COMPANY X

TO: All General Managers at COMPANY X.

FROM: Utsav Patel, Cybersecurity Process Consultant

SUBJECT: Securing Business Strategies and Operations using Information Security Standards

DATE: October 20, 2025

Hello General Managers,

I am Utsav Patel, a Cybersecurity Process Consultant. I am tasked with researching and identifying the necessities of integrating new cybersecurity techniques into operations. After doing extensive research and reviewing documents provided by the National Institute of Standards and Technology known as NIST, I was able to identify multiple areas in different documents to function as recommendations from me to help create a better information security based approach to the business strategies and operations.

After reviewing the variety of NIST documents, I found three NIST Documents: NIST SP 800-12 Rev. 1, NIST SP 800-100, NIST SP 800-35 were best sources to build the foundation of my recommendation. Below is an attached informal report which provides brief summaries on each of the three NIST documents used for developing my recommendations.

If the following informal report is reviewed and meets everyone's satisfaction, I would love to setup some time on everyone calendar to discuss next steps into the matter. My hope is with the research information and documents compiled during my research; we can begin the implementation of the recommendations into a solution which all involved personnel feel satisfactory into moving forward on. Please let me know if there are any questions and concerns about the information attached below or about the overall recommendation of the approach.

I look forward to hearing from everyone and working towards further securing COMPANY X.

Sincerely,

Utsav Patel

Cybersecurity Process Consultant

utsav.patel@aegissecuritypartners.com

Foundational Documents

NIST SP 800-12 Revision 1, “An Introduction to Information Security,” is a publication created on the guiding those newly entering the information security or unfamiliar with the NIST guidelines and frameworks. The document defines information security as the protection of information from unauthorized access to data which can be modified, destroyed, or disclosed in order to maintain the validity of the data. Information security is defined in eight core principles as each are important in creating a solid foundation for information security. These principles basically revolve around supporting the business operations and strategy while having a logical structure set for management. Plus, the security should be structured in proportion to any risks attached to the system. Also, all roles and responsibilities should be defined while each system owner has responsibilities that are not limited to the organization but go beyond the organization. Finally, information security needs a complex and integrated mindset, hence why should always be assessed and monitored to ensure best level of foundation while at the same time constraining itself to the guidelines set by society and traditional factors. The document also dives into in-depth analysis of each personnel’s role and their responsibilities. The document further explains other concepts in information security like threats and vulnerabilities linked to information, policies both required and optional to help create a great framework, and controls needed to be placed to ensure the information is only available to those defined to access it in the first place. The publication acts like a one shop stop where information security is broken down into different concepts to help create a solid foundation in information security despite one’s level of understanding.

The next document for reference is NIST SP 800-35, “Guide to Information Technology Security Services,” is a publication that focuses on the security services and it lifecycle revolving around the services. The document has been created as responsibility of NIST to help manage information security. The publication begins with describing the roles and responsibilities given to each personnel in an organization hierarchy in implementing the security services. The reference establishes the three IT services categories which are management, operational, technical. Management IT services revolves around techniques and problems dealing in the management of computer services in an organization. Operation IT services is based on physical aspects as it relates to operations executed by a person or group of people. Technical IT services is the digital aspects where the execution of a computer system on a certain control or program depends on the dependence of the service. Further breakdowns of services in each category are given in-depth in the document. Next item discussed in the publication is the IT security service lifecycle. The phrases of the lifecycle are respectively: Initiation, Assessment, Solution, Implementation, Operations, Closeout. These six phrases are considered core steps in ensuring a great process of implementing any security service. The document unlike the other two gives an in-depth analysis on one topic, being security services without giving broader definitions.

The next publication is NIST SP 800-100, “Information Security Handbook: A Guide for Managers,” helps managers establish a great foundation for information security program. The publication begins by establishing the importance of information security governance. Managers should create a straightforward and complex governance structure where governing body needs to ensure solid governance over their subjects. Governance is split between two categories, one being a centralized governance structure where one entity is the main

personnel handling that structure while decentralized governance structure where there are policies and procedures set to function as guidelines to self-govern the structure. Information security revolves around a system development lifecycle which are acquisition/development, implementation/assessment, operations/maintenance, sunset(disposal), and initiation. Each principle helps create the foundational structure of a system. The next couple concepts discussed in the publication revolving around reducing the likelihood of concerns. One of the concepts is having personnel go through security awareness and training to have them understand the importance of information security. Another concept is creating proper security planning, risk management, and incident response as they are the core essential elements in ensuring that if the security is compromised then there is some containment processes in place to reduce the effect of the breach. The publication is a great handbook to help managers or management team create a solid foundation in implementing information security.

References

Bowen, P., Hash, J., & Wilson, M. (2006). *Information Security Handbook: A Guide for Managers* (NIST SP 800-100). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-100

Grance, T., Hash, J., Stevens, M., O'Neal, K., & Bartol, N. (2003). *Guide to information technology security services* (NIST SP 800-35; 0 ed., p. NIST SP 800-35). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-35

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). *An introduction to information security* (NIST SP 800-12r1; p. NIST SP 800-12r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-12r1

COMPANY X

TO: CISO of COMPANY X

FROM: Utsav Patel, Cybersecurity Process Consultant, COMPANY X

SUBJECT: Securing Business Strategies and Operations using Information Security Standards

DATE: October 20, 2025

Hello CISO of COMPANY X,

I am Utsav Patel, a Cybersecurity Process Consultant. I am tasked with researching and identifying the necessities of integrating new cybersecurity techniques into operations. After doing extensive research and reviewing documents provided by the National Institute of Standards and Technology known as NIST, I was able to identify multiple areas in different documents to function as recommendations from me to help create a better information security based approach to the business strategies and operations.

Below is an attached formal report which provides an explanation of the current goals set and the expansion of providing more secure structures in the information security section. Using the three NIST documents, I will provide a formal report of analysis on how to implement these concepts into the operations of the company. The report will use examples from the publications to help give one to one scaling for information security.

If the following formal report is reviewed and meets your satisfaction, I would love to set up some time on everyone calendar to discuss next steps into the matter. My hope is with the implementation of information security structure to create a strong foundation for data protection. Please let me know if there are any questions and concerns about the information attached below or about the overall recommendation of the approach

I look forward to hearing from you and working towards further securing COMPANY X.

Sincerely,

Utsav Patel

Cybersecurity Process Consultant

utsav.patel@aegissecuritypartners.com

Securing Business Strategies and Operations using Information Security Standards

REPORT OF FINDINGS

Utsav Patel

LAST REVISED OCTOBER 2025

EXECUTIVE SUMMARY

COMPANY X is planning to perform research and development to bring new products to market. While preparing to conduct research, the organization has been gathering knowledge towards understanding the different categories of security and governance. Hence, the company has requested to conduct research on identifying and investigating the concepts of information security. While conducting investigations and research into gaining in-depth knowledge of information security, several publications created by NIST were found that will be used as sources to give an analysis on the topic. These documents give the ability to not only create new unique products but also update any current products which require more current information security material. Hence why these publications should be used as foundation to help with researching and development not only new products but also restructuring any older products that can help the company gain more foundationally products to help their clients follow current security trends. For more details and specific concerns behind the need to use these documents as foundations will be discussed in the analysis section of the report.

INTRODUCTION

COMPANY X, a Georgia-based firm specializing in Governance Risk and Compliance and Information Security consulting services, wants to refresh their current services menu by researching and developing new products to the market. While researching the current trends, they want to refresh their knowledge of information security to understand if any new approaches can be taken to create a better foundation of information security. As the data compiled about the company's recent performance with new projections from forecasting higher revenues ranges in the coming years, the organization feels greatly confident about securing the investment request for new funding to help facilitate the growth of new products in the current trends. Research and analyzation is being conducted in anticipation of securing the investment request. This research will not only bring opportunities to increase the company's performance with new product offerings but also help the company update their own foundation in information security.

ANALYSIS

Nieles et al. (2017) in NIST SP 800-12 revision 1 introduces the eight core principles on information security out which two concepts "information security requires a comprehensive and integrated approach" and "information security is constrained by societal and cultural factors" (p. 7). If a company ensures they have an approach with entails many areas of information security, they are able to ensure they are able to create both new products while keeping current products updated to make sure, they are able to be used in the future. Meanwhile the cultural and societal factors are critical to ensure a company products are used since if they do not approach current trends, those products might slowly become legacies instead of being foundation for future products. The addition of social media has brought new requirements for information security in an organization where products might revolve around limiting or creating a platform for

social media (Nieles et al., 2017, p. 29). Ensure to keep definition for each personnels role and responsibilities so there is no confusion to properly maintain information security.

In publication NIST SP 800-35, Grance et al. (2003) gives an in-depth analysis of services which can be used as templates to create different products. This document is a great resource to use for the research and development of new products for the company. The services can help build the products while made reaching those estimated revenues being projected to surpass them maybe even. The services are mainly revolving around government-based projects which can be great opening to explore new areas to build a foundation in. Also, the services are divided into three different categories of management, operational, and technical (Grance et al., 2003). Management services can provide the firm with the ability to help expand the need to organize a proper structure to follow access to information, Operational products can target the controls executed by people hence if they provide personnel with proper training to implement better controls. Finally, technical services will give the company the tools to help create system programs which help keep the functions running on an efficient level.

Bowen et al. (2006) in the NIST SP 800-100 publication is a manager guide to ensuring proper information security guidelines. This publication can provide a great source for managers to be able to keep both current and new products dependable. One of the tools mentioned in the document is having employees go through training and awareness. Since the new products are being thought about being created, those new products will require some veteran and new employees to go through training to oversee the products as they will be first generation to offer them to the clients (Bowen et al., 2006, p.28). Since the new products will add to the company, the document also discuss the area of contingency planning. Hence development of new products will also mean the development of new sections in contingency planning.

CONCLUSION

All the content discussed in the previous section is a great starting point to create a newer foundation revolving around information security. The new resources in the form of the NIST documents will provide a great way to research new concepts which further develop newer products. The newer products will not only provide the company with the ability to achieve those future revenues but provide a fresh new services menu to provide for their clients. One of the documents which provides an in depth analysis of services can function as a great research tool to help explore those newer products. Identifying the newer ideas of products may also provide a higher view of maybe updating current products or even legacy products which have not been used as much like before. The company will also attract newer business opportunities as new clients were not once able to be provided for might be approached with the newer varieties of services. Overall, the firm will gain not only opportunities but increase efficiency in business operations and strategies.

REFERENCES

Bowen, P., Hash, J., & Wilson, M. (2006). *Information Security Handbook: A Guide for Managers* (NIST SP 800-100). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-100

Grance, T., Hash, J., Stevens, M., O'Neal, K., & Bartol, N. (2003). *Guide to information technology security services* (NIST SP 800-35; 0 ed., p. NIST SP 800-35). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-35

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). *An introduction to information security* (NIST SP 800-12r1; p. NIST SP 800-12r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-12r1