Risk Management Policy Notes

As part of the security team at Cymbal Bank, I'm responsible for keeping the organization in compliance with applicable regulations. I 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. I was assigned to assess the policy against the NIST SP 800-53 framework. In this activity, I'll assess Cymbal Bank's current risk management policy for compliance with NIST SP 800-53 guidelines, identify areas for improvement, and provide my reasoning.

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	Allowing users to download unvetted software may lead users to download applications that could introduce malware

	software may not be downloaded on devices.	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.