Risk Management Policy Notes (Bri’s answers)

Policy Section	**Recommended Change(s)**	**Reasoning**
Access Control	Workstations should be configured to automatically lock. Privileged functions should not be carried out by non-privileged accounts.	Locking workstations automatically help prevent data breaches if an employee forgets to lock their station. In addition, unauthorized users should not have access to data. Implementing least privilege is most effective.
Configuration Management	Only authorized security team members should install software on devices.	Assessing changes prior to implementation has a positive impact, however all users should not be able to install software on their workstations in order to avoid threats such as phishing.
Physical and Environmental Protection	Once an individual separates from the organization, they should either be archived for logging purposes with credentials revoked or removed from the access list altogether with revoked credentials. In addition, consider implementing another security measure, such as biometrics rather than two forms of ID.	Implementing biometrics or another security measure will prevent impersonation and/or unauthorized individuals accessing server rooms and sensitive data.
Risk Assessment	The security team should consider additional resources to determine the cyber threat environment.	To maintain integrity, security personnel should seek information about the cybersecurity landscape from reputable resources.
Awareness & Training	All employees should undergo regular cybersecurity awareness training.	Since the cybersecurity landscape is constantly changing, all employees should be up to date on training, which includes new employees.

My Self Assessment:
In this activity, I identified areas where the NIST framework could be implemented for risk management policy modifications. The majority of the answers were correct, however, diving a little deeper into the framework for the reasoning section and incorporating terminology from the lessons in this module (Module 3) would have made the Reasoning section much stronger.

Risk Management Policy Notes (Google’s Exemplar)

Policy Section	**Recommended Change(s)**	**Reasoning**
Access Control	In addition to requiring employees to lock their devices, devices should be configured to automatically lock after two minutes of inactivity and require the user to reenter their credentials when they return.	If an employee leaves a device unlocked while stepping away from their workstation, the information on the device may be vulnerable to unauthorized people. This could result in a data breach, which poses reputational and legal risks to the company. Configuring devices to automatically lock after two minutes decreases these risks.
Awareness and Training	New employees should still be trained on cyber threats. Training should be added for current employees on a regular basis and when system changes make training necessary. Training should be specific to each employee's role.	The cyber threat landscape is constantly changing, so it’s important that employees be trained regularly on cybersecurity best practices to prevent a data breach or other incident. Employees in different roles and departments have access to specific information that could result in different kinds of risk—such as business slowdowns if needed systems stop working—or legal risk if sensitive data is leaked.
Configuration Management	Users can install approved, vetted software on their workstations as necessary. Unvetted and/or unapproved software may not be downloaded on devices.	Allowing users to download unvetted software may lead users to download applications that could introduce malware into the environment. Therefore, it is important for Cymbal Bank to know and control the software installed onto its systems.
Identification and Authentication	Employee passwords should be allowed to contain spaces and special characters.	Including special characters allows employees to create stronger, more complex passwords. This makes it more difficult for bad actors to gain unauthorized access, which could lead to data loss.
Physical and Environmental Protection	Individuals must be removed from the server room authorization list if they no longer have a business need to access it.	If an employee switches roles or leaves the company, the individual no longer has a business need to access Cymbal Bank’s server room. Access needs to be tightly controlled to ensure the servers and the data they’re processing aren't vulnerable to unauthorized people.
System and Information Integrity	Security alert and advisory information should be shared throughout the entire organization, not just with the security team.	It’s important for all employees to receive security alerts and advisory information because all employees need to contribute to keep the organization’s infrastructure secure.

GOOGLE RISK MANAGEMENT POLICY ACTIVITY INSTRUCTIONS

Scenario

Review the following scenario.

Then, access the supporting materials before moving on to the next course item to take the quiz. As part of the security team at Cymbal Bank, you're responsible for keeping the organization in compliance with applicable regulations. You also play a part in your organization's risk analysis and risk management processes. Cymbal Bank is updating its risk management policy, and the cloud security team has been asked to revise the sections that deal with IT assets. Cymbal Bank is currently moving its IT infrastructure to a hybrid cloud model. Therefore, it's important for the organization's risk management policy to align with external regulations to avoid the negative impacts of non-compliance. Each member of the team has been asked to assess the risk management policy for compliance with a different risk management framework. You have been assigned to assess the policy against the NIST SP 800-53 framework. In this activity, you'll assess Cymbal Bank's current risk management policy for compliance with NIST SP 800-53 guidelines, identify areas for improvement, and provide your reasoning for 1 your suggested improvements—including the negative organizational impacts Cymbal Bank will mitigate by bringing the policy into compliance.

Step-By-Step Instructions

Consult the supporting materials to answer the quiz questions in the asset that follows. After you complete the quiz, you can compare your answers to the feedback provided.

Step 1: Access supporting materials

The following supporting materials will help you complete this activity. Keep them open as you proceed to the questions.

Step 2: Assess the risk management policy

Assess each section of the Risk management policy for compliance with the corresponding NIST SP 800-53 Revision 5 standards linked in the supporting materials.

Step 3: Identify areas for improvement

Determine what needs to be added or clarified in each section of the Risk management policy to strengthen it and bring it into better alignment with the NIST framework.

Then, in the Policy Section of the Risk management policy notes template, list 4–6 sections of the risk management policy that are non-compliant with NIST SP 800-53.

In the Recommended Change(s) column, write 1–2 sentences explaining the changes or additions you think should be made to the policy to address each of these issues.

Step 4: Provide your reasoning for the changes

In the Reasoning column of the template, write 2–3 sentences explaining your reasoning for the changes you suggested in Step 3. Include how your suggested changes will help improve the cloud environment's security and which negative organizational impacts of non-compliance the changes will help to prevent.