Strategic, Planning, and Policies

Raymond A. Vejar

Grand Canyon University

CYB -535: Policy Management for Security Solutions

Professor Tejiri Jessa

February 21, 2024

Explain how your organization should integrate basic elements of professional discourse, including audience analysis, the writing process, and design elements, into technical communication artifacts.

Professional Discourse:

When presenting our presentation to our board of directors, we want to highlight our professional discourse that will establish an environment that fosters learning and collaboration with them and throughout our organization. By establishing clear communication, our meetings will engage in conversations to gain insight, not just validation of our existing views from our cybersecurity department. We must challenge ourselves to consider different perspectives and acknowledge thoughtful comments and encourage more valuable contributions. Respectful engagement with those who have opposing viewpoints will foster a healthy debate, which we must remember that diversity includes diversity of thought.

Audience Analysis:

Audience analysis, involves identifying the audience and presenting a language that can be written, spoken, or visually constituted by all of our professionals starting at the top of our hierarchy. In order, to share cybersecurity findings our department must know our audience and their needs, expectations, and preferences. We understand throughout our company’s hierarchy there are different levels of technical knowledge, interest, and authority. Thus, we will be using a variety of methods to achieve this information that might include, interviews, surveys, or focus on each department to determine prior knowledge, experience, and needs.

For instance, customers, may want to know how to protect their data and privacy, while managers may want to know the impact

and recommendations, and technical experts may want to know specific details of how a discovery happened, and verify the findings.

Writing and Design Process:

Any, technical communication artifacts created, will go through a series of steps that will produce clear, concise, and effective technical communication documents.

The following steps will include:

- **Planning:** Identify the purpose, audience, and scope.
- **Research:** Information is gathered to support our writing.
- **Drafting:** The first draft of an artifact
- **Revising:** review and improve draft.
- **Editing:** Grammer, spelling, and punctuation errors are corrected.
- **Design elements:**, Use clear and concise language, visuals to illustrate our points, and consistent format throughout our artifacts. To create a visually appealing artifact color, font, and spacing will be used to organize the content making it easy to read.

Examples of technical communication artifacts might include, presentations, websites, user manuals, employee handbooks, standard operating procedures, troubleshooting guides, and any policy documentation etc…

Present your three-to-five-year operational, tactical, and strategic management plan for information security. As part of your plan, evaluate the appropriate security solutions required to design a security architecture.

Are cybersecurity team, has created a three-to-five year operational, tactical, and strategic management plan for our information security here at Society’s Banking Industry. This

information security management plan reflects our commitment to stewardship of sensitive personal information and our critical business information. Therefore, acknowledging the many threats to information security and the importance of protecting the privacy of all our constituents, fulfilling legal obligations, and safeguarding vital business information.

Strategic plan will address our long-term goals on how to provide information security that aligns our business objectives to ensure business continuity, minimize business risk, maximize return on investment, and create business opportunities in the future.

Tactical plan will address our mid-term goals that will evaluate the effectiveness and progress of our existing information security practices, policies, and the security controls implemented used to safeguard our information. Information security benchmarks will be implemented as metrics to establish a baseline security performance, track changes, and provide improvements over time. In addition, annual audits will be conducted to identify vulnerabilities and weaknesses in any security gaps.

Operational planning will address our short-term goals and every day decision making in our operations in terms of providing confidentiality, secure from unwanted authorization, integrity, accurate and free from tampering, and availability, accessible in a timely manner, and along with employee training on how to handle information.

To achieve the appropriate security solutions to provide a secure security architecture are cybersecurity department will follow these steps:

- Build an Information Security Team:
- Inventory and Manage Assets:
- Assess Risk
- Manage Risk
- Develop an Incident Management and Disaster Recovery Plan
- Inventory and Manage Third Parties

- Apply Security Controls
- Establish Security Awareness Training
- Continual Audits

Identify key organizational roles that should be actively involved in the plan's implementation:

It is imperative to identify key organizational roles that will be actively involved in our plan’s implementation. Roles are required within the organization to provide clearly defined responsibilities and an understanding of how the protection of information is to be accomplished. Their purpose is to clarify, coordinate activity, and actions necessary to disseminate security policy, standards, and implementation.

Below are the Society Banking Industry key roles and responsibilities that will be involved in our plan’s implementation:

- **Information Security Board of Directors**

These roles, are to provide oversight, and direction regarding information security and privacy company wide. They will oversee development, implementation, enforcement, and recommended guidelines, operating procedures, and technical standards.

- **Executive Management:**

These executive level roles, generally are responsible for overseeing the overall enterprise information security strategy that ensures information assets are protected. In addition, they will document and disseminate information security policies, procedures, and guidelines throughout the company. Our executive management roles will include, Chief Information Security Officer (CISO), Chief Technology Officer (CTO), and our Chief Risk Officer (CRO).

- **Information System Security Professionals:**

These roles, are responsible for the design, implementation, management, and review of the organization's security policies, standards, baseline, procedures, and guidelines. Our security professionals roles include, Information Technology Security Manager, Information Technology Risk Manager, Compliance Manger, and Information Technology Security Analyst.

- **Data Owners:**

These roles, are accountable for specific data that is transmitted, used, and stored on a system or systems within a department. They will provide direct authority and control over the management and use of specific information. Data owners will include, department managers, supervisors, and designated employee staff.

- **Data Users:**

These roles, are responsible for adhering to policies, guidelines, and procedures pertaining to the protection of our information assets. Report actual or suspected security, policy violations, and recognizing breaches to our information technology during the course of our day-to-day operations. Data Users will be any employee, contractor, or third party that is authorized to access our information systems or information assets.

Evaluate the components of IT governance and cybersecurity frameworks to ensure regulatory compliance within organizations:

The components of IT governance and cybersecurity frameworks have been designed and created to assist organizations to ensure regulatory compliance. Regulatory compliance and security intermingle with each other, and frameworks provide organizations with a structured approach on risk management, decision-making, and managing information technology resources. In addition, frameworks offer guidelines, controls, and

processes, that address security challenges to protect information, infrastructure, and information systems. Security compliance controls, are selected and implemented as safeguards, or countermeasures used to avoid, detect, counteract or minimize security; therefore, keeping organizations in compliance to regulations and industry standards. The idea, is to combine elements of several frameworks to leverage their strengths of each, to an organizations specific needs and objectives based on their services. Frameworks, should be used to guide and align their information technology goals with their business's goals.

Therefore, understanding the scope of each framework is imperative, For instance, our financial institution will have to abide by multiple frameworks to stay in compliance.

Below are a few example of frameworks and regulations that pertain to the financial industry:

- The European General Data Protection Regulation (EU-GDPR)
- Kingdom General Data Protection Regulation (UK-GDPR)
- NIST Cybersecurity Framework (CSF)
- The Sarbanes-Oxley (SOX) act of 2002
- Payment Card Industry (PCI) Data Security Standards (DSS)
- The Bank Secrecy Act (BSA)
- The Gramm–Leach–Bliley Act (GLBA)

Examine how you can identify, formulate, and solve computing problems by communicating effectively with a range of audiences through professional oral and written skills:

Communicating effectively with a range of audiences through professional oral and written communication is imperative, when it comes to identifying, formulating, and solving computer problems. Written and verbal communication is the ability to articulate thoughts and express ideas effectively to inform,

instruct, and listen for meaning and understanding. It is imperative, to use both oral and written communication skills, so our company can convey ideas comprehensively, and adapt to diverse communication scenarios. In particular, written communication skills are crucial for crafting professional documents that will include, emails, cover letters, text, and reports, while professional oral communication encompasses the ability to express thoughts, opinions, and information through spoken words. Our goal, at Society Banking industry, is to empower employees to navigate challenges, convey their ideas persuasively, and achieve their goals with confidence through effective communication whether oral or written.

Below are some steps that our company follows to communicate effectively with different audiences and levels of our organization to solve computing problems.

- Know our Audience:
- Choose the right channel
- Adapt your style
- Listen actively
- Follow up

Using the company from Topic 1, explain how the three-to-five-year InfoSec plan aligns with and supports the organization's mission and vision statements. Note: These goals are usually created by the CEO of the company and then translated into more specific goals for the levels below:

Our, three-to-five-year information security management plan, reflects Society’s Banking Industry commitment to stewardship of our sensitive personal information and critical business information. In acknowledgement of the many threats to information security and the importance of protecting the privacy of our constituents, safeguarding vital business information, and fulfilling legal and compliance obligations. All employees share

responsibility for the security of our information and resources in their respective roles, which starts at the top of our employee hierarchy from our CEO, Managing Directors, Vice Presidents, C-Level executives, and all employees. Bench marks have been implemented in our security plan to measure our organization’s baseline security performance, make improvements to our security program over time, and comparison of its performance against industry peers, competitors, and different business units. In addition, with our bench marks, continuous audits will take place annually, or with any changes to our environment.

Society’s Banking Industry goals and vision is to satisfy our customers' financial needs and help them succeed financially. This unites us around a simple premise: Customers can be better served when they have a relationship with a trusted provider that knows them well, provides reliable guidance, and can serve their full range of financial needs.

Our mission is to deliver stable, secure, scalable, and innovative services at speeds that delight and satisfy our customers, and unleash the skills potential of our employees. We're proactively enhancing our security to help protect your accounts and information, which enables our customers to have 24 hours a day, 7 days a week banking access through- in branch, online, ATMs, and other channels.

Describe the differences between policies, standards, guidelines, and procedures:

Policies:

Identifies the rules and procedures for all individuals accessing and using our information technology assets and resources.

Standards:

Series of documented processes that define how to implement, manage, and monitor various security controls. Standards, are seen as more strictly enforceable.

Guidelines:

Address safeguarding the confidentiality and security of customer information and ensuring the proper disposal of customer information. They are directed toward preventing or responding to foreseeable threats to, or unauthorized access to use of, information.

Procedures:

A set sequence of necessary activities that performs a specific security task or function. Procedures are normally designed as a series of steps to be followed as a consistent and repetitive approach or cycle to accomplish an end result.

Evaluate the appropriateness of cybersecurity frameworks for developing a cybersecurity program to align with business needs:

The appropriateness of cybersecurity frameworks for developing a cyber security program to align with business needs depends on several factors, including size of an organization, your industry, and specific needs. A Cybersecurity framework is a set of guidelines, best practices, and standards designed to help organizations protect their information systems and data from cyber threats. Organizations should align cybersecurity with their business goals, and create a security strategy that is both effective and business-driven. This approach helps prioritize resources, reduce business risks, and demonstrate the value of security investments to senior management and stakeholders. By selecting and implementing the right framework for an organization, will improve your security posture, reduce risk, and ensure compliance with industry-specific regulations.

https://youtu.be/JFpJJaj-lVY