ACME

PROJECT MANAGEMENT

Name: Juliano Alves de Souza
Date: 08/17/2024

CYB420
SNHU

CYB 420 Project Two Milestone One Project Charter

I. Project Charter

Project Name
ACME Multilayered Security Enhancement

Mission Statement
The ACME Multilayered Security Enhancement Initiative is a strategic endeavor designed to protect and secure the very foundation of our organization's operations—its data, processes, and people. In today's rapidly evolving digital landscape, where cyber threats grow increasingly sophisticated, ACME cannot afford to leave any aspect of its security to chance. This initiative is not just about fixing vulnerabilities; it is about transforming our security infrastructure into a resilient, proactive shield against potential threats. Our mission is to elevate ACME's security posture by implementing a comprehensive, multi-layered defense strategy that addresses critical vulnerabilities across three core domains: people, process, and technology. We will empower our employees through targeted security awareness programs, ensuring they are the first line of defense against social engineering and insider threats. We will strengthen access control mechanisms, granting only the necessary permissions to safeguard sensitive data. Furthermore, we will deploy an automated patch management system to ensure that our technology is always up-to-date and protected from known exploits. This initiative is more than a project—it is a commitment to securing ACME's future. By fortifying our defenses, we not only protect our current operations but also pave the way for sustainable growth, regulatory compliance, and the trust of our stakeholders. The ultimate goal is to build a security infrastructure that is not just reactive, but resilient, capable of withstanding the challenges of today and tomorrow.

Organization

Prompt	Answer
business needs	**Business Needs:** A. **Enhance Security Awareness and Training:** Implementing targeted security training will reduce the likelihood of successful social engineering attacks and improve overall security hygiene among employees, which is crucial for protecting sensitive information. B. **Strengthening Access Control Management:** By refining access control policies and integrating role-based access control (RBAC), ACME will ensure that only authorized personnel have access to sensitive data, thereby minimizing insider threats and unauthorized access. C. **Implement Patch Management:** Regular updates and automated patch management will protect the organization from vulnerabilities in software and hardware, reducing the risk of cyber-attacks that could disrupt operations or result in data breaches.

Prompt	Answer
Project's methods of **scalability**.	**Scalability Methods:** D. **Modular Training Programs:** Security awareness programs will be designed in modules, allowing for easy updates and additions as new threats emerge. E. **Role-Based Access Control (RBAC):** The access control policies will be scalable to accommodate organizational growth and changes in roles and responsibilities. F. **Automated Patch Management Systems:** Implementing scalable patch management tools that can manage an increasing number of devices and software applications as the company expands.

Project Completion

Prompt	Answer
The **scope**.	**Scope of Deliverables:** A. **People Domain:** Implementation of comprehensive security awareness and training programs, including regular workshops and simulations. B. **Process Domain:** Development and deployment of robust access control policies and procedures, along with a fully documented incident response plan. C. **Technology Domain:** Deployment of an automated patch management system to ensure all software and devices are consistently updated and secure.

Assess Potential **business impacts**	**Potential Business Impacts:** Positive Impacts: A. **Reduced Risk of Breaches:** Enhanced training and awareness programs will significantly lower the likelihood of successful social engineering and physical security breaches. Employees, as the first line of defense, will be better equipped to recognize and prevent potential threats, thereby protecting ACME's critical assets. B. **Improved Regulatory Compliance:** By strengthening access control and implementing robust incident response procedures, ACME will align more closely with industry standards and regulations. This alignment not only helps in avoiding costly fines and penalties but also enhances the company's reputation as a secure and compliant organization in the eyes of customers and partners. C. **Increased Operational Efficiency:** Regular and automated software updates will reduce system vulnerabilities, leading to fewer security incidents. This proactive approach will minimize downtime and operational disruptions, resulting in smoother, more efficient business processes and improved overall productivity. Adverse Impacts: A. **Initial Disruptions During Implementation:** The introduction of new security measures, such as security awareness training, access controls, and patch management systems, may initially cause disruptions to daily operations. Employees may require time to adapt to new protocols, which could temporarily slow down productivity. B. **Increased Short-Term Costs:** The implementation of comprehensive security measures, including the potential hiring of contractors or specialized personnel, will increase short-term operational costs. These

Prompt	Answer
	expenses include not only the direct costs of the new systems but also the potential need for overtime or additional training sessions to ensure full compliance. C. **Resistance to Change:** Organizational change, especially when it involves new security protocols, may face resistance from employees who are accustomed to existing processes. This resistance can slow down the adoption of new practices, potentially leading to delays in realizing the full benefits of the security enhancements. D. **Potential Overhead in System Management:** The deployment of new security technologies and processes may introduce additional layers of complexity in system management. IT staff may need to allocate more time and resources to monitor and maintain these new systems, which could lead to increased workload and potential bottlenecks in other areas of IT support.

Detailed Implementation Approach:

- **People Domain:**
  Security Awareness and Training Programs: Regular training sessions will be conducted for all employees focusing on physical security, phishing recognition, and incident reporting.
    I. **Tools and Platforms:** KnowBe4, SANS Security Awareness.
    II. **Metrics for Success:** Reduction in successful phishing attempts, increased incident reporting rates.

- **Process Domain:**

  i) **Robust Access Control Policies:** Implement role-based access control (RBAC) to ensure employees access only necessary resources.

  a) Tools and Platforms: Active Directory, Policy Management Systems.

  b) Metrics for Success: Regular access audits showing compliance, reduced instances of unauthorized access.

  ii) **Incident Response Plan:** Develop a comprehensive plan for identifying, containing, eradicating, and recovering from security incidents.

  a) Guidelines: NIST SP 800-61.

  b) Metrics for Success: Faster incident response times, successful recovery from simulated incidents.

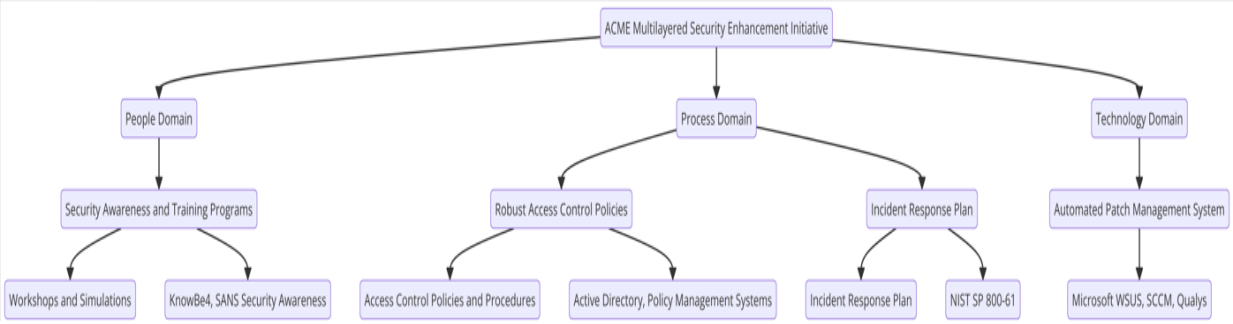
- **Technology Domain:**

  Patch Management: Implement an automated system to keep software on all devices up to date.

  I. **Tools and Platforms:** Microsoft WSUS, SCCM, Qualys.

  II. **Metrics for Success:** Regular compliance audits showing up-to-date software, reduction in incidents due to unpatched vulnerabilities.

- Project Diagram:



ll. Communication Plan Table:

Goals: The communication plan will focus on achieving the following goals:

1. **Ensure Transparency:** Provide clear and timely updates to all stakeholders to maintain transparency throughout the project lifecycle.
2. **Facilitate Collaboration:** Foster open communication among team members to encourage collaboration and quick resolution of issues.
3. **Manage Expectations:** Keep stakeholders informed about project progress, potential risks, and any necessary changes to manage their expectations effectively.
4. **Support Decision-Making:** Deliver critical information to decision-makers at the right time to support informed decision-making and project adjustments.
5. **Promote Accountability:** Ensure that all team members are aware of their responsibilities and deadlines, promoting accountability and adherence to the project timeline.

Communication	Goal	Method	Frequency	Owner	Audience
Project status report	Review project status and discuss potential issues or delays	Email	Weekly	Project manager	Project team and project sponsor

Communication	Goal	Method	Frequency	Owner	Audience
Risk Management Meetings	Discuss potential risks and mitigation strategies	Virtual Meeting	Bi-weekly	Project Manager	Project Team, Risk Management Committee
Stakeholder Briefings	Update stakeholders on project progress and address any concerns	Presentation (In-person/Virtual)	Monthly	Project Manager	Stakeholders, Executive Leadership
Task Progress Reports	Track daily progress on tasks and milestones	Project Management Software	Daily updates with a Weekly Summary	Team Leads	Project Team
Issue Escalation Reports	Report and escalate issues that need immediate attention	Email with Follow-up Meeting if Necessary	As Needed	Team Leads/Project Manager	Project Manager, Relevant Team Members

a) Phases, Milestones, and Tasks:

How will each component of your communication plan contribute to providing frequent, open, and transparent communication for phases, milestones, and tasks in the project?

The communication plan is structured to provide frequent, open, and transparent communication at each phase, milestone, and task of the project. For example:

- **Initiation Phase:** Regular updates to stakeholders during the project kick-off and initial planning meetings to set expectations.
- **Execution Phase:** Weekly project status reports and daily task progress reports to ensure all team members are aligned and aware of ongoing activities.
- **Monitoring and Controlling Phase:** Bi-weekly risk management meetings and issue escalation reports to address any challenges promptly.
- **Closing Phase:** Final stakeholder briefings to present the project outcomes and discuss any lessons learned.

Each component of the communication plan is designed to keep all relevant parties informed and engaged, ensuring that the project progresses smoothly, and any issues are addressed proactively.

b) Scope Creep Management Plan:

1. Develop a Detailed Plan to Adjust for Scope Creep

Scope creep refers to the addition of tasks, features, or deliverables that go beyond the initial project scope, which can lead to timeline delays and budget overruns if not managed properly. Based on the recent Gantt chart updates, the plan to adjust for scope creep includes:

- **Identify Additional Tasks Early:**
    - As new requirements arise, such as the document conversion function requested by stakeholders, these should be promptly added to the Gantt chart under a dedicated section or as an extension of existing tasks. For example, if a task related to "Document Conversion Implementation" is added, it should be aligned with existing milestones like "Patch Management Deployment Completed."
- **Reallocate Resources:**
    - Allocate additional resources such as contractors or existing team members to manage new tasks without affecting the progress of existing ones. For instance,

the introduction of a database administrator (DBA) specialized in document conversion can be added as a resource to oversee the new tasks.

- **Adjust Timelines:**
    - Modify the timeline in the Gantt chart to reflect the additional work required for scope creep. This may involve extending certain tasks or adding new dependencies to ensure that new tasks are completed on time without delaying the entire project.
- **Monitor and Control:**
    - Regularly monitor progress against the updated Gantt chart and ensure that any scope changes are documented, communicated, and approved by stakeholders. This involves adding checkpoints to the project schedule to reassess the impact of scope changes on the timeline and budget.

2. Justify Why This Plan Will Effectively Address Scope Creep

This plan is effective because it involves proactive identification and integration of scope changes into the existing project framework. By immediately addressing additional tasks in the Gantt chart, allocating necessary resources, and adjusting timelines, the project maintains its momentum without unexpected delays. The use of monitoring checkpoints ensures that the project stays aligned with stakeholder expectations and that any deviations are quickly rectified.

3. Assess the Potential Impact of Budget

Scope creep often leads to additional costs, particularly if added resources, like the DBA for document conversion, need to be hired or if existing resources need to work overtime. The impact on the budget includes:

- **Additional Personnel Costs:**
    - Hiring specialized contractors like a DBA can increase labor costs.
- **Extended Timeline:**
    - Adjusting the timeline might mean additional project management hours, which could lead to increased overhead.
- **Software and Tools:**
    - Implementing new software for document conversion or patch management might require purchasing additional licenses or tools.

To manage the budget impact, it is critical to reassess the project budget and either secure additional funding from stakeholders or reallocate existing funds by reprioritizing tasks.

4. Communicate the New Plan to Stakeholders

Effective communication is key to managing stakeholder expectations when scope creep occurs:

- **Formal Updates:**
    - Present the updated Gantt chart to stakeholders, highlighting where new tasks have been added and how they affect the overall timeline and budget. This should be done during scheduled stakeholder briefings.

- **Transparency in Costs:**
    - Clearly communicate any budget adjustments needed due to scope creep and justify these costs with detailed explanations of the additional value provided by the new tasks.
- **Seek Approval:**
    - Ensure that any scope changes are formally approved by stakeholders before moving forward. This prevents any misunderstandings later in the project.

- **Regular Check-Ins:**
    - Continue regular check-ins with stakeholders to update them on progress and any further adjustments needed as a result of scope creep.

References

Chapple, M., Stewart, J. M., & Gibson, D. (2021). *ISC2 CISSP Certified Information Systems Security Professional Official Study Guide* (9th ed.). Sybex.

National Institute of Standards and Technology (NIST). (2012). *Computer Security Incident Handling Guide: Special Publication 800-61 Revision 2*. https://doi.org/10.6028/NIST.SP.800-61r2

KnowBe4. (2024). *Security Awareness Training*. https://www.knowbe4.com/security-awareness-training