

## CYB 420 Project Two Communication Plan Template

### Communication Table

Complete this template by replacing the bracketed text with the relevant information in each row.

Use the first row as an example to help guide your responses. If you believe a project status report, as suggested in the example row, would be a useful inclusion in your communication plan, you may choose to incorporate one in your plan or make your own adjustments. You can also change the number of rows in this table to match your needs.

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
Kickoff Meeting	Introduce project scope, objectives, and expectations	Video Conference	Once	Project Manager	Project Team, Stakeholders
Risk Management Updates	Identify and address emerging risks	Email	Bi-weekly	Project Manager	Risk Management Team, Stakeholders
Training Progress Report	Update on security awareness training implementation	Presentation	Monthly	Training Lead	Employees, Management
Final Project Review	Evaluate project outcomes and next steps	In-person Meeting	End of Project	Project Manager	Stakeholders, Project Team

### 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?

- **Project Status Report:** Weekly updates ensure stakeholders and team members stay informed on progress, allowing for early identification of potential roadblocks. These updates help track milestone completion and adjust project priorities as needed.
- **Kickoff Meeting:** This phase establishes clear expectations and aligns all involved parties on project goals, scope, and responsibilities. It also clarifies team roles and ensures efficient task delegation.
- **Risk Management Updates:** Enables proactive identification and mitigation of cybersecurity risks, reducing disruptions. Timely communication of risks allows teams to implement necessary adjustments before they impact critical milestones.
- **Training Progress Report:** This report ensures that the implementation of security awareness training remains on track and effective. It also helps evaluate employees' engagement in training sessions and identify areas requiring additional focus.
- **Milestones & Task Coordination:** Regular milestone check-ins ensure that all tasks progress as scheduled. Teams are encouraged to report any delays or blockers that may be impacting project completion.
- **Final Project Review:** This formally assesses the project's success and any areas for future improvement. It also ensures that all security enhancements have been properly implemented and validated.

## Project Charter

### Mission Statement:

This project aims to enhance ACME Company's network security by addressing vulnerabilities in three key risk domains: people, processes, and technology. The project will implement security awareness training to mitigate human error, establish

structured security policies to streamline incident response, and deploy network segmentation to strengthen infrastructure defenses. These initiatives will improve the company's security posture, ensuring resilience against evolving threats. By proactively addressing these vulnerabilities, ACME Company will reduce the risk of cyberattacks and data breaches, ensuring business continuity and regulatory compliance. A strong security foundation will also improve stakeholder trust and help the organization stay ahead of industry security standards.

**Business Needs:**

The project will meet ACME Company's business needs by enhancing cybersecurity measures, ensuring regulatory compliance, and improving operational efficiency. Security awareness training will empower employees to recognize and mitigate threats. Formalized security policies will create a structured approach to incident response. Network segmentation will limit lateral threat movement and improve infrastructure resilience. These improvements will support long-term data integrity and protect sensitive business information from potential cyber threats. Additionally, investing in security enhancements will safeguard customer data, preserve the company's reputation, and ensure continued business growth. Meeting these security needs will also reduce downtime caused by cyber incidents, leading to greater operational efficiency and financial stability.

**Scalability:**

This project is scalable, enabling future expansion and adaptation to emerging threats. Periodic updates and ongoing security training will ensure that employees remain informed about evolving risks. We will regularly review and update security policies to reflect industry best practices. As the company grows, it can extend network segmentation strategies to ensure continued security across all operational levels. By maintaining a flexible approach, ACME Company can sustain its security posture and adapt to future

technological advancements. Additionally, as new security technologies emerge, they can be seamlessly integrated into the existing framework, ensuring long-term resilience against cyber threats. The scalability of these security measures will support the organization's growth and protect newly developed digital infrastructure.

**Potential Business Impact:**

The implementation of these security measures will reduce the risk of cyber incidents caused by human error, outdated policies, and network vulnerabilities. The organization will experience increased data protection, regulatory compliance, and improved business continuity. The enhanced security measures will also strengthen stakeholder confidence and position ACME Company as a cybersecurity-conscious enterprise. Reducing security risks will also help avoid potential financial losses from data breaches and downtime, ensuring that operations continue smoothly. Employees will feel more confident in recognizing and responding to cyber threats, leading to a more security-conscious workplace culture. Ultimately, the project will reinforce ACME Company's reputation as a trusted organization that prioritizes data security and compliance with industry regulations.

## **Scope Creep Plan**

**Adjusting for Scope Creep:**

Scope creep occurs when unexpected changes are added to a project after it has started. A document conversion function has been added to the project scope in this case. The company will contract a database administrator to install and integrate the necessary software to address this change. This adjustment requires modifying the Gantt chart to accommodate the new task while ensuring

compliance with project deadlines. The document conversion function will need to be tested before full implementation to ensure compatibility with existing systems. Additionally, we will train employees to use the new function. Since the team did not initially plan this addition, they must carefully coordinate to ensure the extra workload does not disrupt other tasks. The project team will also review any potential risks associated with this change, such as system incompatibility or additional security concerns. Communication with stakeholders will be a priority to ensure transparency and alignment with business goals. We will provide regular status updates to track progress and address any issues. By carefully managing this addition, the project can stay on track while still delivering the requested functionality.

**Justification for Scope Adjustments:**

The team added the document conversion function to enhance data integrity and ensure consistent storage of reports as PDFs. This adjustment aligns with the company's broader security and compliance objectives. Without this function, reports may be stored in multiple formats, leading to inconsistencies and potential security vulnerabilities. Hiring a database administrator ensures that the implementation is handled efficiently and with minimal disruptions. Integrating this feature now rather than later will prevent additional delays and costs in the future. This adjustment supports long-term operational efficiency by standardizing report formatting and improving accessibility. This function is incorporated based on business needs and stakeholder input, ensuring the project aligns with company goals. Additionally, including this function now reduces the need for future modifications, which could be more costly and time-consuming. The project team will ensure that the change is effectively communicated to all relevant departments to facilitate a smooth transition.

**Budget Impact:**

Adding this function will impact the budget, as hiring a database administrator will require additional funds. We will conduct a cost-benefit analysis to determine whether budget reallocations are necessary. If the cost is too high, stakeholders may need to approve additional funding to ensure the project remains feasible. The team will also explore potential savings by adjusting resource allocation elsewhere in the project. While the upfront cost may be higher, the long-term benefits of improved data security and efficiency will justify the expense. We will carefully adjust the budget to avoid unnecessary strain on existing resources. Our team will conduct a financial review to identify other areas' cost savings opportunities. The potential savings from a standardized reporting system, which reduces future maintenance efforts, will justify the additional cost. Transparent financial reporting will be provided to stakeholders to ensure transparency in decision-making.

**Communicating Scope Creep to Stakeholders:**

To ensure stakeholders are informed, a meeting will be scheduled to discuss the impact of this change. A detailed breakdown of the required adjustments will be presented, including timeline modifications and budget considerations. We will provide clear documentation explaining why this function is necessary to help stakeholders understand its importance. We will send regular progress reports to keep stakeholders updated on the progress made by the implementation. Open communication will help prevent misunderstandings and ensure continued support for the project. Addressing stakeholder concerns early will reduce the risk of pushback or delays. The team will also establish clear guidelines for handling future changes to prevent additional scope creep. Providing stakeholders with a well-documented explanation will foster trust and confidence in project execution. We will schedule regular check-ins to keep all parties aligned throughout the process.

## **Gantt Chart Update:**

The Gantt chart was updated to accommodate the addition of a new task, "Implement Document Conversion Function," introduced due to scope creep. This task was strategically placed within the Security Audits and Final Testing phase to ensure seamless integration without disrupting the project timeline. The new task starts on May 26, 2025, and ends on June 15, 2025, parallel to "Final Testing and Approval." To align with available resources, the Software Engineers Team Lead was assigned to oversee the implementation, ensuring proper system integration while maintaining security and data integrity. No other task deadlines were changed, as the document conversion function was incorporated without extending the overall project duration. A new milestone was not required since the function is part of the final security improvements before project closure. These updates ensure the project remains on track, effectively managing scope creep while meeting stakeholder expectations.