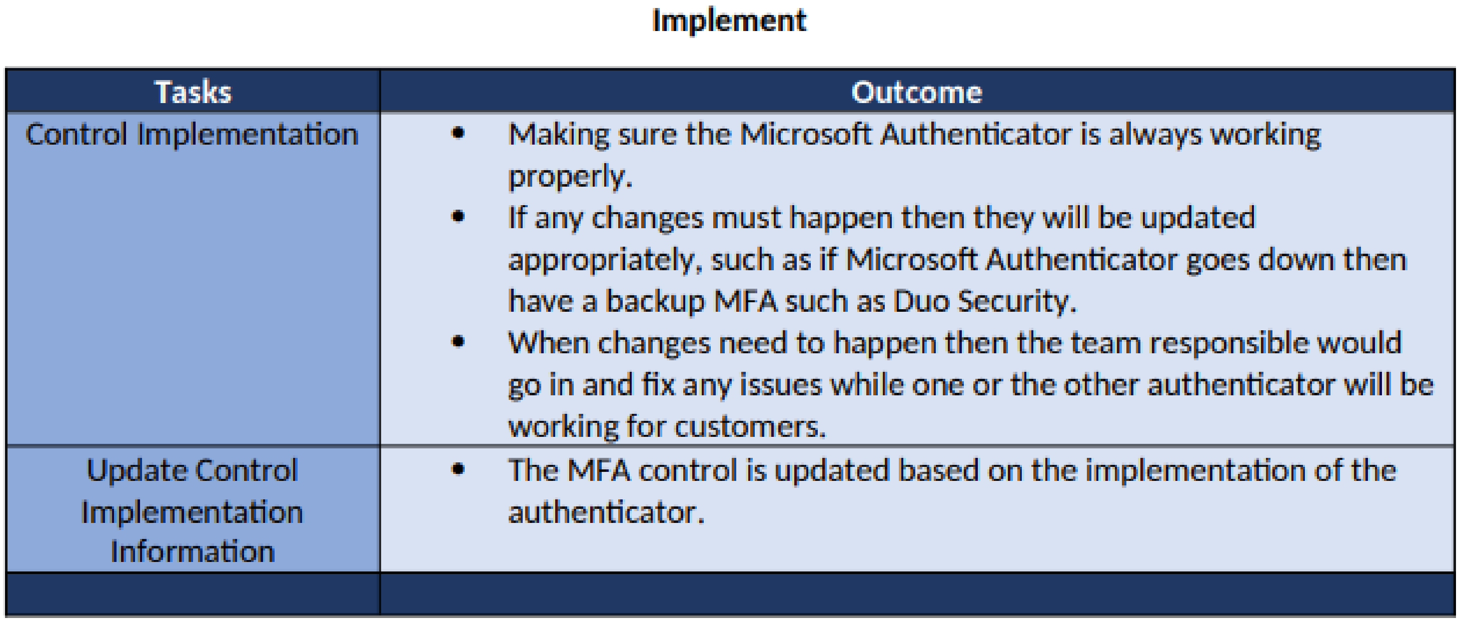
Select for Security Technical Control



Select

Tasks	Outcome
Control Selection	• Review the multi-factor authorization setup for usage ready. • Multi-factor authenticators that can be used in a system are: o Microsoft Authenticator ▪ More for Enterprise companies o Google Authenticator ▪ More for Small-Business companies o Duo Security ▪ More for Enterprise companies
Control Tailoring	• The selected MFA such as Microsoft Authenticator is ready for the company to implement and use.
Control Allocation	• The risk level is high since MFA protects account information.
Documentation of Planned Control Implementations	• The MFA strategy with Microsoft Authenticator is documented and reviewed.
Continuous Monitoring Strategy- System	• The MFA control would be monitored to make sure the Microsoft Authenticator is working correctly.
Plan Review and Approval	• The security manager would review and approve cany changes.

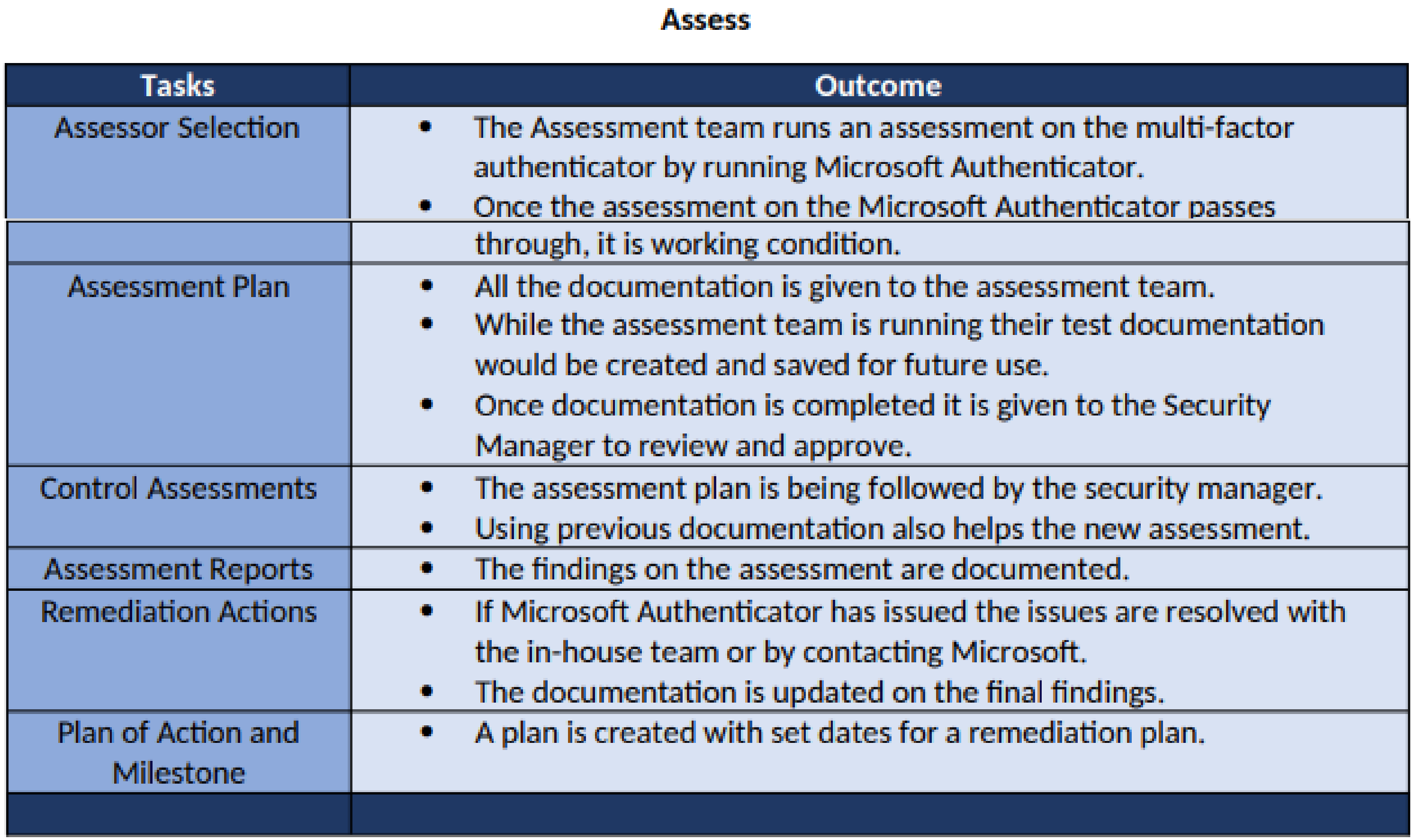
Implement for Security Technical Control



Implement

Tasks	Outcome
Control Implementation	• Making sure the Microsoft Authenticator is always working properly. • If any changes must happen then they will be updated appropriately, such as if Microsoft Authenticator goes down then have a backup MFA such as Duo Security. • When changes need to happen then the team responsible would go in and fix any issues while one or the other authenticator will be working for customers.
Update Control Implementation Information	• The MFA control is updated based on the implementation of the authenticator.

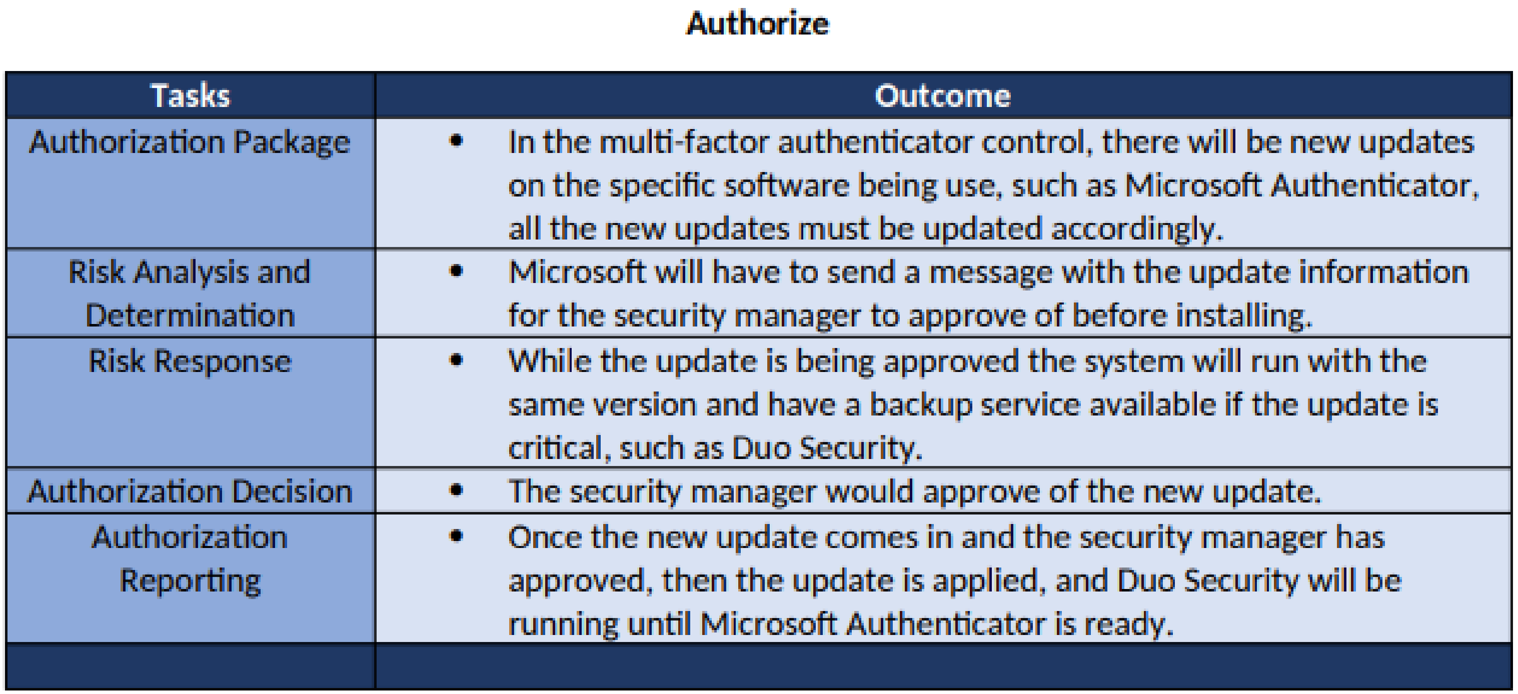
Assess for Security Technical Control



Assess

Tasks	Outcome
Assessor Selection	• The Assessment team runs an assessment on the multi-factor authenticator by running Microsoft Authenticator. • Once the assessment on the Microsoft Authenticator passes through, it is working condition.
Assessment Plan	• All the documentation is given to the assessment team. • While the assessment team is running their test documentation would be created and saved for future use. • Once documentation is completed it is given to the Security Manager to review and approve.
Control Assessments	• The assessment plan is being followed by the security manager. • Using previous documentation also helps the new assessment.
Assessment Reports	• The findings on the assessment are documented.
Remediation Actions	• If Microsoft Authenticator has issued the issues are resolved with the in-house team or by contacting Microsoft. • The documentation is updated on the final findings.
Plan of Action and Milestone	• A plan is created with set dates for a remediation plan.

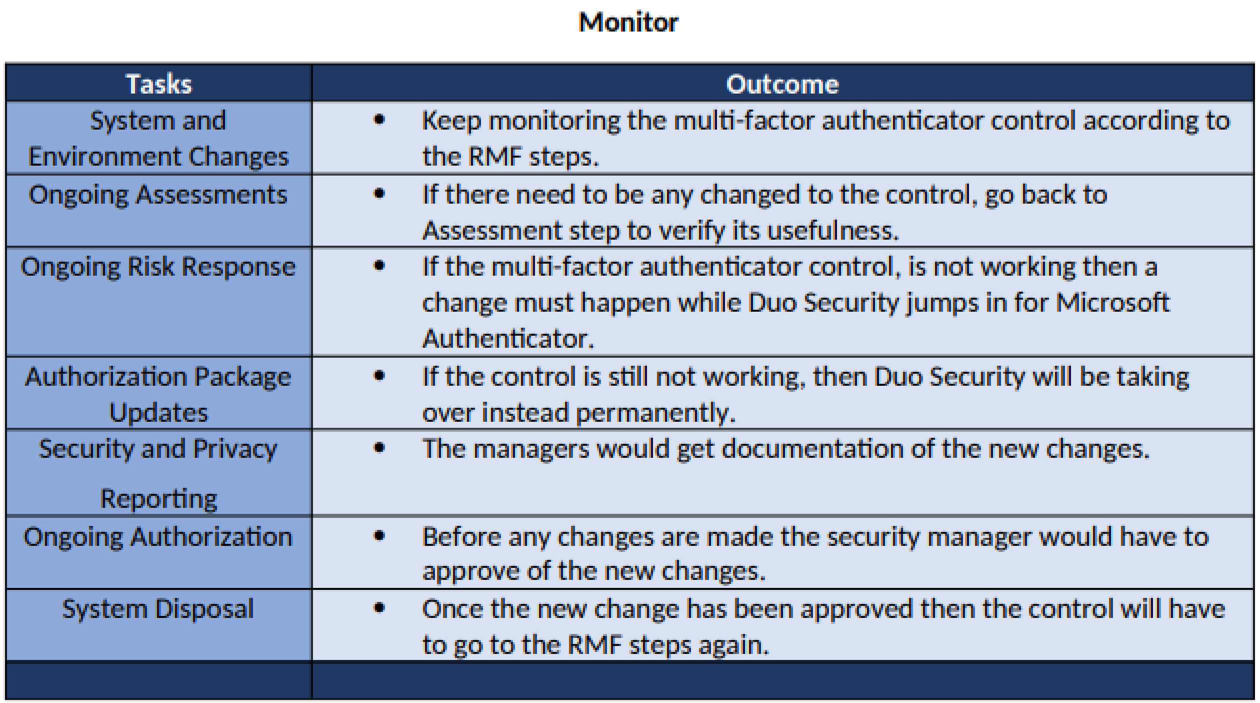
Authorize for Security Technical Control



Authorize

Tasks	Outcome
Authorization Package	• In the multi-factor authenticator control, there will be new updates on the specific software being use, such as Microsoft Authenticator, all the new updates must be updated accordingly.
Risk Analysis and Determination	• Microsoft will have to send a message with the update information for the security manager to approve of before installing.
Risk Response	• While the update is being approved the system will run with the same version and have a backup service available if the update is critical, such as Duo Security.
Authorization Decision	• The security manager would approve of the new update.
Authorization Reporting	• Once the new update comes in and the security manager has approved, then the update is applied, and Duo Security will be running until Microsoft Authenticator is ready.

Monitor for Security Technical Control



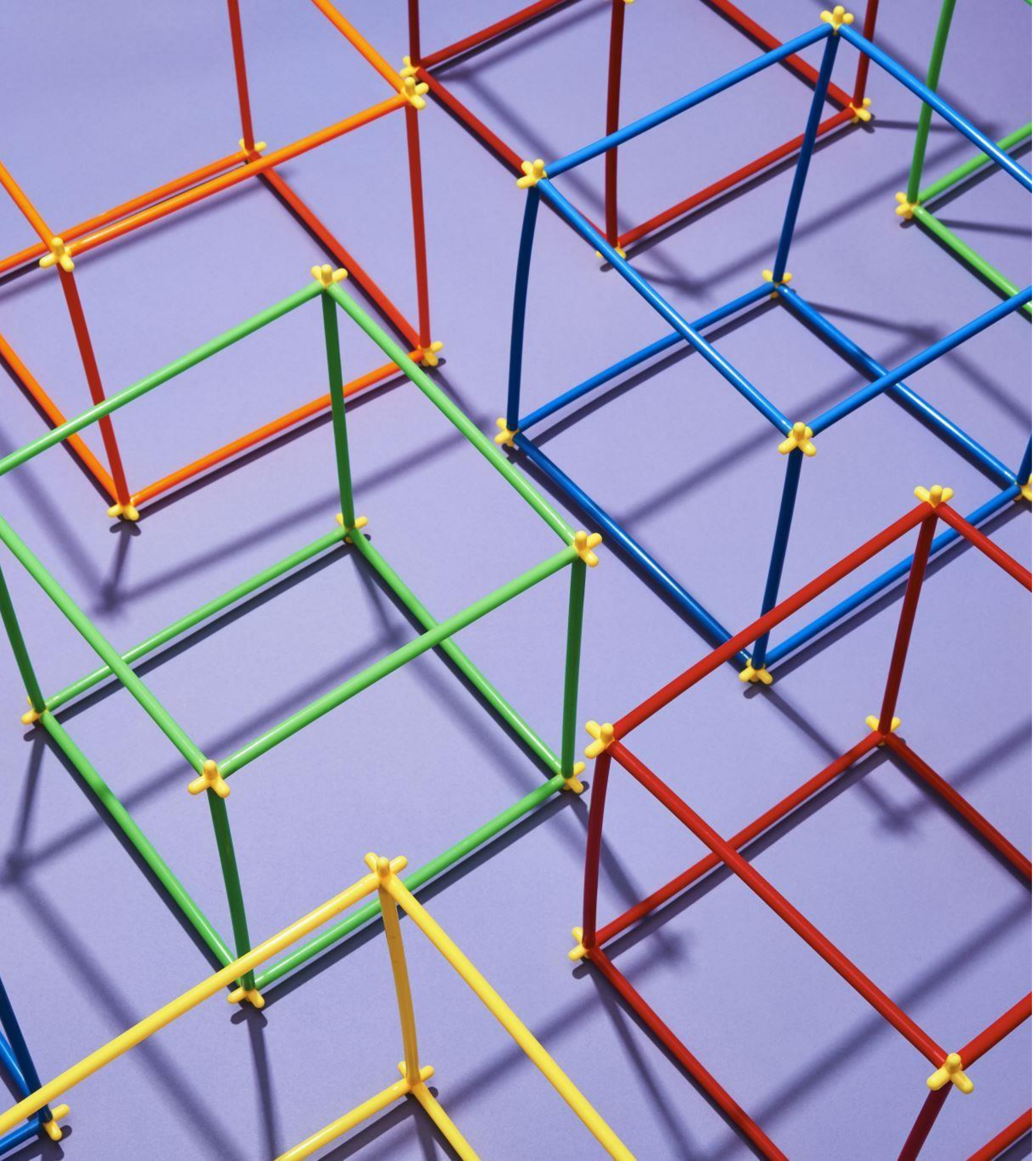
Monitor

Tasks	Outcome
System and Environment Changes	• Keep monitoring the multi-factor authenticator control according to the RMF steps.
Ongoing Assessments	• If there need to be any changed to the control, go back to Assessment step to verify its usefulness.
Ongoing Risk Response	• If the multi-factor authenticator control, is not working then a change must happen while Duo Security jumps in for Microsoft Authenticator.
Authorization Package Updates	• If the control is still not working, then Duo Security will be taking over instead permanently.
Security and Privacy Reporting	• The managers would get documentation of the new changes.
Ongoing Authorization	• Before any changes are made the security manager would have to approve of the new changes.
System Disposal	• Once the new change has been approved then the control will have to go to the RMF steps again.

Selecting a tool for security domains

Security Domains: Server, Identity Managment, Network, and Data Protection

Tools: Windows Firewall Control 4, Oracle Identity Management, Snort, and Clickup

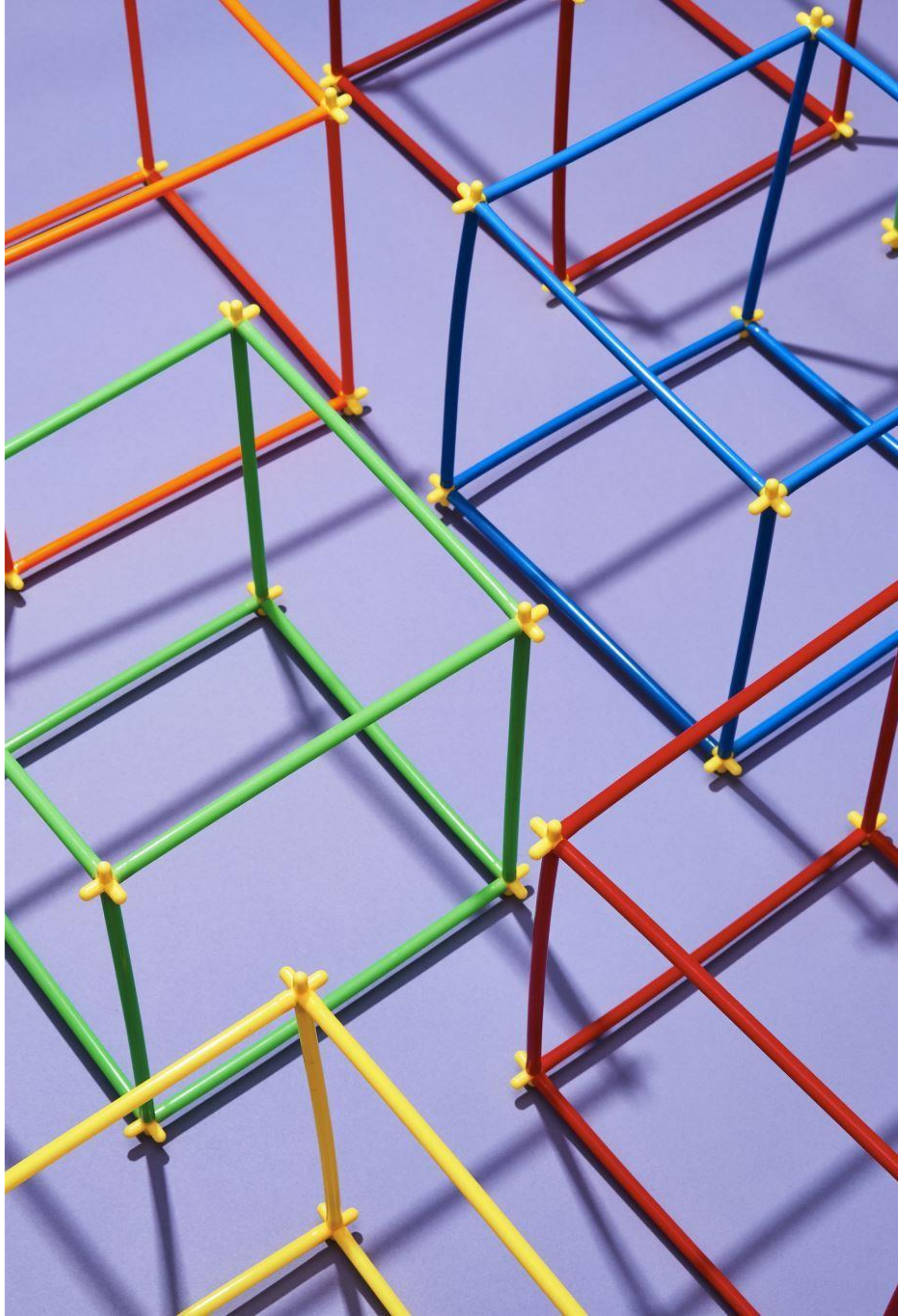


Server: Host Firewall

- A host-based firewall is a piece of firewall software that runs on an individual computer that is connected to a network.
- Windows Firewall Control 4
  - Extends the functions of Windows firewalls and provides new features.
  - Vendor: Binisoft
  - Categories:
    - Disable the ability of other programs to tamper Windows Firewall rules.
    - Possibility to find and display duplicate firewall rules.
    - Offers filtering modes such as high, medium, low and no filtering.
    - Protection to unauthorized uninstallations

IAM: Identity Provisioning

- The process of creating, managing, and deleting digital identities in a computer system.
- Oracle Identity Management
  - Offers secured access to Enterprise applications for both cloud and on-premises deployment.
  - Vendor: Oracle
  - Categories:
    - Flexible protection for workloads
    - Helps companies comply with regulatory mandates and reduces operational costs.
    - Highly customizable and can be deployed as software or on the cloud.



Network: Link Layer Network Security

- Manages sets of bits for transmission in the form of packets.
- Snort
  - A network-based intrusion detection system.
  - Vendor: Cisco
  - Categories:
    - Real-time traffic monitor
    - Packet Logging
    - Open Source
    - Can be installed in any network environment

Data Protection: Secure Collaboration

- A type of electronic information sharing capability for multiple parties to securely share data.
- ClickUp
  - Productivity and secure collaboration tools used by small and large companies.
  - Vendor: Mango Technologies, Inc.
  - Categories:
    - Uses Amazon Web Services (AWS) for all the data they hold.
    - All the communication are encrypted over 256-bit SSL.
    - They train all their employees on the latest security protocols.