

IAS466 – Risk Analyst Capstone – OCTAVE Final project – Swisher manufacturing

Daniel Joseph Duncan



April 12, 2023

Pennsylvania College of technology

1 College Ave., Williamsport, PA, 17701

Contents

[Executive Summary 5](#_Toc132236343)

[**Process 1** 7](#_Toc132236344)

[A1.1 | Identify Senior Management Assets and Relative Priorities 7](#_Toc132236345)

[A1.2 | Identify Senior Management Areas of Concern 8](#_Toc132236346)

[A1.3 | Identify Security Requirements for Most Important Senior Management Assets 10](#_Toc132236347)

[A1.4a | Identify Senior Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities 11](#_Toc132236348)

[A1.4b | Identify Senior Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities 15](#_Toc132236349)

[A1.4c | Identify Senior Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities 20](#_Toc132236350)

[A1.5 | Select or Confirm Operational Areas to Evaluate 24](#_Toc132236351)

[**Process 2** 24](#_Toc132236352)

[A2.1 | Identify Operational Area Management Assets and Relative Priorities 24](#_Toc132236353)

[A2.2 | Identify Operational Area Management Areas of Concern 26](#_Toc132236354)

[A2.3 | Identify Security Requirements for Most Important Operational Area Management Assets 27](#_Toc132236355)

[A2.4a | Capture Operational Area Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities 28](#_Toc132236356)

[A2.4b | Capture Operational Area Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities 31](#_Toc132236357)

[A2.4c | Capture Operational Area Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities 35](#_Toc132236358)

[A2.4d | Capture Operational Area Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities 38](#_Toc132236359)

[A2.4e | Capture Operational Area Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities 42](#_Toc132236360)

[A2.5 | Select and Confirm Staff to Include 45](#_Toc132236361)

[**Process 3** 45](#_Toc132236362)

[A3.1 | Identify Staff Assets and Relative Priorities 45](#_Toc132236363)

[A3.2 | Identify Staff Areas of Concern 47](#_Toc132236364)

[A3.3 | Identify Security Requirements for Most Important Staff Assets 48](#_Toc132236365)

[A3.4a | Capture Staff Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities 49](#_Toc132236366)

[A3.4b | Capture Staff of Current Protection Strategy Practices and Organizational Vulnerabilities 51](#_Toc132236367)

[A3.4c | Capture Staff Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities 54](#_Toc132236368)

[A3.4d | Capture Staff Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities 57](#_Toc132236369)

[A3.4e | Capture Staff Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities 60](#_Toc132236370)

[A3.5 | Communicate Results from Process 1 and 2 and Summary 63](#_Toc132236371)

[Process 4 63](#_Toc132236372)

[A4.1 | Identify Staff Assets and Relative Priorities 63](#_Toc132236373)

[A4.2a | Refine Security Requirements for Critical Assets 68](#_Toc132236374)

[A4.2b | Refine Security Requirements for Critical Assets 69](#_Toc132236375)

[A4.2c | Refine Security Requirements for Critical Assets 70](#_Toc132236376)

[A4.2e | Refine Security Requirements for Critical Assets 72](#_Toc132236377)

[A4.2f | Refine Security Requirements for Critical Assets 73](#_Toc132236378)

[A4.3a | Identify Threats to Critical Assets 74](#_Toc132236379)

[A4.3a.1 | Identify Threats to Critical Assets Human Actors Using Network Access Threat Tree 76](#_Toc132236380)

[A4.3a.2 | Identify Threats to Critical Assets Human Actors Using Physical Access Threat Tree 77](#_Toc132236381)

[A4.3a.3 | Identify Threats to Critical Assets System Problems Threat Tree 78](#_Toc132236382)

[A4.3a.4 | Identify Threats to Critical Assets Other Problems Threat Tree 79](#_Toc132236383)

[A4.3b | Identify Threats to Critical Assets 80](#_Toc132236384)

[A4.3b.1 | Identify Threats to Critical Assets Human Actors Using Network Access Threat Tree 81](#_Toc132236385)

[A4.3b.2 | Identify Threats to Critical Assets Human Actors Using Physical Access Threat Tree 83](#_Toc132236386)

[A4.3b.3 | Identify Threats to Critical Assets System Problems Threat Tree 84](#_Toc132236387)

[A4.3b.4 | Identify Threats to Critical Assets Other Problems Threat Tree 85](#_Toc132236388)

[A4.3c | Identify Threats to Critical Assets 86](#_Toc132236389)

[A4.3c.1 | Identify Threats to Critical Assets Human Actors Using Network Access Threat Tree 87](#_Toc132236390)

[A4.3c.2 | Identify Threats to Critical Assets Human Actors Using Physical Access Threat Tree 88](#_Toc132236391)

[A4.3c.3 | Identify Threats to Critical Assets System Problems Threat Tree 90](#_Toc132236392)

[A4.3c.4 | Identify Threats to Critical Assets Other Problems Threat Tree 91](#_Toc132236393)

[A4.3d | Identify Threats to Critical Assets 92](#_Toc132236394)

[A4.3d.1 | Identify Threats to Critical Assets Human Actors Using Network Access Threat Tree 93](#_Toc132236395)

[A4.3d.2 | Identify Threats to Critical Assets Human Actors Using Physical Access Threat Tree 94](#_Toc132236396)

[A4.3d.3 | Identify Threats to Critical Assets System Problems Threat Tree 95](#_Toc132236397)

[A4.3d.4 | Identify Threats to Critical Assets Other Problems Threat Tree 96](#_Toc132236398)

[A4.3e | Identify Threats to Critical Assets 97](#_Toc132236399)

[A4.3e.1 | Identify Threats to Critical Assets Human Actors Using Network Access Threat Tree 99](#_Toc132236400)

[A4.3e.2 | Identify Threats to Critical Assets Human Actors Using Physical Access Threat Tree 100](#_Toc132236401)

[A4.3e.3 | Identify Threats to Critical Assets System Problems Threat Tree 101](#_Toc132236402)

[A4.3e.4 | Identify Threats to Critical Assets Other Problems Threat Tree 102](#_Toc132236403)

[Process 5 104](#_Toc132236404)

[A5.1a | Identify Key Classes of Components 104](#_Toc132236405)

[A5.1b | Identify Key Classes of Components 105](#_Toc132236406)

[A5.1c | Identify Key Classes of Components 107](#_Toc132236407)

[A5.1d | Identify Key Classes of Components 109](#_Toc132236408)

[A5.1e | Identify Key Classes of Components 110](#_Toc132236409)

[A5.1f | Identify Key Classes of Components 112](#_Toc132236410)

[A5.2 | Identify Infrastructure Components to Examine 115](#_Toc132236411)

[Process 6 122](#_Toc132236412)

[A6.1 | Review Technology Vulnerabilities and Summarize Results 122](#_Toc132236413)

[A6.2 | Vulnerability Evaluation Summary 126](#_Toc132236414)

[A6.3 | Actions and Recommendations for Addressing Technology Vulnerabilities 127](#_Toc132236415)

[Process 7 128](#_Toc132236416)

[A7.1 | Identify the Impact of Threats to Critical Assets 128](#_Toc132236417)

[A7.2 | Create Risk Evaluation Criteria 133](#_Toc132236418)

[Process 8 136](#_Toc132236419)

[A8.1.SP1 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 136](#_Toc132236420)

[A8.1.SP2 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 137](#_Toc132236421)

[A8.1.SP3 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 138](#_Toc132236422)

[A8.1.SP4 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 139](#_Toc132236423)

[A8.1.SP5 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 141](#_Toc132236424)

[A8.1.SP6 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 142](#_Toc132236425)

[A8.1.OP1.1 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 143](#_Toc132236426)

[A8.1.OP1.2 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 144](#_Toc132236427)

[A8.1.OP1.3 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 145](#_Toc132236428)

[A8.1.OP2.1 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 146](#_Toc132236429)

[A8.1.OP2.2 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 148](#_Toc132236430)

[A8.1.OP2.3 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 148](#_Toc132236431)

[A8.1.OP2.4 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 149](#_Toc132236432)

[A8.1.OP2.5 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 151](#_Toc132236433)

[A8.1.OP2.6 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 152](#_Toc132236434)

[A8.1.OP2.7 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information 153](#_Toc132236435)

[A8.1.OP3.1 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnera1ilities, Security Requirements, and Risk Information 154](#_Toc132236436)

[A8.1.OP3.2 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnera1ilities, Security Requirements, and Risk Information 155](#_Toc132236437)

[A8.2 | Consolidate Protection Strategy Information 156](#_Toc132236438)

[A8.3a | Create Mitigation Plans 158](#_Toc132236439)

[A8.3b | Create Mitigation Plans 161](#_Toc132236440)

[A8.3c | Create Mitigation Plans 164](#_Toc132236441)

[A8.3d | Create Mitigation Plans 167](#_Toc132236442)

[A8.3e | Create Mitigation Plans 170](#_Toc132236443)

[A8.4 | Create Action List 172](#_Toc132236444)

[Conclusion 174](#_Toc132236445)

# Executive Summary

Swisher Manufacturing has been in operation for thirty-five years and is responsible for manufacturing and delivering affordable, custom made, and high-quality cleaning and industrial equipment including equipment used in food service, janitorial services, and parts used in cleaning, cutting coolant systems, and other systems that may be used in laboratory or industrial facilities. Swisher found its success from the development and introduction of automation to its production line allowing for Swisher Manufacturing to produce industrial grade products in high-volumes and consistent with the specifications required by its clients. Swisher Manufacturing also funds and supports an internal Research and Development department to improve upon its automation systems for continued advantages over their competitors that provide at most a 30% cheaper product than any other available on the market.

With the success of Swisher Manufacturing its senior management have decided to stay proactive when implementing information technologies into its business model and turn a focus on IT security to ensure the protection of its assets and client’s assets as the quantity and quality of information Swisher becomes responsible for increases with its success. These concerns first became apparent when senior management raised concerns that its top management staff have not been acting with a level of assurance for the protection of its sensitive data that is expected or required for the level of impact an incident would have on the company.

Swisher Manufacturing identified several security models to help address their concerns however these models did not meet with all of the specific issues management wanted to address or were questionable in how effective they would be when considering the criticality of the assets stored and managed by Swisher have on the success of the company. Swisher is an organization that has found its success from developing automation technology to meet the unique and specific demands of their clients and in turn have decided that they needed a unique and specific security assessment and mitigation plan to meet theirs.

This OCTAVE Risk Management Framework builds onto itself using system development life cycle strategies to improve upon the risk assessments and mitigation strategies identified through its process. First, the security professionals conducting this OCTAVE will identify the assets, relative priorities, security requirements, and knowledge of current security strategies and known vulnerabilities from each department of Swisher Manufacturing. Each department identified for interview and analysis are Senior Management, Operational Area Management, Operational Staff, and IT Staff. The systems that were identified within Swisher are Administrative, Human Resources, Accounting, Lab (Research and Development), and Production. The staff included in this OCTAVE process include President and CEO, V.P. of Sales – North America, Site Manager, Plant Production Manager, Site Safety Manager, Engineering Manager, Site Accounting Manager, Site Human Resources Manager, secretary to the site manager, Inventory Planning and Purchasing Agent, Production Engineer, Production Worker, and System Administrator. Next, the OCTAVE process will begin analysis of systems of interest and their components to identify vulnerabilities and areas of risk for audit to identify the threats to Swishers critical assets. Critical infrastructure will be identified and an approach to addressing possible vulnerabilities will be detailed to being an audit for evaluation and development of necessary actions and recommendations to consider for addressing them. Additionally, OCTAVE will identify impacts of these threats to Swishers critical assets and analysts will help identify levels of impact based on Swisher’s security, financial, and operational needs. Review of surveys and threat trees will conduct a review all identified vulnerabilities and protection strategies to produce mitigation plans and action lists for Swisher to consider when managing these vulnerabilities.

# **Process 1**

## A1.1 | Identify Senior Management Assets and Relative Priorities

**Worksheets Used in this Activity:**

* Asset Worksheet (W1.1)

**Outputs of this Activity:**

* Senior Management Assets with Relative Priorities (O1.1)

***Asset Worksheet***

|  |
| --- |
| **Assets**  Senior Manager’s Statements: |
| * + 1. **What are your important issues?** * Protecting our IPs (Intellectual Property), our partner’s IPs, and our customers IPs from unauthorized access. * Protecting our proprietary hardware, software, and data from unauthorized access. * Developing, implementing, and maintain secure, and accurate storage, and backups of our proprietary design data, inventory data, and scheduling data. * Developing, implementing, and maintaining a business continuity plan and disaster recovery plan. * Protecting our clientele’s personal and financial information from unauthorized access. * Client and internal product data and pricingmust be protected from unauthorized access. * Client and internal product data and pricing must be readily available and accurate when it is distributed. * Documentation and secure backups of contracts must be protected from intentional or unintentional breaches, alteration, or deletion. * Employees should be able to access the company’s system from off-site for access to real-time pricing and contract information. |
| * + 1. **Are there any other assets *that* you are required to protect (e.g. by law or regulation)?** * Clientele, partner’s, organizational, and employee’s:   + IP,   + proprietary information,   + financial information,   + and personal information must be confidential and protected from unauthorized access, modification, or removal from organizational systems and secure storage. |
| * + 1. **What related assets are important?** * Customers conducting business with us * Competitive edge within the industry * Ability to produce cheaper products, but only at a higher volume. * Outsourcing financial processing and storage responsibilities to a servicing bank. * Highly qualified engineers and required and enforced three-year non-competition agreements, and non-disclosure agreements. * IT System is being managed by an IT Administrator, who without, the company would not have anyone capable of managing their systems. This IT System is not being managed during second or third shift as there is only one person employed to manage it. |
| * + 1. **From the assets that you have identified, which are the most important? What is your rationale for selecting these assets as important?** * Protecting the proprietary information, IP, and protected information such as financial and PII of Swisher, their partners, and their clients is essential to ensure continued business operations. This information ensures Swisher can   continue to provide the quality of service at the costs necessary to maintain business and to retain the necessary trust and assurance necessary for their clients and future clients to continue to conduct business with them.   * Documentation of contracts, financial records, and company stored data must be protected from unauthorized modification and should be readily available and current when it is needed. Costs to business can be misappropriated or loss to profit can occur due to falsified financial records resulting in incorrect statistical analysis. |

## A1.2 | Identify Senior Management Areas of Concern

**Worksheets Used in this Activity:**

* Areas of Concern Worksheet (W1.2)

**Outputs of this Activity:**

* Senior Management Areas of Concern (O1.2)

***Areas of Concern Worksheet***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *What Scenarios Threaten Your Important Assets?* | | | | |
| **Color Coding to Match Sources of Threats to Outcomes**  **Outcomes:** | | | | |
| ***Disclosure or Viewing of Sensitive Information*** | Disclosure | ***Destruction or Loss of Important Information, Hardware, or Software*** | | Destruction or Loss |
| ***Modification of Important or Sensitive Information*** | Modification | ***Interruption of Access to Important Information, Software Applications, or Services (email, Web, etc.)*** | | Interruption of Access |
| **Sources of Threats** | Color Coding to Match Sources of Threats to Outcomes and Description to Provide Understanding | | | |
| **Intellectual Property and Proprietary Information** | Disclosure | Modification | Destruction or Loss | Interruption of Access |
| * Disclosure of Swisher Intellectual Property, or Swishers’ clients’ Intellectual Property will substantially harm Swisher due to the resulting loss of competitive advantages provided by Swishers’ proprietary assets and due to the loss of client trust resulting in a guaranteed loss of their business. * Unauthorized modification of Intellectual Property or proprietary information would result in substantial loss of company time and resources to attempt to recovery or reproduce lost assets, if it is even possible to do so. * Destruction or loss of Intellectual Property or proprietary information would result in substantial loss of company time and resources to attempt to recovery or reproduce lost assets, if it is even possible to do so. * Interruption of access to Intellectual Property or proprietary information would result in substantial loss of company time and resources while recovering access is made due the resulting halts in production. | | | |
| **Confidential/Protected Data (PII, Financial Records, etc.)** | Disclosure | Modification | Destruction or Loss | Interruption of Access |
| * Disclosure or viewing of confidential/protected data such as PII, Financial Records, and Timecards may result in breach of local, state, and federal laws and regulations. * Unauthorized Modification of confidential/protected data such as PII, Financial Records, and Timecards will result in breach of local, state, and federal laws and regulations and disrupt normal business operations during recovery of integrity of these assets. * Destruction or loss of confidential/protected data such as PII, Financial Records, and Timecards may result in breach of local, state, and federal laws and regulations and disrupt normal business operations during recovery of integrity of these assets. * Interruption of access to confidential/protected data such as PII, Financial Records, and Timecards may result in breach of local, state, and federal laws and regulations and disrupt normal business operations and disrupt normal business operations during recovery of availability of these assets. | | | |
| **Documentation and Storage of Operational Data (Hardware and Software Profiles)** | Disclosure | Modification | Destruction or Loss | Interruption of Access |
| * Disclosure of Swishers’ hardware and software proprietary designs and profiles and will cause substantial harm to Swisher due to the resulting loss of competitive advantages. * Modification of hardware and software proprietary designs and profiles and will cause substantial harm to Swisher due to the resulting disruption of normal business operations during recovery of these assets. * Destruction or loss of hardware and software proprietary designs and profiles and will cause substantial harm to Swisher due to the resulting disruption of normal business operations during recovery of these assets. * Interruption of access to hardware and software proprietary designs and profiles and will cause substantial harm to Swisher due to the resulting disruption of normal business operations during recovery of these assets. | | | |

## A1.3 | Identify Security Requirements for Most Important Senior Management Assets

**Worksheets Used in this Activity:**

* Security Requirements Worksheet (W1.3)

**Outputs of this Activity:**

* Security Requirements for Senior Management Assets (O1.3)

**Security Requirements Worksheet**

|  |  |
| --- | --- |
| **Security Requirements** | |
| **Intellectual Property and Proprietary Information** | **Confidentiality:**   * This must only be accessible by authorized individuals for use only when it is needed. * This must remain confidential.   **Integrity:**   * This must only be altered by individuals with the authorizations to do so.   **Availability:**   * This must be readily available, 24/7. |
| **Confidential/Protected Data (PII, Financial Records, etc.)** | **Confidentiality:**   * This must only be accessible by authorized individuals for use only when it is needed. * This must remain confidential.   **Availability:**   * This must be readily available, 24/7.   **Integrity:**   * This must only be altered by individuals with the authorizations to do so. |
| **Documentation and Storage of Operational Data (Hardware and Software Profiles)** | **Confidentiality:**   * This must only be accessible by authorized individuals for use only when it is needed. * This must remain confidential.   **Integrity:**  This must only be altered by individuals with the authorizations to do so.  **Availability:**   * This must be readily available, 24/7. |

## A1.4a | Identify Senior Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities

**Worksheets Used in this Activity:**

* Senior Management Survey (W1.4)
* Protection Strategy Worksheet (W1.5)

**Outputs of this Activity:**

* Senior Management Results Survey (O1.4)
* Current Senior Management Protection Strategy Practices (O1.5)
* Senior Management Organizational Vulnerabilities (O1.6)

**Senior Management Survey**

Name (Optional):

Position: President and CEO

|  |  |
| --- | --- |
| **Senior Management Survey** | |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented, and conformance is periodically verified. | Yes No Don’t  Know |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | Yes No Don’t  Know |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | Yes No Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | Yes No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes No Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Yes No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes No Don’t  Know |
| The organization uniformly enforces its security policies. | Yes No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes No Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | Yes No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | Yes No Don’t  Know |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | Yes No Don’t  Know |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | Yes No Don’t  Know |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No Don’t  Know |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | Yes No Don’t  Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Yes No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes No Don’t  Know |

**Protection Strategy Worksheet**

|  |
| --- |
| **Protection Strategy** |
| * + 1. Which issues from the survey would you like to discuss more in detail? |
| * + 1. What important issues did the survey not cover? |
| * + 1. Are there specific security policies, procedures, and practices unique to certain assets? What are they? |
| * + 1. Do you think that your organization’s protection strategy is effective?  * + 1. How do you know? |

## A1.4b | Identify Senior Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities

**Worksheets Used in this Activity:**

* Senior Management Survey (W1.4)
* Protection Strategy Worksheet (W1.5)

**Outputs of this Activity:**

* Senior Management Results Survey (O1.4)
* Current Senior Management Protection Strategy Practices (O1.5)
* Senior Management Organizational Vulnerabilities (O1.6)

**Senior Management Survey**

Name (Optional):

Position: V.P. for Sales – North America

|  |  |
| --- | --- |
| **Senior Management Survey** | |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented, and conformance is periodically verified. | Yes No Don’t  Know |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | Yes No Don’t  Know |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | Yes No Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | Yes No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes No Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Yes No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes No Don’t  Know |
| The organization uniformly enforces its security policies. | Yes No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes No Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | Yes No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | Yes No Don’t  Know |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | Yes No Don’t  Know |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | Yes No Don’t  Know |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No Don’t  Know |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | Yes No Don’t  Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Yes No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes No Don’t  Know |

**Protection Strategy Worksheet**

|  |
| --- |
| **Protection Strategy** |
| * + 1. Which issues from the survey would you like to discuss more in detail? |
| * + 1. What important issues did the survey not cover? |
| * + 1. Are there specific security policies, procedures, and practices unique to certain assets? What are they? |
| * + 1. Do you think that your organization’s protection strategy is effective?  * + 1. How do you know? |

## A1.4c | Identify Senior Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities

**Worksheets Used in this Activity:**

* Senior Management Survey (W1.4)
* Protection Strategy Worksheet (W1.5)

**Outputs of this Activity:**

* Senior Management Results Survey (O1.4)
* Current Senior Management Protection Strategy Practices (O1.5)
* Senior Management Organizational Vulnerabilities (O1.6)

**Senior Management Survey**

Name (Optional):

Position: Site Manager

|  |  |
| --- | --- |
| **Senior Management Survey** | |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented, and conformance is periodically verified. | Yes No Don’t  Know |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | Yes No Don’t  Know |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | Yes No Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | Yes No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes No Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Yes No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes No Don’t  Know |
| The organization uniformly enforces its security policies. | Yes No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes No Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | Yes No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | Yes No Don’t  Know |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | Yes No Don’t  Know |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | Yes No Don’t  Know |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No Don’t  Know |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | Yes No Don’t  Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Yes No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes No Don’t  Know |

**Protection Strategy Worksheet**

|  |
| --- |
| **Protection Strategy** |
| * + 1. Which issues from the survey would you like to discuss more in detail? |
| * + 1. What important issues did the survey not cover? |
| * + 1. Are there specific security policies, procedures, and practices unique to certain assets? What are they? |
| * + 1. Do you think that your organization’s protection strategy is effective?  * + 1. How do you know? |

## A1.5 | Select or Confirm Operational Areas to Evaluate

**Worksheets Used in this Activity:**

**Outputs of this Activity:**

* Operational Areas to Evaluate (O1.7)

# **Process 2**

## A2.1 | Identify Operational Area Management Assets and Relative Priorities

***Asset Worksheet***

|  |
| --- |
| **Assets**  Operational Area Management Statements: |
| * + 1. **What are your important issues?** * Monitoring systems need to be implemented that detect and alert employees when unauthorized physical access to the facility occur for reduced risk of organizational liability by reducing the risk of an incident involving injury or death. * Physical access controls need to be implemented to prevent unauthorized access to labs containing openly displayed IP and proprietary data. Desk check policies should also be implemented to protect this information is publicly accessible spaces. * Difficulties with implementing backing up files within an appropriate frequency due to processes that run for long periods of time and cannot be interrupted. * Financial records must be confidential, unaltered, and readily available to authorized users. * Order processing can be incomplete when receipts aren’t processed by warehouse workers to show a product has been placed into inventory. The billing cycle is monthly so if a product’s data isn’t updated in the system it may take up to a month to bill a client for it. * Accounts payable cannot be updated and payments cannot be made timely if orders received are not processed when they are received. * Important software has been in use for 20+ years, while there has been no issues in that time, if this software were to fail to work or generate false information there can be serious issues to production and business. * Inventory and vendor contact information is stored locally on one persons’ hard drive due to concerns with network security. * A lot of time is being wasted on playing “on-line casinos” during downtimes in the process schedules. * Only engineers have access to the terminals that monitor the production control systems, there is no way for non-engineers to monitor production as its running. * Bandwidth being overworked from non-work-related use. * Employee non-work-related internet usage can result in malware on the network/system. * Employees’ using each other badges so monitoring of location and behavior is ineffective. * Critical systems not isolated from the network, could result in substantial damages to IP and proprietary property if a breach were to occur. (Lab) |
| * + 1. **Are there any other assets *that* you are required to protect (e.g. by law or regulation)?** * Monitoring systems that detect and alert employees when exposure to toxic air-borne materials becomes hazardous cannot fail. * Employee timecards and payroll records must be kept confidential and unaltered. |
| * + 1. **What related assets are important?** |
| * + 1. **From the assets that you have identified, which are the most important? What is your rationale for selecting these assets as important?** * Physical access controls need to be implemented to prevent unauthorized access to labs containing openly displayed IP and proprietary data. Desk check policies should also be implemented to protect information that is in publicly accessible spaces. * Order processing can be incomplete when receipts aren’t processed by warehouse workers to show a product has been placed into inventory. The billing cycle is monthly so if a product’s data isn’t updated in the system it may take up to a month to bill a client for it or ordering products can be delayed when they are needed to finish production. * Employee non-work-related internet usage can result in malware on the network/system. While there are security mechanisms in place to manage incidents of malicious activity on the network, there is an unnecessary risk being added to malware being allowed onto the network by unmanaged internet use. |

## A2.2 | Identify Operational Area Management Areas of Concern

***Areas of Concern Worksheet***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *What Scenarios Threaten Your Important Assets?* | | | | |
| **Color Coding to Match Sources of Threats to Outcomes**  **Outcomes:** | | | | |
| ***Disclosure or Viewing of Sensitive Information*** | Disclosure | ***Destruction or Loss of Important Information, Hardware, or Software*** | | Destruction or Loss |
| ***Modification of Important or Sensitive Information*** | Modification | ***Interruption of Access to Important Information, Software Applications, or Services (email, Web, etc.)*** | | Interruption of Access |
| **Sources of Threats** | Color Coding to Match Sources of Threats to Outcomes and Description to Provide Understanding | | | |
| **Network** | Disclosure | Modification | Destruction or Loss | Interruption of Access |
| * Disclosure or viewing of confidential/protected data that is stored, communicated, or managed over the network should only be accessible by authorized users. The network should be secure from malware or other malicious actors seeks to gain unauthorized access to these assets. * Unauthorized modification of the network may lead to disclosure, destruction or loss, or interruption on the network resulting in data breaches, loss of company assets, and interruption to business operations. * Destruction or loss of the network may result in loss of stored or active operations and assets on the network and will result in interruption to business operations. * Interruption of access to the network will result in loss of business operation. | | | |
| **Documentation and Storage of Financial Data (Financial Records, Contracts, and Receipts for Order Processing)** | Disclosure | Modification | Destruction or Loss | Interruption of Access |
| * Disclosure or viewing of stored financial data may result in breach of local, state, and federal laws and regulations and disrupt normal business operations or cost the organization money while dealing with any resulting lawsuits for damages imposed by local, state, and federal data breach laws. * Modification of stored financial data may result in breach of local, state, and federal laws and regulations and disrupt normal business operations during recovery of integrity of these assets. * Destruction or loss of stored financial data may result in breach of local, state, and federal laws and regulations and disrupt normal business operations during recovery of integrity of these assets. * Interruption of access to stored financial data may result in breach of local, state, and federal laws and regulations and disrupt normal business operations during recovery of availability of these assets. | | | |

## A2.3 | Identify Security Requirements for Most Important Operational Area Management Assets

**Security Requirements Worksheet**

|  |  |
| --- | --- |
| **Security Requirements** | |
| **Network** | **Confidentiality:**   * This must only be accessible by authorized individuals for use only when it is needed.   **Availability:**   * This must be readily available, 24/7. * This must remain confidential.   **Integrity:**   * This must only be altered by individuals with the authorizations to do so. |
| **Documentation and Storage of Financial Data (Financial Records, Contracts, and Receipts for Order Processing)** | **Availability:**   * This must be readily available, 24/7.   **Confidentiality:**   * This must only be accessible by authorized individuals for use only when it is needed. * This must remain confidential.   **Integrity:**   * This must only be altered by individuals with the authorizations to do so. |

## A2.4a | Capture Operational Area Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities

**Operational Area Management Survey**

Name (Optional):

Position: Plant Production Manager

|  |  |
| --- | --- |
| **Operational Area Management Survey** | |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented, and conformance is periodically verified. | Yes No Don’t  Know |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | Yes No Don’t  Know |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | Yes No Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | Yes No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes No Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Yes No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes No Don’t  Know |
| The organization uniformly enforces its security policies. | Yes No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes No Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | Yes No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | Yes No Don’t  Know |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | Yes No Don’t  Know |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | Yes No Don’t  Know |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No Don’t  Know |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | Yes No Don’t  Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Yes No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes No Don’t  Know |

## A2.4b | Capture Operational Area Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities

**Operational Area Management Survey**

Name (Optional):

Position: Site Safety Manager

|  |  |
| --- | --- |
| **Operational Area Management Survey** | |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented, and conformance is periodically verified. | Yes No Don’t  Know |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | Yes No Don’t  Know |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | Yes No Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | Yes No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes No Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Yes No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes No Don’t  Know |
| The organization uniformly enforces its security policies. | Yes No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes No Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | Yes No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | Yes No Don’t  Know |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | Yes No Don’t  Know |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | Yes No Don’t  Know |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No Don’t  Know |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | Yes No Don’t  Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Yes No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes No Don’t  Know |

## A2.4c | Capture Operational Area Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities

**Operational Area Management Survey**

Name (Optional):

Position: Engineering Manager

|  |  |
| --- | --- |
| **Operational Area Management Survey** | |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented, and conformance is periodically verified. | Yes No Don’t  Know |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | Yes No Don’t  Know |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | Yes No Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | Yes No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes No Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Yes No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes No Don’t  Know |
| The organization uniformly enforces its security policies. | Yes No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes No Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | Yes No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | Yes No Don’t  Know |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | Yes No Don’t  Know |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | Yes No Don’t  Know |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No Don’t  Know |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | Yes No Don’t  Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Yes No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes No Don’t  Know |

## A2.4d | Capture Operational Area Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities

**Operational Area Management Survey**

Name (Optional):

Position: Site Accounting Manager

|  |  |
| --- | --- |
| **Operational Area Management Survey** | |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented, and conformance is periodically verified. | Yes No Don’t  Know |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | Yes No Don’t  Know |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | Yes No Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | Yes No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes No Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Yes No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes No Don’t  Know |
| The organization uniformly enforces its security policies. | Yes No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes No Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | Yes No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | Yes No Don’t  Know |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | Yes No Don’t  Know |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | Yes No Don’t  Know |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No Don’t  Know |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | Yes No Don’t  Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Yes No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes No Don’t  Know |

## A2.4e | Capture Operational Area Management Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities

**Operational Area Management Survey**

Name (Optional):

Position: Site Human Resources Manager

|  |  |
| --- | --- |
| **Operational Area Management Survey** | |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented, and conformance is periodically verified. | Yes No Don’t  Know |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | Yes No Don’t  Know |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | Yes No Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | Yes No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes No Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Yes No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes No Don’t  Know |
| The organization uniformly enforces its security policies. | Yes No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes No Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | Yes No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | Yes No Don’t  Know |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | Yes No Don’t  Know |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | Yes No Don’t  Know |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No Don’t  Know |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | Yes No Don’t  Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Yes No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes No Don’t  Know |

## A2.5 | Select and Confirm Staff to Include

# **Process 3**

## A3.1 | Identify Staff Assets and Relative Priorities

***Asset Worksheet***

|  |
| --- |
| **Assets**  Operational Area Management Statements: |
| * + 1. **What are your important issues?** * Monitoring systems need to be implemented that detect and alert employees when unauthorized physical access to the facility occur for reduced risk of organizational liability by reducing the risk of an incident involving injury or death. * Physical access controls need to be implemented to prevent unauthorized access to labs containing openly displayed IP and proprietary data. Desk check policies should also be implemented to protect this information is publicly accessible spaces. * Difficulties with implementing backing up files within an appropriate frequency due to processes that run for long periods of time and cannot be interrupted. * Financial records must be confidential, unaltered, and readily available to authorized users. * Order processing can be incomplete when receipts aren’t processed by warehouse workers to show a product has been placed into inventory. The billing cycle is monthly so if a product’s data isn’t updated in the system it may take up to a month to bill a client for it. * Accounts payable cannot be updated and payments cannot be made timely if orders received are not processed when they are received. * Important software has been in use for 20+ years, while there has been no issues in that time, if this software were to fail to work or generate false information there can be serious issues to production and business. * Inventory and vendor contact information is stored locally on one persons’ hard drive due to concerns with network security. * A lot of time is being wasted on playing “on-line casinos” during downtimes in the process schedules. * Only engineers have access to the terminals that monitor the production control systems, there is no way for non-engineers to monitor production as its running. * Bandwidth being overworked from non-work-related use. * Employee non-work-related internet usage can result in malware on the network/system. * Employees’ using each other badges so monitoring of location and behavior is ineffective. * Critical systems not isolated from the network, could result in substantial damages to IP and proprietary property if a breach were to occur. (Lab) |
| * + 1. **Are there any other assets *that* you are required to protect (e.g. by law or regulation)?** * Monitoring systems that detect and alert employees when exposure to toxic air-borne materials becomes hazardous cannot fail. * Employee timecards and payroll records must be kept confidential and unaltered. |
| * + 1. **What related assets are important?** |
| * + 1. **From the assets that you have identified, which are the most important? What is your rationale for selecting these assets as important?** * Physical access controls need to be implemented to prevent unauthorized access to labs containing openly displayed IP and proprietary data. Desk check policies should also be implemented to protect this information is publicly accessible spaces. * Order processing can be incomplete when receipts aren’t processed by warehouse workers to show a product has been placed into inventory. The billing cycle is monthly so if a product’s data isn’t updated in the system it may take up to a month to bill a client for it or ordering products can be delayed when they are needed to finish production. * Employee non-work-related internet usage can result in malware on the network/system. While there are security mechanisms in place to manage incidents of malicious activity on the network, there is an unnecessary risk being added to malware being allowed onto the network by unmanaged internet use. |

## A3.2 | Identify Staff Areas of Concern

***Areas of Concern Worksheet***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *What Scenarios Threaten Your Important Assets?* | | | | |
| **Color Coding to Match Sources of Threats to Outcomes**  **Outcomes:** | | | | |
| ***Disclosure or Viewing of Sensitive Information*** | Disclosure | ***Destruction or Loss of Important Information, Hardware, or Software*** | | Destruction or Loss |
| ***Modification of Important or Sensitive Information*** | Modification | ***Interruption of Access to Important Information, Software Applications, or Services (email, Web, etc.)*** | | Interruption of Access |
| **Sources of Threats** | Color Coding to Match Sources of Threats to Outcomes and Description to Provide Understanding | | | |
| **Network** | Disclosure | Modification | Destruction or Loss | Interruption of Access |
| * Disclosure or viewing of confidential/protected data that is stored, communicated, or managed over the network should only be accessible by authorized users. The network should be secure from malware or other malicious actors seeks to gain unauthorized access to these assets. * Unauthorized modification of the network may lead to disclosure, destruction or loss, or interruption on the network resulting in data breaches, loss of company assets, and interruption to business operations. * Destruction or loss of the network may result in loss of stored or active operations and assets on the network and will result in interruption to business operations. * Interruption of access to the network will result in loss of business operation. | | | |
| **Documentation and Storage of Financial Data (Financial Records, Contracts, and Receipts for Order Processing)** | Disclosure | Modification | Destruction or Loss | Interruption of Access |
| * Disclosure or viewing of stored financial data may result in breach of local, state, and federal laws and regulations and disrupt normal business operations or cost the organization money while dealing with any resulting lawsuits for damages imposed by local, state, and federal data breach laws. * Modification of stored financial data may result in breach of local, state, and federal laws and regulations and disrupt normal business operations during recovery of integrity of these assets. * Destruction or loss of stored financial data may result in breach of local, state, and federal laws and regulations and disrupt normal business operations during recovery of integrity of these assets. * Interruption of access to stored financial data may result in breach of local, state, and federal laws and regulations and disrupt normal business operations during recovery of availability of these assets. | | | |

## A3.3 | Identify Security Requirements for Most Important Staff Assets

**Security Requirements Worksheet**

|  |  |
| --- | --- |
| **Security Requirements** | |
| **Network** | **Confidentiality:**   * This must only be accessible by authorized individuals for use only when it is needed.   **Availability:**   * This must be readily available, 24/7. * This must remain confidential.   **Integrity:**   * This must only be altered by individuals with the authorizations to do so. |
| **Documentation and Storage of Financial Data (Financial Records, Contracts, and Receipts for Order Processing)** | **Availability:**   * This must be readily available, 24/7.   **Confidentiality:**   * This must only be accessible by authorized individuals for use only when it is needed. * This must remain confidential.   **Integrity:**   * This must only be altered by individuals with the authorizations to do so. |

## A3.4a | Capture Staff Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities

**Staff Survey**

Name (Optional):

Position: Secretary to the Site Manager

|  |  |
| --- | --- |
| **Staff Survey** | |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented, and conformance is periodically verified. | Yes No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes No Don’t  Know |
| The organization uniformly enforces its security policies. | Yes No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No Don’t  Know |
| **System and Network Management** | |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Yes No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes No Don’t  Know |

## A3.4b | Capture Staff of Current Protection Strategy Practices and Organizational Vulnerabilities

**Staff Survey**

Name (Optional):

Position: Inventory Planning and Purchasing Agent

|  |  |
| --- | --- |
| **Staff Survey** | |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented, and conformance is periodically verified. | Yes No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes No Don’t  Know |
| The organization uniformly enforces its security policies. | Yes No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No Don’t  Know |
| **System and Network Management** | |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Yes No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes No Don’t  Know |

## A3.4c | Capture Staff Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities

**Staff Survey**

Name (Optional):

Position: Production Engineer

|  |  |
| --- | --- |
| **Staff Survey** | |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented, and conformance is periodically verified. | Yes No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes No Don’t  Know |
| The organization uniformly enforces its security policies. | Yes No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No Don’t  Know |
| **System and Network Management** | |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Yes No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes No Don’t  Know |

## A3.4d | Capture Staff Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities

**Staff Survey**

Name (Optional):

Position: Production Worker

|  |  |
| --- | --- |
| **Staff Survey** | |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented, and conformance is periodically verified. | Yes No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes No Don’t  Know |
| The organization uniformly enforces its security policies. | Yes No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No Don’t  Know |
| **System and Network Management** | |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Yes No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes No Don’t  Know |

## A3.4e | Capture Staff Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities

**IT Staff Survey**

Name (Optional):

Position: System Administrator

|  |  |
| --- | --- |
| **IT Staff Survey** | |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented, and conformance is periodically verified. | Yes No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes No Don’t  Know |
| The organization uniformly enforces its security policies. | Yes No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No Don’t  Know |
| **System and Network Management** | |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Yes No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes No Don’t  Know |

## A3.5 | Communicate Results from Process 1 and 2 and Summary

# Process 4

## A4.1 | Identify Staff Assets and Relative Priorities

**Asset Group Worksheet**

|  |  |
| --- | --- |
| Asset Group | |
| **Senior Management** | |
| *Important Asset* | *Rationale for Selection* |
| Intellectual Property and Proprietary Information | The Confidentiality, Integrity, and Availability of this information ensures Swisher can continue to provide the quality of service at the costs necessary to maintain business and to retain the necessary trust and assurance necessary for their clients and future clients to continue to conduct business with them. |
| Confidential/Protected Data (PII, Financial Records, etc.) | The Confidentiality, Integrity, and Availability of this information ensures Swisher can continue to retain the necessary trust and assurance necessary for their clients and future clients to continue to conduct business with them. This category of information is classified as protected by local, state, and national law. Costs of business can be misappropriated or loss to profit can occur due to falsified financial records resulting in incorrect statistical analysis. |
| Documentation and Storage of Operational Data (Hardware and Software Profiles, Scheduling Data, Inventory, etc.) | The Confidentiality, Integrity, and Availability of this information ensures Swisher can continue to provide the quality of service at the costs necessary to maintain business, continue valuable research to continue to develop its operational capacities, and maintain and document business functions to ensure operational success. |
| *Other Assets*  Customers  Competitive edge within the industry  Ability to produce cheaper products at a higher volume.  Outsourcing financial processing and storage responsibilities to a servicing bank.  Highly qualified engineers and required and enforced three-year non-competition agreements, and non-disclosure agreements.  IT System is being managed by an IT Administrator, who without, the company would not have anyone capable of managing their systems. This IT System is not being managed during second or third shift as there is only one person employed to manage it. | |

|  |  |
| --- | --- |
| Asset Group | |
| **Operational Area Management** | |
| *Important Asset* | *Rationale for Selection* |
| Physical Access Controls | Unauthorized access is being granted to areas with protected information such as IP, proprietary information, login credentials, and R&D data being openly displayed. Physical Access Controls must be implemented and enforced to ensure confidentiality, integrity, and availability of protected information assets. |
| Documentation and Procedures for Accounting Systems/Order Processing | The integrity and availability of order processing data is essential for assuring accuracy of inventory and billing to ensure billing/payment is made timely and clients are not billed for non-existent products. |
| Network Access and Use | The Confidentiality of the information stored and accessible, the Integrity, and Availability of the Network is essential to ensure protected assets and data are not accessed, modified, or deleted by malicious actors, and available for continued business operations. Too much non-work-related activity can result in a slower network and introduces increased risk to malware or unauthorized access. |
| Documentation and Storage of Operational Data (Hardware and Software Profiles, Inventory Data, Schedules, Research and Development Data, etc.) | The Confidentiality, Integrity, and Availability of this information ensures Swisher can continue to provide the quality of service at the costs necessary to maintain business, continue valuable research to continue to develop its operational capacities, and maintain and document business functions to ensure operational success. |
| *Other Assets*  Air Control and Monitoring Systems  IT System is being managed by an IT Administrator, who without, the company would not have anyone capable of managing their systems. This IT System is not being managed during second or third shift as there is only one person employed to manage it.  Identification Badges  User Access Controls  Automation Controls  Production System Software | |

|  |  |
| --- | --- |
| Asset Group | |
| **Staff** | |
| *Important Asset* | *Rationale for Selection* |
| Office Systems (Applications, E-mail, calendars) | These systems manage internal and external communications between the company, its clients, and its employees. These systems also manage scheduling and notification of events and important information to its users including senior management and employees. The information being managed on these systems may include protected data, effect business function, and could result in data breach or detriment to business function due to its connection to the network and internet. |
| Inventory Documentation | The integrity and availability of the inventory management system responsible for accurate documentation of organizational inventory is essential for materials and products to be sent to the appropriate location for manufacturing and development of product. This inventory is not considered to be reliable due to issues with management of documentation due to continuous loss of time correcting mistakes from input errors. Swisher uses Just-In-Time methodology for ordering and managing inventory, so it is critical that this system is as accurate and up to date as possible. |
| Scheduling System | The scheduling system is responsible for managing orders, production, and billing. Inaccuracies within this system can cause orders and production to be late and loss of trust and business from clients. The billing cycle is monthly so inaccuracies with scheduling can result in billing clients for products that are not completed and ready to be sold or for late billing on products that have already been shipped. |
| Production Control System | The production control systems are responsible for the automation process of production. If these fail to work or inputs are not correct or accurate serious complications can result in damage to products and loss of production time. |
| *Other Assets*  Inventory  Shipping Label Printers  Physical Data and Information Documentation  Locally stored data on a single hard drive  Pricing information  Contact Names and Phone Numbers of Clients  IT Staff | |

|  |  |
| --- | --- |
| Asset Group | |
| IT Staff | |
| *Important Asset* | *Rationale for Selection* |
| Production System | The production systems are responsible for the automation process of production. If these fail to work or inputs are not correct or accurate serious complications can result in damage to products and loss of production time. Misuse of these systems can result in slower response times and can result in allowing malware onto the systems. Unauthorized access to these systems can result in loss of integrity or confidentiality of data stored or used. The availability of the production system can not be down for more than a few hours before loss of normal business operations occur. |
| Lab System | The lab system stores protected information assets including IP, proprietary information, and R&D data. The confidentiality, integrity, and availability of this system is critical for business functionality and operations. |
| Network | The network itself is a critical asset, both the administrative network and the production network exist on the network as separate logical networks.  The administrative network stores all data and applications. This includes all protected information assets that must be secured for these assets’ confidentiality, integrity, and availability essential for business functionality and operations.  The production network manages automation and IT devices in the production plant, without the continued confidentiality, integrity, and availability of this network all production will stop until it is restored. |
| Contingency Planning and Disaster Recovery Planning | There is only one IT Staff employed and managing IT systems. There is no one employed to manage second or third shift or to cover responsibilities in the event the IT Staff is not available such as when they have work external to the physical location. There is no current contingency plan for an incident involving IT systems and assets for when the IT Staff is not available. |
| *Other Assets* | |

## A4.2a | Refine Security Requirements for Critical Assets

**Security Requirements Group Worksheet**

| Security Requirements Group | |
| --- | --- |
| Asset: Intellectual Property and Proprietary Information | |
| Security Requirements  (\* indicates most important) | Security Requirements  (\* indicates most important) |
| Senior Management | Operational Area Management |
| CONFIDENTIALITY   * Disclosure: IP and Proprietary Information of Swisher and our clients must be protected from unauthorized access to ensure Swishers competitive edge and client trust and continued business.   INTEGRITY  AVAILABILITY  OTHER | CONFIDENTIALITY  AVAILABILITY  INTEGRITY  OTHER |
| Staff | IT Staff |
| CONFIDENTIALITY  INTEGRITY  AVAILABILITY  OTHER | CONFIDENTIALITY   * Disclosure: IP and Proprietary Information of Swisher and our clients must be protected from unauthorized access to ensure Swishers competitive edge and client trust and continued business.   INTEGRITY  AVAILABILITY  OTHER |

## A4.2b | Refine Security Requirements for Critical Assets

**Security Requirements Group Worksheet**

| Security Requirements Group | |
| --- | --- |
| Asset: Confidential/Protected Data (PII, Financial Records, etc.) | |
| Security Requirements  (\* indicates most important) | Security Requirements  (\* indicates most important) |
| Senior Management | Operational Area Management |
| CONFIDENTIALITY   * Disclosure: These assets are protected information by local, state, and federal law and regulations. Access is restricted to Site Human Resources Manager, theirs staff, and the Site Manager.   AVAILABILITY   * Interruption: These assets must securely stored and backed up to ensure availability and integrity.   INTEGRITY  OTHER | CONFIDENTIALITY   * Disclosure: Timecards and Payroll Cards must be confidential with access restricted to the Site Account Manager, their staff, and the Site Manager.   INTEGRITY   * Modification: Timecards and Payroll Cards must not be altered or modified without authorization from the Site Account Manager, their staff, and the Site Manager.   AVAILABILITY  OTHER |
| Staff | IT Staff |
| CONFIDENTIALITY  INTEGRITY  AVAILABILITY  OTHER | CONFIDENTIALITY  INTEGRITY  AVAILABILITY  OTHER |

## A4.2c | Refine Security Requirements for Critical Assets

**Security Requirements Group Worksheet**

| Security Requirements Group | |
| --- | --- |
| Asset: Documentation and Storage of Operational Data (Hardware and Software Profiles, Scheduling Data, Inventory, etc.) | |
| Security Requirements  (\* indicates most important) | Security Requirements  (\* indicates most important) |
| Senior Management | Operational Area Management |
| CONFIDENTIALITY   * Disclosure: The advantages Swisher has over its competitors comes from the hardware and software profiles of their production systems to develop and produce products at a 30%-40% lower price compared to other manufacturers. These profiles are the key to this success and must not be accessed by unauthorized users.   AVAILABILITY  INTEGRITY   * Modification: Incorrect/Inaccurate modification of scheduling data due to human error or intentional malicious intent.   OTHER | AVAILABILITY  INTEGRITY   * Modification: Incorrect/Inaccurate modification of scheduling data due to human error or intentional malicious intent.   CONFIDENTIALITY  OTHER |
| Staff | IT Staff |
| AVAILABILITY   * Interruption: Loss of production up-time due to loss of availability of scheduling or inventory data.   INTEGRITY   * Modification: Incorrect/Inaccurate modification of scheduling data due to human error or intentional malicious intent.   CONFIDENTIALITY  OTHER | CONFIDENTIALITY   * Disclosure: The advantages Swisher has over its competitors comes from the hardware and software profiles of their production systems to develop and produce products at a 30%-40% lower price compared to other manufacturers. These profiles are the key to this success and must not be accessed by unauthorized users.   AVAILABILITY   * Interruption: Loss of production up-time due to loss of availability of scheduling or inventory data.   INTEGRITY   * Modification: Incorrect/Inaccurate modification of scheduling data due to human error or intentional malicious intent.   OTHER |

## A4.2e | Refine Security Requirements for Critical Assets

**Security Requirements Group Worksheet**

| Security Requirements Group | |
| --- | --- |
| Asset: Documentation and Procedures for Accounting Systems/Order Processing | |
| Security Requirements  (\* indicates most important) | Security Requirements  (\* indicates most important) |
| Senior Management | Operational Area Management |
| INTEGRITY  AVAILABILITY  CONFIDENTIALITY  OTHER | INTEGRITY   * Modification: Improper modification such as incorrect data input, untimely data input, or no data input when input is required.   AVAILABILITY   * Loss or Interruption: The billing cycle is monthly so loss or interruption to these services can result in prolonged wait for payments received or paid.   CONFIDENTIALITY  OTHER |
| Staff | IT Staff |
| INTEGRITY   * Modification: Improper modification such as incorrect data input, untimely data input, or no data input when input is required.   AVAILABILITY   * Loss or Interruption: The billing cycle is monthly so loss or interruption to these services can result in prolonged wait for payments received or paid.   CONFIDENTIALITY  OTHER | INTEGRITY  AVAILABILITY  CONFIDENTIALITY  OTHER |

## A4.2f | Refine Security Requirements for Critical Assets

**Security Requirements Group Worksheet**

| Security Requirements Group | |
| --- | --- |
| Asset: Network Access and Use | |
| Security Requirements  (\* indicates most important) | Security Requirements  (\* indicates most important) |
| Senior Management | Operational Area Management |
| CONFIDENTIALITY  AVAILABILITY  INTEGRITY  OTHER | CONFIDENTIALITY   * Disclosure: Unauthorized access from persons accessing the network can result in confidential information and data being stolen or leaked.   AVAILABILITY   * Loss: Unauthorized access from persons accessing the network can result in confidential information and data being deleted or removed from the network.   INTEGRITY   * Modification: Unauthorized access from persons accessing the network can result in confidential information and data being altered to be incorrect.   OTHER |
| Staff | IT Staff |
| CONFIDENTIALITY   * Disclosure: Unauthorized access from persons accessing the network can result in confidential information and data being stolen or leaked.   AVAILABILITY   * Loss: Unauthorized access from persons accessing the network can result in confidential information and data being deleted or removed from the network.   INTEGRITY   * Modification: Unauthorized access from persons accessing the network can result in confidential information and data being altered to be incorrect.   OTHER | CONFIDENTIALITY   * Disclosure: Unauthorized access from persons accessing the network can result in confidential information and data being stolen or leaked.   AVAILABILITY   * Loss: Unauthorized access from persons accessing the network can result in confidential information and data being deleted or removed from the network.   INTEGRITY   * Modification: Unauthorized access from persons accessing the network can result in confidential information and data being altered to be incorrect.   OTHER |

## A4.3a | Identify Threats to Critical Assets

**Areas of Concern Worksheet**

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset:** Intellectual Property and Proprietary Information | |
| *Senior Management Area of Concern* | *Impact* |
| Disclosure | IP and Proprietary Information of Swisher and our clients must be protected from unauthorized access to ensure Swishers competitive edge and client trust and continued business. |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset:** | |
| *IT Staff Area of Concern* | *Impact* |
| Disclosure | IP and Proprietary Information of Swisher and our clients must be protected from unauthorized access to ensure Swishers competitive edge and client trust and continued business. |

### A4.3a.1 | Identify Threats to Critical Assets Human Actors Using Network Access Threat Tree

**Human Actors Using Network Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  | network |  |  |  |  |  |  |  |  |
| Intellectual Property and Proprietary Information |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**: Intellectual Property and Proprietary Information can be disclosed to unauthorized entities by a disgruntled worker, or malicious actor with gained access to the network or unintentionally from an employee falling for a successful social engineering attempt or from accidentally publishing this protected information via email or other form of network-based communication platform.

### A4.3a.2 | Identify Threats to Critical Assets Human Actors Using Physical Access Threat Tree

**Human Actors Using Physical Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  | physical |  |  |  |  |  |  |  |  |
| Intellectual Property and Proprietary Information |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**: Intellectual Property and Proprietary Information can be disclosed to unauthorized entities by a disgruntled worker taking physical documentation off-site, verbally disclosing this information, or allowing unauthorized access to the facility. This information is displayed on whiteboards, sticky notes on desks, etc. and can be viewed or stolen by persons with access to these locations. These locations often times have unauthorized persons in them. The environment and relaxed nature around these locations may result in employees being unaware of what is public facing and what is considered confidential which may lead to this information being disclosed without understanding the consequences.

### A4.3a.3 | Identify Threats to Critical Assets System Problems Threat Tree

**System Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  | **HIGH** |
|  |  | software defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  | **HIGH** |
|  |  | viruses |  | modification |  |  |
|  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
| Intellectual Property and Proprietary Information |  |  |  | disclosure |  |  |
|  |  | system crashes |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | hardware defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |

**Note**: Software defects may result in loss of stored data or result in vulnerabilities allowing for malware to infect the system causing disclosure of this protected information. This information is stored on a logical network separate from other, more vulnerable networks, but the risk of this network being infected is not zero.

### A4.3a.4 | Identify Threats to Critical Assets Other Problems Threat Tree

**Other Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | power supply problems |  | modification |  |  |
|  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | telecommunications |  | modification |  |  |
|  |  | problems or unavailability |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
| Intellectual Property and Proprietary Information |  |  |  | disclosure |  |  |
|  |  | third-party problems |  | modification |  |  |
|  |  | or unavailability of |  | loss, destruction |  |  |
|  |  | third-party systems |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | natural disasters |  | modification |  |  |
|  |  | (e.g., flood, fire, tornado) |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | physical configuration or |  | modification |  |  |
|  |  | arrangement of buildings, |  | loss, destruction |  |  |
|  |  | offices, or equipment |  | interruption |  |  |

**Note**:

## A4.3b | Identify Threats to Critical Assets

**Areas of Concern Worksheet**

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset:** Confidential/Protected Data (PII, Financial Records, etc.) | |
| *Senior Management Area of Concern* | *Impact* |
| Disclosure: | These assets are protected information by local, state, and federal law and regulations. Access is restricted to Site Human Resources Manager, their staff, and the Site Manager. |
| Interruption: | These assets must securely stored and backed up to ensure availability and integrity. |
| Areas of Concern Group | | |
| **Asset:** | | |
| *Operational Area Management Area of Concern* | *Impact* | |
| Disclosure: | Timecards and Payroll Cards must be confidential with access restricted to the Site Account Manager, their staff, and the Site Manager. | |
| Modification: | Timecards and Payroll Cards must not be altered or modified without authorization from the Site Account Manager, their staff, and the Site Manager. | |

### A4.3b.1 | Identify Threats to Critical Assets Human Actors Using Network Access Threat Tree

**Human Actors Using Network Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | accidental |  | modification |  | **MEDIUM** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  |  |  |  |  | interruption |  | **LOW** |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | deliberate |  | modification |  | **MEDIUM** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  |  |  |  |  | interruption |  | **LOW** |
|  |  | network |  |  |  |  |  |  |  |  |
| Confidential/Protected Data (PII, Financial Records, etc.) |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | accidental |  | modification |  | **MEDIUM** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  |  |  |  |  | interruption |  | **LOW** |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | deliberate |  | modification |  | **MEDIUM** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  |  |  |  |  | interruption |  | **LOW** |



**Note**: Confidential/Protected Data (PII, Financial Records, etc.) can be disclosed to unauthorized entities by a disgruntled worker, or malicious actor with gained access to the network or unintentionally from an employee falling for a successful social engineering attempt or from accidentally publishing this protected information via email or other form of network-based communication platform. Back up failures may result in inaccurate records, or issues with the system preventing can result in loss of access. Financial Records such as credit card information are stored off-site by a servicing bank, Swisher may still be held liable or lose client trust for any disclosure, modification, or loss of this information.

### A4.3b.2 | Identify Threats to Critical Assets Human Actors Using Physical Access Threat Tree

**Human Actors Using Physical Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | accidental |  | modification |  | **MEDIUM** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | deliberate |  | modification |  | **MEDIUM** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  | physical |  |  |  |  |  |  |  |  |
| Confidential/Protected Data (PII, Financial Records, etc.) |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**: Confidential/Protected Data (PII, Financial Records, etc.) can be disclosed to unauthorized entities by a disgruntled worker taking physical documentation off-site, or verbally disclosing this information.

### A4.3b.3 | Identify Threats to Critical Assets System Problems Threat Tree

**System Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  | **HIGH** |
|  |  | software defects |  | modification |  | **MEDIUM** |
|  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  | interruption |  | **LOW** |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  | **HIGH** |
|  |  | viruses |  | modification |  | **MEDIUM** |
|  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  | interruption |  | **LOW** |
|  |  |  |  |  |  |  |
| Confidential/Protected Data (PII, Financial Records, etc.) |  |  |  | disclosure |  |  |
|  |  | system crashes |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | **LOW** |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | hardware defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | **LOW** |

**Note**: Issues with Software Defects, System Crashes, or Hardware Defects may result in back up failures, inaccurate records, or issues with the system causing loss of access. Successful malware intrusion can result in disclosure, modification of records, loss/destruction of records, or interruption of access to records.

### A4.3b.4 | Identify Threats to Critical Assets Other Problems Threat Tree

**Other Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | power supply problems |  | modification |  |  |
|  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  | interruption |  | **LOW** |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | telecommunications |  | modification |  |  |
|  |  | problems or unavailability |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
| Confidential/Protected Data (PII, Financial Records, etc.) |  |  |  | disclosure |  | **HIGH** |
|  |  | third-party problems |  | modification |  |  |
|  |  | or unavailability of |  | loss, destruction |  |  |
|  |  | third-party systems |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | natural disasters |  | modification |  |  |
|  |  | (e.g., flood, fire, tornado) |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | physical configuration or |  | modification |  |  |
|  |  | arrangement of buildings, |  | loss, destruction |  |  |
|  |  | offices, or equipment |  | interruption |  |  |

**Note**:

## A4.3c | Identify Threats to Critical Assets

**Areas of Concern Worksheet**

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset:** Documentation and Storage of Operational Data (Hardware and Software Profiles, Scheduling Data, Inventory, etc.) | |
| *Senior Management Area of Concern* | *Impact* |
| Disclosure | The advantages Swisher has over its competitors comes from the hardware and software profiles of their production systems to develop and produce products at a 30%-40% lower price compared to other manufacturers. These profiles are the key to this success and must not be accessed by unauthorized users. |
| Modification | Incorrect/Inaccurate modification of scheduling data due to human error or intentional malicious intent. |
| Areas of Concern Group | | |
| **Asset:** | | |
| *Operational Area Management Area of Concern* | *Impact* | |
| Modification | Incorrect/Inaccurate modification of scheduling data due to human error or intentional malicious intent. | |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset:** | |
| *Staff Area of Concern* | *Impact* |
| Interruption | Loss of production up-time due to loss of availability of scheduling or inventory data. |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset:** | |
| *IT Staff Area of Concern* | *Impact* |
| Disclosure | The advantages Swisher has over its competitors comes from the hardware and software profiles of their production systems to develop and produce products at a 30%-40% lower price compared to other manufacturers. These profiles are the key to this success and must not be accessed by unauthorized users. |
| Interruption | Loss of production up-time due to loss of availability of scheduling or inventory data. |
| Modification | Incorrect/Inaccurate modification of scheduling data due to human error or intentional malicious intent. |

### A4.3c.1 | Identify Threats to Critical Assets Human Actors Using Network Access Threat Tree

**Human Actors Using Network Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | accidental |  | modification |  | **HIGH** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  |  |  |  |  | interruption |  | **MEDIUM** |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | deliberate |  | modification |  | **HIGH** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  |  |  |  |  | interruption |  | **MEDIUM** |
|  |  | network |  |  |  |  |  |  |  |  |
| Documentation and Storage of Operational Data |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**:

### A4.3c.2 | Identify Threats to Critical Assets Human Actors Using Physical Access Threat Tree

**Human Actors Using Physical Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | accidental |  | modification |  | **HIGH** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  |  |  |  |  | interruption |  | **MEDIUM** |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | deliberate |  | modification |  | **HIGH** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  |  |  |  |  | interruption |  | **MEDIUM** |
|  |  | physical |  |  |  |  |  |  |  |  |
| Documentation and Storage of Operational Data |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | accidental |  | modification |  | **HIGH** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  |  |  |  |  | interruption |  | **MEDIUM** |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | deliberate |  | modification |  | **HIGH** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  |  |  |  |  | interruption |  | **MEDIUM** |



**Note**:

### A4.3c.3 | Identify Threats to Critical Assets System Problems Threat Tree

**System Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | software defects |  | modification |  | **HIGH** |
|  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  | interruption |  | **MEDIUM** |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  | **HIGH** |
|  |  | viruses |  | modification |  | **HIGH** |
|  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  | interruption |  | **MEDIUM** |
|  |  |  |  |  |  |  |
| Documentation and Storage of Operational Data |  |  |  | disclosure |  |  |
|  |  | system crashes |  | modification |  | **HIGH** |
|  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  | interruption |  | **MEDIUM** |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | hardware defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  | interruption |  | **MEDIUM** |

**Note**:

### A4.3c.4 | Identify Threats to Critical Assets Other Problems Threat Tree

**Other Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | power supply problems |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | telecommunications |  | modification |  |  |
|  |  | problems or unavailability |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
| Documentation and Storage of Operational Data |  |  |  | disclosure |  |  |
|  |  | third-party problems |  | modification |  |  |
|  |  | or unavailability of |  | loss, destruction |  |  |
|  |  | third-party systems |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | natural disasters |  | modification |  |  |
|  |  | (e.g., flood, fire, tornado) |  | loss, destruction |  | **HIGH** |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | physical configuration or |  | modification |  |  |
|  |  | arrangement of buildings, |  | loss, destruction |  |  |
|  |  | offices, or equipment |  | interruption |  |  |

**Note**:

## A4.3d | Identify Threats to Critical Assets

**Areas of Concern Worksheet**

|  |  |
| --- | --- |
| Areas of Concern Group | |
| Asset: Documentation and Procedures for Accounting Systems/Order Processing | |
| *Operational Area Management Area of Concern* | *Impact* |
| Modification: | Improper modification such as incorrect data input, untimely data input, or no data input when input is required. |
| Loss or Interruption | The billing cycle is monthly so loss or interruption to these services can result in prolonged wait for payments received or paid. |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset:** | |
| *Staff Area of Concern* | *Impact* |
| Modification | Improper modification such as incorrect data input, untimely data input, or no data input when input is required. |
| Loss or Interruption | The billing cycle is monthly so loss or interruption to these services can result in prolonged wait for payments received or paid. |

### A4.3d.1 | Identify Threats to Critical Assets Human Actors Using Network Access Threat Tree

**Human Actors Using Network Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  | **LOW** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  | **LOW** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  | network |  |  |  |  |  |  |  |  |
| Documentation and Procedures for Accounting Systems/Order Processing |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**:

### A4.3d.2 | Identify Threats to Critical Assets Human Actors Using Physical Access Threat Tree

**Human Actors Using Physical Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  | **LOW** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  | **LOW** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  | physical |  |  |  |  |  |  |  |  |
| Documentation and Procedures for Accounting Systems/Order Processing |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**:

### A4.3d.3 | Identify Threats to Critical Assets System Problems Threat Tree

**System Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | software defects |  | modification |  | **LOW** |
|  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | viruses |  | modification |  | **LOW** |
|  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
| Documentation and Procedures for Accounting Systems/Order Processing |  |  |  | disclosure |  |  |
|  |  | system crashes |  | modification |  | **LOW** |
|  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | hardware defects |  | modification |  | **LOW** |
|  |  |  |  | loss, destruction |  | **LOW** |
|  |  |  |  | interruption |  |  |

**Note**:

### A4.3d.4 | Identify Threats to Critical Assets Other Problems Threat Tree

**Other Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | power supply problems |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | telecommunications |  | modification |  |  |
|  |  | problems or unavailability |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
| Documentation and Procedures for Accounting Systems/Order Processing |  |  |  | disclosure |  |  |
|  |  | third-party problems |  | modification |  |  |
|  |  | or unavailability of |  | loss, destruction |  |  |
|  |  | third-party systems |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | natural disasters |  | modification |  |  |
|  |  | (e.g., flood, fire, tornado) |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | physical configuration or |  | modification |  |  |
|  |  | arrangement of buildings, |  | loss, destruction |  |  |
|  |  | offices, or equipment |  | interruption |  |  |

**Note**:

## A4.3e | Identify Threats to Critical Assets

**Areas of Concern Worksheet**

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset:** Network Access and Use | |
| *Operational Area Management Area of Concern* | *Impact* |
| Disclosure | Unauthorized access from persons accessing the network can result in confidential information and data being stolen or leaked. |
| Loss | Unauthorized access from persons accessing the network can result in confidential information and data being deleted or removed from the network. |
| Modification | Unauthorized access from persons accessing the network can result in confidential information and data being altered to be incorrect. |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset:** | |
| *Staff Area of Concern* | *Impact* |
| Disclosure | Unauthorized access from persons accessing the network can result in confidential information and data being stolen or leaked. |
| Loss | Unauthorized access from persons accessing the network can result in confidential information and data being deleted or removed from the network. |
| Modification | Unauthorized access from persons accessing the network can result in confidential information and data being altered to be incorrect. |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset:** | |
| *IT Staff Area of Concern* | *Impact* |
| Disclosure | Unauthorized access from persons accessing the network can result in confidential information and data being stolen or leaked. |
| Loss | Unauthorized access from persons accessing the network can result in confidential information and data being deleted or removed from the network. |
| Modification | Unauthorized access from persons accessing the network can result in confidential information and data being altered to be incorrect. |

### A4.3e.1 | Identify Threats to Critical Assets Human Actors Using Network Access Threat Tree

**Human Actors Using Network Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | accidental |  | modification |  | **HIGH** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  |  |  |  |  | interruption |  | **LOW** |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | **HIGH** |
|  |  |  |  |  |  | deliberate |  | modification |  | **HIGH** |
|  |  |  |  |  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  |  |  |  |  | interruption |  | **LOW** |
|  |  | network |  |  |  |  |  |  |  |  |
| Network Access and Use |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**:

### A4.3e.2 | Identify Threats to Critical Assets Human Actors Using Physical Access Threat Tree

**Human Actors Using Physical Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  |  |  |  |  | interruption |  | **LOW** |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  |  |  |  |  | interruption |  | **LOW** |
|  |  | physical |  |  |  |  |  |  |  |  |
| Network Access and Use |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**:

### A4.3e.3 | Identify Threats to Critical Assets System Problems Threat Tree

**System Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | software defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | **LOW** |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  | **HIGH** |
|  |  | viruses |  | modification |  | **HIGH** |
|  |  |  |  | loss, destruction |  | **HIGH** |
|  |  |  |  | interruption |  | **LOW** |
|  |  |  |  |  |  |  |
| Network Access and Use |  |  |  | disclosure |  |  |
|  |  | system crashes |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | **LOW** |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | hardware defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | **LOW** |

**Note**:

### A4.3e.4 | Identify Threats to Critical Assets Other Problems Threat Tree

**Other Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | power supply problems |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | **LOW** |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | telecommunications |  | modification |  |  |
|  |  | problems or unavailability |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | **LOW** |
|  |  |  |  |  |  |  |
| Network Access and Use |  |  |  | disclosure |  |  |
|  |  | third-party problems |  | modification |  |  |
|  |  | or unavailability of |  | loss, destruction |  |  |
|  |  | third-party systems |  | interruption |  | **LOW** |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | natural disasters |  | modification |  |  |
|  |  | (e.g., flood, fire, tornado) |  | loss, destruction |  | **HIGH** |
|  |  |  |  | interruption |  | **LOW** |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | physical configuration or |  | modification |  |  |
|  |  | arrangement of buildings, |  | loss, destruction |  |  |
|  |  | offices, or equipment |  | interruption |  | **LOW** |

**Note**:

# Process 5

## A5.1a | Identify Key Classes of Components

|  |  |  |
| --- | --- | --- |
| **Intellectual Property and Proprietary Information** | | |
| **System(s) of Interest** | Intellectual Property and Proprietary Information are themselves the system of interest. | |
| **Key Classes of Components** | Desktops (PCs)  Laptops  Production Systems  Automated Manufacturing Systems  Production Network  Administrative Network  Lab Network  Anti-Malware Software |

|  |  |
| --- | --- |
| **Class of Component** | **Rationale for Selection** |
| * Servers | Swisher Databases are stored and managed on Swisher Data Servers. These databases store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * Networking components | Swisher Intellectual Property and other protected information assets are stored and managed on Swisher Databases.  Swisher Databases are stored and managed on Swisher Data Servers.  Swisher Servers connects to Switches which route data between Swishers Desktop (PCs), Laptops, IoT Devices, Swisher Data Servers, and the internet.  Access Points act as a wireless connection link between devices on Swishers networks to switches, to routers, and then to either the data server or the internet.  While the networks are logically separated all have access to both the internet and the data server. It is essential that these are secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * Security components | Logically isolated networks and traffic to reduce risk of malware on one infecting all of them.  Anti-Malware package installed on the networks to reduce risk of malware effecting the network and devices using it.  These security components are essential for the protection of sensitive data and essential services and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * Desktop workstations | Used by every department within Swisher. Desktops (PCs) store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * Home computers |  |
| * Laptops | Laptops store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * Storage devices | Hard drives on Desktops (PCs) and Laptops for local storage. Hard drives are not reported to but are accessible to potentially store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * Wireless components |  |
| * Others (list)   Website |  |

## A5.1b | Identify Key Classes of Components

|  |  |  |
| --- | --- | --- |
| **Confidential/Protected Data (PII, Financial Records, etc.)** | | |
| **System(s) of Interest** | Confidential/Protected Data (PII, Financial Records, etc.) are themselves the system of interest. | |
| **Key Classes of Components** | Desktops (PCs)  Accounting System  Human Resources System  Administrative Network  Anti-Malware Software |
| **Class of Component** | Rationale for Selection |
| * **Servers** | Swisher Databases are stored and managed on Swisher Data Servers. These databases store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Networking components** | Swisher Intellectual Property and other protected information assets are stored and managed on Swisher Databases.  Swisher Databases are stored and managed on Swisher Data Servers.  Swisher Servers connects to Switches which route data between Swishers Desktop (PCs), Laptops, IoT Devices, Swisher Data Servers, and the internet.  Access Points act as a wireless connection link between devices on Swishers networks to switches, to routers, and then to either the data server or the internet.  While the networks are logically separated all have access to both the internet and the data server. It is essential that these are secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Security components** | Logically isolated networks and traffic to reduce risk of malware on one infecting all of them.  Anti-Malware package installed on the networks to reduce risk of malware effecting the network and devices using it.  These security components are essential for the protection of sensitive data and essential services and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Desktop workstations** | Used by every department within Swisher. Desktops (PCs) store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Home computers** |  |
| * **Laptops** |  |
| * **Storage devices** | Hard drives on Desktops (PCs) and Laptops for local storage. Hard drives are not reported to but are accessible to potentially store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Wireless components** |  |
| * **Others (list)**   **Website** |  |

## A5.1c | Identify Key Classes of Components

|  |  |  |
| --- | --- | --- |
| **Documentation and Storage of Operational Data** | | |
| **System(s) of Interest** | Documentation and Storage of Operational Data are themselves the system of interest. | |
| **Key Classes of Components** | Desktops (PCs)  Production System  Automated Manufacturing Systems  Production Network  Administrative Network  Anti-Malware Software |
| **Class of Component** | Rationale for Selection |
| * **Servers** | Swisher Databases are stored and managed on Swisher Data Servers. These databases store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Networking components** | Swisher Intellectual Property and other protected information assets are stored and managed on Swisher Databases.  Swisher Databases are stored and managed on Swisher Data Servers.  Swisher Servers connects to Switches which route data between Swishers Desktop (PCs), Laptops, IoT Devices, Swisher Data Servers, and the internet.  Access Points act as a wireless connection link between devices on Swishers networks to switches, to routers, and then to either the data server or the internet.  While the networks are logically separated all have access to both the internet and the data server. It is essential that these are secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Security components** | Logically isolated networks and traffic to reduce risk of malware on one infecting all of them.  Anti-Malware package installed on the networks to reduce risk of malware effecting the network and devices using it.  These security components are essential for the protection of sensitive data and essential services and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Desktop workstations** | Used by every department within Swisher. Desktops (PCs) store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Home computers** |  |
| * **Laptops** |  |
| * **Storage devices** | Hard drives on Desktops (PCs) and Laptops for local storage. Hard drives are not reported to but are accessible to potentially store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Wireless components** |  |
| * **Others (list)**   **Website** |  |

## A5.1d | Identify Key Classes of Components

|  |  |  |
| --- | --- | --- |
| **Documentation and Procedures for Accounting Systems/Order Processing** | | |
| **System(s) of Interest** | Documentation and Procedures for Accounting Systems/Order Processing is its own system of interest. | |
| **Key Classes of Components** | Desktop (PCs)  Accounting System  Administrative Network  Anti-Malware Software |
| **Documentation and Storage of Operational Data** | | |
| **System(s) of Interest** | Documentation and Storage of Operational Data are themselves the system of interest. | |
| **Key Classes of Components** | Desktops (PCs)  Production System  Automated Manufacturing Systems  Production Network  Administrative Network  Anti-Malware Software |
| **Class of Component** | Rationale for Selection |
| * **Servers** | Swisher Databases are stored and managed on Swisher Data Servers. These databases store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Networking components** | Swisher Intellectual Property and other protected information assets are stored and managed on Swisher Databases.  Swisher Databases are stored and managed on Swisher Data Servers.  Swisher Servers connects to Switches which route data between Swishers Desktop (PCs), Laptops, IoT Devices, Swisher Data Servers, and the internet.  Access Points act as a wireless connection link between devices on Swishers networks to switches, to routers, and then to either the data server or the internet.  While the networks are logically separated all have access to both the internet and the data server. It is essential that these are secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Security components** | Logically isolated networks and traffic to reduce risk of malware on one infecting all of them.  Anti-Malware package installed on the networks to reduce risk of malware effecting the network and devices using it.  These security components are essential for the protection of sensitive data and essential services and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Desktop workstations** | Used by every department within Swisher. Desktops (PCs) store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Home computers** |  |
| * **Laptops** |  |
| * **Storage devices** | Hard drives on Desktops (PCs) and Laptops for local storage. Hard drives are not reported to but are accessible to potentially store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Wireless components** |  |
| * **Others (list)**   **Website** |  |

## A5.1e | Identify Key Classes of Components

|  |  |  |
| --- | --- | --- |
| **Documentation and Procedures for Accounting Systems/Order Processing** | | |
| **System(s) of Interest** | Documentation and Procedures for Accounting Systems/Order Processing is its own system of interest. | |
| **Key Classes of Components** | Desktop (PCs)  Accounting System  Administrative Network  Anti-Malware Software |
| **Class of Component** | Rationale for Selection |
| * **Servers** | Swisher Databases are stored and managed on Swisher Data Servers. These databases store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Networking components** | Swisher Intellectual Property and other protected information assets are stored and managed on Swisher Databases.  Swisher Databases are stored and managed on Swisher Data Servers.  Swisher Servers connects to Switches which route data between Swishers Desktop (PCs), Laptops, IoT Devices, Swisher Data Servers, and the internet.  Access Points act as a wireless connection link between devices on Swishers networks to switches, to routers, and then to either the data server or the internet.  While the networks are logically separated all have access to both the internet and the data server. It is essential that these are secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Security components** | Logically isolated networks and traffic to reduce risk of malware on one infecting all of them.  Anti-Malware package installed on the networks to reduce risk of malware effecting the network and devices using it.  These security components are essential for the protection of sensitive data and essential services and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Desktop workstations** | Used by every department within Swisher. Desktops (PCs) store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Home computers** |  |
| * **Laptops** |  |
| * **Storage devices** | Hard drives on Desktops (PCs) and Laptops for local storage. Hard drives are not reported to but are accessible to potentially store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Wireless components** |  |
| * **Others (list)**   **Website** | Website stores public facing ordering and shipping information and handles retail business transactions. Swishers webserver is stored and managed on the Swisher Data Server which collects user information and manages retail orders. While the website does not store credit card information or PII it is essential for conducting retail business online and communicated purchases to the accounting systems for order processing. |

## A5.1f | Identify Key Classes of Components

|  |  |  |
| --- | --- | --- |
| **Network Access and Use** | | |
| **System(s) of Interest** | Network Access and Use is its own system of interest. | |
| **Key Classes of Components** | Desktops (PCs)  Laptops  Production System  Automated Manufacturing System  IoT Devices  Accounting System  Human Resources System  Production Network  Administrative Network  Lab Network  Anti-Malware Software |
| **Class of Component** | Rationale for Selection |
| * **Servers** | Swisher Databases are stored and managed on Swisher Data Servers. These databases store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Networking components** | Swisher Intellectual Property and other protected information assets are stored and managed on Swisher Databases.  Swisher Databases are stored and managed on Swisher Data Servers.  Swisher Servers connects to Switches which route data between Swishers Desktop (PCs), Laptops, IoT Devices, Swisher Data Servers, and the internet.  Access Points act as a wireless connection link between devices on Swishers networks to switches, to routers, and then to either the data server or the internet.  While the networks are logically separated all have access to both the internet and the data server. It is essential that these are secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Security components** | Logically isolated networks and traffic to reduce risk of malware on one infecting all of them.  Anti-Malware package installed on the networks to reduce risk of malware effecting the network and devices using it.  These security components are essential for the protection of sensitive data and essential services and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Desktop workstations** | Used by every department within Swisher. Desktops (PCs) store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Home computers** |  |
| * **Laptops** | Laptops store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Storage devices** | Hard drives on Desktops (PCs) and Laptops for local storage. Hard drives are not reported to but are accessible to potentially store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. |
| * **Wireless components** |  |
| * **Others (list)**   **Website** | Website stores public facing ordering and shipping information and handles retail business transactions. Swishers webserver is stored and managed on the Swisher Data Server which collects user information and manages retail orders. While the website does not store credit card information or PII it is essential for conducting retail business online. |

## A5.2 | Identify Infrastructure Components to Examine

| **Class of Component** | **Selected Component/ IP Addresses/Host Names** | **Rationale** | **Approach** |
| --- | --- | --- | --- |
| Data Server | -----------------  -----------------  -----------------  -----------------  -----------------  ----------------- | Swisher Databases are stored and managed on Swisher Data Servers. These databases store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. | Ensure data stored on the data server is encrypted.  Ensure the data server has a secure connection to its routers using SSH or equivalent network communication protocol.  Ensure the server has SSL protocols or equivalent encryption protocol.  Ensure the data server has user account and privilege management with access restricted to only authorized users.  Ensure there is server password security requirements implemented and enforced.  Ensure software updates are regularly applied to the data server.  Ensure regular backups of stored data are done and are encrypted. |
| Networking Components | -----------------  -----------------  ----------------- | While the networks are logically separated by its components all networks have access to both the internet and the data server. It is essential that these are secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. | Ensure the implementation of NAC on the network.  Ensure that the NAC on the network has established and enforced use cases to restrict user access to sensitive data and system access.  Ensure firewall or equivalent network protection software is implemented.  Ensure firewall has policies that will effectively block malicious activity and unauthorized access on the network.  Ensure all routers are using WPA3 or WPA2 and not older wifi security certificates.  Ensure all routers are updating their software regularly.  Ensure all networks have a secure password to prevent unauthorized connections.  Ensure that administrative accounts are not connected to the routers when they are not actively performing administrative duties on them.  Ensure all unused ports are disabled on network switches.  Ensure port security settings on network switches.  Ensure MAC addresses are secure on network switches.  Ensure all switches are updating their software regularly. |
| Security Components | -----------------  -----------------  ----------------- | Logically isolated networks and traffic to reduce risk of malware on one infecting all of them.  Anti-Malware package installed on the networks to reduce risk of malware effecting the network and devices using it.  These security components are essential for the protection of sensitive data and essential services and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. | Ensure anti-malware software is implemented to secure the data server.  Ensure anti-malware software is implemented to secure the routers.  Ensure anti-malware software is implemented to secure the switches.  Ensure anti-malware software is implemented to secure access points.  Ensure anti-malware software is implemented to secure desktop workstations.  Ensure anti-malware software is implemented to secure laptops.  Ensure anti-malware software is updated regularly. |
| Desktop Workstations | -----------------  -----------------  ----------------- | Used by every department within Swisher. Desktops (PCs) store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. | Ensure application control policies are implemented and enforced on laptops.  Ensure monitoring and documentation of activity of access and use on laptops.  Ensure policies and implemented and enforced to restrict personal use of laptops.  Ensure access is removed from terminated employees to laptops.  Ensure policies are implemented and enforced for timely removal of access of terminated employees to laptops.  Ensure screen saver policy is implemented and enforced on laptops. |
| Laptops |  | Laptops store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. Laptops are brough off-site and are at higher risk of exposure due to connecting to networks not managed by Swisher. | Ensure application control policies are implemented and enforced on laptops.  Ensure monitoring and documentation of activity of access and use on laptops.  Ensure policies and implemented and enforced to restrict personal use of laptops.  Ensure access is removed from terminated employees to laptops.  Ensure policies are implemented and enforced for timely removal of access of terminated employees to laptops.  Ensure screen saver policy is implemented and enforced on laptops. |
| Storage Devices |  | External hard drives for Desktops (PCs) and Laptops for local storage. External hard drives are not reported to but are accessible to potentially store and manage sensitive information assets and must remain secure from unauthorized access and disruption to maintain confidentiality, integrity, and availability of the information they stored and manage. | Ensure external hard drives are encrypted.  Ensure external hard drives have secure passwords to prevent unauthorized access.  Ensure accurate documentation and tracking of external hard drives.  Ensure accurate documentation of all data and software stored and managed on external hard drives. |

# Process 6

## A6.1 | Review Technology Vulnerabilities and Summarize Results

| **Class** | **Selected Component/ IP Address/Host Name** | **Vulnerability Summary** |
| --- | --- | --- |
| Data Server | -----------------  -----------------  -----------------  -----------------  -----------------  ----------------- | *7 Pass:* Data stored on the data server is encrypted.  *8 Pass:* The data server has a secure connection to its routers using SSH or equivalent network communication protocol.  *5 Fail:* The server does not have SSL protocols or equivalent encryption protocol.  *6 Pass:* The data server has user account and privilege management with access restricted to only authorized users.  *5 Fail:* There is no server password security requirements implemented and enforced on the data server.  *11 Fail:* Software updates are not regularly applied to the data server.  *7 Pass*: Regular backups of stored data are done and are encrypted on the data server. |
| Networking Components | -----------------  -----------------  ----------------- | *8 Pass:* NAC is implemented on the network.  *7 Pass:* NAC on the network establishes and enforces use cases.  *6 Pass*: Anti-malware software is implemented on the network.  *7 Pass*: Anti-malware policies effectively block malicious activity and unauthorized access on the network.  *7 Pass*: All routers are using WPA3 or WPA2 security certificates.  *4 Failed*: Routers are not having regular software updates.  *10 Failed:* Networks do not have secure passwords to prevent unauthorized connections.  *10 Failed:* Administrative accounts are not disconnected from routers when they are not in use.  *3 Failed*: Unused ports are not disabled on network switches.  *4 Failed*: Port security settings are not optimized on network switches.  *9 Pass:* MAC addresses are secure on network switches. |
| Security Components | -----------------  -----------------  ----------------- | *7 Pass:* Anti-malware software is implemented to secure the data server.  *8 Pass:* Anti-malware software is implemented to secure the routers.  *10 Fail:* Anti-malware software is not implemented to secure switches.  *3 Fail:* Anti-malware software is not implemented to secure access points.  *8 Pass:* Anti-malware software is implemented to secure desktop workstations.  *7 Pass:* Anti-malware software is implemented to secure laptops.  *6 Pass:* Anti-malware software is updated regularly. |
| Desktop Workstations | -----------------  -----------------  ----------------- | *6 Pass:* Application control policies are implemented and enforced on desktop workstations.  *6 Pass:* There is monitoring and documentation of activity of access and use on desktop workstations.  *7 Pass:* Policies are implemented and enforced on desktop workstations to enforce restricted personal use.  *6 Pass:* Access is removed from terminated employees desktop workstations.  *11 Fail:* Policies are not implemented and enforced for timely removal of access of terminated employees to desktop workstations.  *9 Fail:* Screen saver policy is not implemented and enforced on desktop workstations |
| Laptops | -----------------  -----------------  ----------------- | *5 Fail:* Application control policies are not implemented and enforced on laptops.  *7 Pass:* There is monitoring and documentation of activity of access and use on laptops.  *5 Fail:* Policies are implemented and enforced on laptops to enforce restricted personal use.  *3 Fail:* Access is removed from terminated employee’s laptops.  *6 Pass:* Policies are not implemented and enforced for timely removal of access of terminated employees to laptops.  *9 Fail:* Screen saver policy is not implemented and enforced on laptops. |
| Storage Devices | -----------------  -----------------  ----------------- | *7 Pass:* External hard drives are encrypted.  *8 Pass:* External hard drives have secure passwords to prevent unauthorized access.  *2 Fail:* Documentation and tracking of external hard drives is not accurate.  *11 Fail:* Documentation of all data and software stored and managed on external hard drives is not accurate. |

## A6.2 | Vulnerability Evaluation Summary

|  |  |
| --- | --- |
| **Vulnerability Severity Level** | **Meaning** |
| High-severity vulnerabilities | Must be fixed immediately (within the next week) |
| Medium-severity vulnerabilities | Must be fixed soon (within 1 month) |
| Low-severity vulnerabilities | May be fixed later |

| **Class of Component** | **Selected Component/ IP Address(es)** | **Tool/Method/ Approach** | **Vulnerability Summary** |
| --- | --- | --- | --- |
| Data Server | -------------------  ------------------- | Have IT Staff check for and test for vulnerabilities identified to be examined. | 0 - High  3 - Medium  0 - Low |
| Networking Components | -------------------  ------------------- |  |  |
| Have IT Staff check for and test for vulnerabilities identified to be examined. | 2 - High  3 - Medium  0 - Low |
| Security Components | -------------------  ------------------- |  |  |
| Have IT Staff check for and test for vulnerabilities identified to be examined. | 0 - High  2 - Medium  0 - Low |
| Desktop Workstations | -------------------  ------------------- |  |  |
| Have IT Staff check for and test for vulnerabilities identified to be examined. | 0 - High  2 - Medium  0 - Low |
| Laptops | ------------------- | Have IT Staff check for and test for vulnerabilities identified to be examined. | 0 - High  4 - Medium  0 - Low |
| Storage Devices | -------------------  ------------------- | Have IT Staff check for and test for vulnerabilities identified to be examined. | 0 - High  2 - Medium  0 - Low |
|  |  |

## A6.3 | Actions and Recommendations for Addressing Technology Vulnerabilities

| Actions and Recommendations for Addressing Technology Vulnerabilities |
| --- |
| IT Staff will configure and enforce SSL protocols or equivalent encryption protocols on Swisher data servers.  IT Staff will develop, implement, and enforce password requirements on Swisher data server.  IT Staff will enable and monitor Swisher data servers to ensure regular updating of firmware and software. |
| IT Staff will enable and monitor Swisher routers to ensure regular updating of firmware and software.  IT Staff will develop, implement, and enforce password requirements on Swisher networks.  IT Staff will ensure administrative accounts are not connected to routers when these privileged accounts are not actively in use.  IT Staff will disable unused ports on network switches.  IT Staff will develop, implement, and enforce optimized port security settings on Swisher network switches. |
|  |
| IT Staff will implement anti-malware software to secure Swisher switches.  IT Staff will implement anti-malware software to secure Swisher access points. |
|  |
| IT Staff will implement and enforce policies that will timely remove all access of terminated employees to desktop workstations.  IT Staff will implement and enforce screen saver policies on desktop workstations. |
| IT Staff will implement and enforce application control policies on laptops.  IT Staff will implement and enforce restricted personal use policies on laptops.  IT Staff will timely remove terminated employee’s access to laptops.  IT Staff will implement and enforce screen saver policies on laptops. |
| IT Staff will update and maintain accurate documentation and tracking of external hard drives.  IT Staff will maintain accurate documentation of all data and software stored and managed on external hard drives. |

# Process 7

## A7.1 | Identify the Impact of Threats to Critical Assets

| **Asset** | **Outcome** | **Impact Description** | **Values** |
| --- | --- | --- | --- |
|  | Disclosure | Disclosure of Intellectual Property and/or Proprietary Information will result in losses in Swishers’ competitive edge it holds over its competitors. Additionally, disclosure will result in loss of client trust and business. Swisher may face lawsuits for negligence from clients if disclosure results in loss in client confidential information or damages to business assets such as profit. | High |
|  | Modification |  |  |
| Intellectual Property and Proprietary Information |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | Loss/ destruction | Loss or Destruction of Intellectual Property and/or Proprietary Information will result in losses in Swishers’ competitive edge it holds over its competitors. Additionally, loss or destruction may result in loss of client trust and business. | High |
|  | Interruption |  |  |
|  |  |  |  |

| **Asset** | **Outcome** | **Impact Description** | **Values** |
| --- | --- | --- | --- |
| Confidential/Protected Data (PII, Financial Records, etc.) | Disclosure | These assets are protected information by local, state, and federal law and regulations. Access is restricted to Site Human Resources Manager, their staff, and the Site Manager. Disclosure will result in legal fines and lawsuits for negligence. | High |
|  | Modification | Timecards and Payroll Cards must not be altered or modified without authorization from the Site Account Manager, their staff, and the Site Manager. Modification of this information may result in loss of time to normal business operation and incorrect or failed billing to clients resulting in temporary loss of Swisher finances or loss of client trust. | Medium |
|  |  |
|  |  |
|  |  |
|  | Loss/ destruction | These assets must securely be stored and backed up to ensure availability. Loss or destruction of this information may result in loss of time to normal business operation. | Low |
|  | Interruption | These assets must securely be stored and backed up to ensure availability. Interruption to this information may result in loss of time to normal business operation. | Low |
|  |  |

| **Asset** | **Outcome** | **Impact Description** | **Values** |
| --- | --- | --- | --- |
| Documentation and Storage of Operational Data (Hardware and Software Profiles, Scheduling Data, Inventory, etc.) | Disclosure | The advantages Swisher has over its competitors comes from the hardware and software profiles of their production systems to develop and produce products at a 30%-40% lower price compared to other manufacturers. These profiles are the key to this success and must not be accessed by unauthorized users. | High |
|  | Modification | Incorrect/Inaccurate modification of scheduling data due to human error or intentional malicious intent may result in interruptions to productions or production of assets outside of specification resulting in damages to client trust, or lawsuits for negligence. | High |
|  |  |
|  |  |
|  |  |
|  | Loss/ destruction | Loss of production up-time due to loss of availability of scheduling or inventory data may result in failures to meet deadlines for orders and loss of custom trust. The advantages Swisher has over its competitors comes from the hardware and software profiles of their production systems to develop and produce products at a 30%-40% lower price compared to other manufacturers. These profiles are the key to this success and must not be accessed by unauthorized users. | High |
|  | Interruption | Loss of production up-time due to loss of availability of scheduling or inventory data may result in failures to meet deadlines for orders and loss of custom trust. | Medium |
|  |  |

| **Asset** | **Outcome** | **Impact Description** | **Values** |
| --- | --- | --- | --- |
|  | Disclosure |  |  |
| Documentation and Procedures for Accounting Systems/Order Processing | Modification | Improper modification such as incorrect data input, untimely data input, or no data input when input is required. Modification of this information may result in loss of time to normal business operation and incorrect or failed billing to clients resulting in temporary loss of Swisher finances or loss of client trust. | Low |
|  |  |
|  |  |
|  |  |
|  | Loss/ destruction | The billing cycle is monthly so loss or destruction to these services can result in prolonged wait for payments received or paid. Additionally, loss or destruction of this information may result in loss of time to normal business operation and incorrect or failed billing to clients resulting in temporary loss of Swisher finances or loss of client trust. | Low |
|  | Interruption |  |  |
|  |  |

| **Asset** | **Outcome** | **Impact Description** | **Values** |
| --- | --- | --- | --- |
|  | Disclosure | Unauthorized access from persons accessing the network can result in confidential information and data being stolen or leaked. Disclosure of Intellectual Property and/or Proprietary Information will result in losses in Swishers’ competitive edge it holds over its competitors. Additionally, disclosure will result in loss of client trust and business. Swisher may face lawsuits for negligence from clients if disclosure results in loss in client confidential information or damages to business assets such as profit. | High |
| Network Access and Use |  | Unauthorized access from persons accessing the network can result in confidential information and data being altered to be incorrect. Additionally, this modification will result in adverse effects to any of Swishers’ systems that the unauthorized modification targets. | High |
|  | Modification |
|  |  |
|  |  |
|  | Loss/ destruction | Unauthorized access from persons accessing the network can result in confidential information and data being deleted or removed from the network. Loss or Destruction of Intellectual Property and/or Proprietary Information will result in losses in Swishers’ competitive edge it holds over its competitors. Additionally, loss or destruction may result in loss of client trust and business. The billing cycle is monthly so loss or destruction to these services can result in prolonged wait for payments received or paid. Additionally, loss or destruction of this information may result in loss of time to normal business operation and incorrect or failed billing to clients resulting in temporary loss of Swisher finances or loss of client trust. | High |
|  | Interruption | The network must be secured from interruption up to ensure availability. Interruption to this information may result in loss of time to normal business operation. | Low |
|  |  |

## A7.2 | Create Risk Evaluation Criteria

| **Impact Area** | **High** | **Medium** | **Low** |
| --- | --- | --- | --- |
| Reputation/ Customer Confidence | * Reputation irrevocably destroyed or damaged * Loss of rating or accreditation by review organizations * More than 30% drop in customers due to loss of confidence | * Reputation damaged; some effort and expense required to recover * Reduction or warning of reduction of rating or accreditation by authorizing organizations * 10 to 30% drop in customers due to loss of confidence * Public violations of Privacy Act: (1) disclosure to personnel within the organization and facility without the need to know; (2) anyone who violates the Privacy Act and reveals sensitive financial or PII information * Clients seek service from competitor | * Reputation minimally affected; little or no effort or expense required to recover * No change in rating or accreditation by authorizing organizations * Less than 10% drop in customers due to loss of confidence * Non-public violation of Privacy Act (disclosure to personnel within the organization and facility with a need to know – trusted agent) |
| Life/ Health of Customers | * Loss of customer or employee life * Permanent impairment of one or more significant aspects of customer’s or employee’s health (e.g., loss of use of one or more limbs, blindness, brain damage) * Employee unable to work for more than a week * Safety violated | * Customer or employee life threatened but recoverable with additional treatment * Temporary or recoverable impairment of customer’s or employee’s health (e.g., recovering use of limbs through physical therapy) * Employee unable to work for one to two days * Safety affected | * No loss or significant threat to customer or employee life * Minimal, immediately treatable degradation in customer or employee heath with recovery within four days * Safety questioned |
| Productivity | * Employees unable to perform critical job aspects for two or more days * 40% or more increase in work hours required of at least 10% of general staff for >two days * Irrecoverable loss of essential production and/or business assets | * Physicians and/or nursing staff work increased by 10-40% for one day * Increases in general staff work of 10-40% for one day * Inefficient continuity of production; delays while recovering losses or interrupted information or assets | * Employees inconvenienced for less than a day but no measurable increase in work effort * Systems inconvenienced for less than a day but no measurable increase in work effort occurs |
| Fines/ Legal Penalties | * Fines of greater than $100,000 levied * One or more non-frivolous lawsuits of more than $750,000 filed by customers * Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices | * Fines of $10,000 to $100,000 levied * One or more non-frivolous lawsuits between $250,000 and $750,000 filed by customers * Government or other investigative organization requests information or records (low-profile) | * No fine or a fine of less than $10,000 levied * Lawsuit of less than $250,000 or frivolous lawsuit (95% sure it can be overturned) filed by customer * No queries from government or other investigative organizations |
| Finances | * Yearly operational costs up 15% * 20% yearly revenue loss * One-time financial cost > $750,000 * Uncorrectable errors in funding and personnel | * Yearly operational costs up 2-15% * 5-20% yearly revenue loss * One-time financial cost of $25K to $750,000 * Partially correctable errors in funding and personnel | * Increase of less than 2% in operating costs * <5% yearly revenue loss * One-time financial cost of <$25K * Inconvenient but correctable errors in funding and personnel |
| Other  (Facilities) | * Loss of an entire facility or building due to fire, or air quality monitoring system failure * Loss of production space for more than a month | * Damage to a facility or building requiring temporary relocation of assets * Loss of production space for more than a week | * Negligible impact on daily operations * Loss of production space for more than a day |

# Process 8

## A8.1.SP1 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| **Security Awareness and Training (SP1): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Unclear | Unclear | No | Yes |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Unclear | Yes | Unclear | No |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | Unclear | Yes | Yes | No |

| **Security Awareness and Training (SP1): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | IT Staff should meet with management to discuss security roles and responsibilities and disclose verified documentation for approval and improved understanding from management. | Management buy in is important for development and enforcement of IT security. |
| Operational Area Management | IT Staff should check-in with management to ensure services, mechanisms, and technologies are being managed by a capable or available staff member. | IT Staff is essentially saying here that they are not adequate enough in-house expertise to manage Swisher’s systems. This may be an implication of another issue but should still be addressed. |
| Staff |  |  |
| IT Staff | Ensure IT Staff are receiving Security ATE too. | SATE is intended to promote security against current and future threats and should be modified to meet the needs of all staff, even the ones that are experts. |

## A8.1.SP2 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| **Security Strategy (SP2): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| The organization’s business strategies routinely incorporate security considerations. | Unclear | Yes |  | Yes |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | Unclear | Yes |  | Yes |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | Unclear | No |  | Yes |

| **Security Strategy (SP2): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | IT Staff should meet with management to discuss security topics for approval of current and future mechanisms, improved management understanding on Swisher security policies and posture, and to encourage manager buy-in. | Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs they may struggle to develop and maintain a strong security posture. |
| Operational Area Management |  |  |
| Staff |  |  |
| IT Staff |  |  |

## A8.1.SP3 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| **Security Management (SP3): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Management allocates sufficient funds and resources to information security activities. | Unclear | Yes | Unclear | Unclear |
| Security roles and responsibilities are defined for all staff in the organization. | Unclear | Yes | Unclear | Yes |
| The organization’s hiring and termination practices for staff take information security issues into account. | Unclear | Yes | Unclear | No |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Unclear | Yes | Unclear | No |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Unclear | Yes |  | Yes |

| **Security Management (SP3): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | IT Staff should meet with management to discuss security topics for approval of current and future mechanisms, improved management understanding on Swisher security policies and posture, and to encourage manager buy-in. | Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs they may struggle to develop and maintain a strong security posture. |
| Operational Area Management |  |  |
| Staff | It is not terribly important that staff is aware of the details of these topics. |  |
| IT Staff |  |  |

## A8.1.SP4 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| **Security Policies and Regulations (SP4): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Unclear | Unclear | No | Yes |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes | Yes | Unclear | Yes |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Unclear | Unclear |  | Yes |
| The organization uniformly enforces its security policies. | Unclear | Yes | No | Yes |

| **Security Policies and Regulations (SP4): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs, they may struggle to develop and maintain a strong security posture. | Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs, they may struggle to develop and maintain a strong security posture. |
| Operational Area Management | Operational Managers do not know if its evaluating and ensuring compliance with major security requirements but is certain that they enforce them. | Miscommunication of what policies are being enforced or what they are enforcing can result in violations of policy when this happens at a management level. |
| Staff | Staff should be aware of policies, how to locate them, and the importance of them. | Staff are not aware of policies, how to access them, so these policies may not be enforced at a worker level. |
| IT Staff |  |  |

## A8.1.SP5 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| **Collaborative Security Management (SP5): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Unclear | Yes | No | Yes |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | Unclear | Yes |  | No |

| **Collaborative Security Management (SP5): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs, they may struggle to develop and maintain a strong security posture | Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs, they may struggle to develop and maintain a strong security posture. |
| Operational Area Management |  |  |
| Staff | Staff should be aware of policies, how to locate them, and the importance of them. | Staff are not aware of policies, how to access them, so these policies may not be enforced at a worker level. |
| IT Staff | The only outsourced security service is the servicing bank that manages customer credit card information. | Swisher should still ensure their servicing bank is meeting regulatory standards and has strong public facing policies. |

## A8.1.SP6 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| **Contingency Planning/Disaster Recovery (SP6): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| An analysis of operations, applications, and data criticality has been performed. | Yes | No |  | Yes |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | No | No |  | Yes |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | No | Unclear |  | No |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes | No | Unclear | Yes |

| **Contingency Planning/Disaster Recovery (SP6): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | Disaster recovery planning is not being maintained or developed to meet current organizational needs. | Failure to implement and maintain an effective disaster recovery plan can result in loss of life, injury, or unnecessary damage to organization assets. |
| Operational Area Management |  |  |
| Staff |  |  |
| IT Staff |  |  |

## A8.1.OP1.1 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| **Physical Security Plans and Procedures (OP1.1): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes | Yes | No | Yes |
| There are documented policies and procedures for managing visitors. | Unclear | Yes | No | Yes |
| There are documented policies and procedures for physical control of hardware and software. | Unclear | Yes | No | No |

| **Physical Security Plans and Procedures (OP1.1): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management |  |  |
| Operational Area Management |  |  |
| Staff | Staff should be made aware of policies regarding guests or physically handing hardware or modifying software. | Guests may end up accessing restricted areas without authorization. Hardware or software configurations may be adjusted outside of alignment with organization parameters. |
| IT Staff |  |  |

## A8.1.OP1.2 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| **Physical Access Control (OP1.2): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Unclear | Yes | Unclear | Yes |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Unclear | Yes | Yes | Yes |

| **Physical Access Control (OP1.2): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs, they may struggle to develop and maintain a strong security posture | Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs, they may struggle to develop and maintain a strong security posture. |
| Operational Area Management |  |  |
| Staff |  |  |
| IT Staff |  |  |

## A8.1.OP1.3 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| Monitoring and Auditing Physical Security (OP1.3): Survey Results | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Maintenance records are kept to document the repairs and modifications of a facility’s physical components. |  |  |  | Yes |
| An individual’s or group’s actions, with respect to all physically controlled media, can be accounted for. |  |  |  | Yes |
| Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed. |  | Unclear |  | No |

| **Monitoring and Auditing Physical Security (OP1.3): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management |  |  |
| Operational Area Management | Operational Management should audit and verify IT Staff are performing audits and are monitoring logs. | There is only one IT Staff, having confirmation that this task is being done should be supported by management. |
| Staff |  |  |
| IT Staff |  |  |

## A8.1.OP2.1 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| **System and Network Management (OP2.1): Survey Results** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Survey Statement** | | **Senior Managers** | | **Operational Area Managers** | **Staff** | **IT Staff** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | | Unclear | | Yes |  | Yes | |
| Sensitive information is protected by secure storage (e.g., backups stored off site, discard process for sensitive information). | |  | |  |  | No | |
| The integrity of installed software is regularly verified. | |  | |  |  | Yes | |
| All systems are up to date with respect to revisions, patches, and recommendations in security advisories. | |  | |  |  | Yes | |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | | Unclear | | Yes | Yes | No | |
| Changes to IT hardware and software are planned, controlled, and documented. | |  | |  |  | No | |
| IT staff members follow procedures when issuing, changing, and terminating users’ passwords, accounts, and privileges.   * Unique user identification is required for all information system users, including third-party users. * Default accounts and default passwords have been removed from systems. | |  | |  |  | Yes | |
| Only necessary services are running on systems – all unnecessary services have been removed. | |  | |  |  | Yes | |
| **System and Network Management (OP2.1): Contextual Information** | | | | | | |
| **Organizational Level** | **Protection Strategy Practices** | | **Organizational Vulnerabilities** | | | |
| Senior Management |  | |  | | | |
| Operational Area Management |  | |  | | | |
| Staff |  | |  | | | |
| IT Staff | IT Staff should ensure regular backups and encryption of this data.  Documentation of IT hardware changes must be made, approved, and recorded for future reference. | | IT Staff is not aware of changes made to hardware and software planned or otherwise. | | | |

## A8.1.OP2.2 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| **System Administration Tools (OP2.2): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. |  |  |  | Yes |

## A8.1.OP2.3 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| **Monitoring and Auditing IT Security (OP2.3): Survey Results** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Survey Statement** | | **Senior Managers** | | **Operational Area Managers** | **Staff** | **IT Staff** |
| System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure. | |  | |  |  | Yes |
| Firewall and other security components are periodically audited for compliance with policy. | |  | |  |  | No |
| **Monitoring and Auditing IT Security (OP2.3): Contextual Information** | | | | | | |
| **Organizational Level** | **Protection Strategy Practices** | | **Organizational Vulnerabilities** | | | |
| Senior Management |  | |  | | | |
| Operational Area Management |  | |  | | | |
| Staff |  | |  | | | |
| IT Staff | IT Staff should ensure that anti-malware software is regularly updated and tested to ensure compliance with organization and regulatory compliance. | | Unpatched and untested firewalls can result in successful attacks on Swisher networks. | | | |

## A8.1.OP2.4 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| **Authentication and Authorization (OP2.4): Survey Results** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Survey Statement** | | **Senior Managers** | | **Operational Area Managers** | **Staff** | **IT Staff** |
| Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections. | |  | | No |  | Unclear |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | | Unclear | | No |  | Unclear |
| Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner. Methods or mechanisms are periodically reviewed and verified. | |  | |  |  | Yes |
| **Authentication and Authorization (OP2.4): Contextual Information** | | | | | | |
| **Organizational Level** | **Protection Strategy Practices** | | **Organizational Vulnerabilities** | | | |
| Senior Management |  | |  | | | |
| Operational Area Management |  | |  | | | |
| Staff |  | |  | | | |
| IT Staff | Access control management policies should be developed, implemented, and maintained to ensure unauthorized access can not be made to Swisher systems | |  | | | |

## A8.1.OP2.5 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| **Vulnerability Management (OP2.5): Survey Results** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Survey Statement** | | **Senior Managers** | | **Operational Area Managers** | **Staff** | **IT Staff** |
| There is a documented set of procedures for managing vulnerabilities, including   * selecting vulnerability evaluation tools, checklists, and scripts * keeping up to date with known vulnerability types and attack methods * reviewing sources of information on vulnerability announcements, security alerts, and notices * identifying infrastructure components to be evaluated * scheduling of vulnerability evaluations * interpreting and responding to the results * maintaining secure storage and disposition of vulnerability data | |  | |  |  | Yes |
| Vulnerability management procedures are followed and are periodically reviewed and updated. | |  | |  |  | Yes |
| Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified. | |  | |  |  | Yes |
| **Vulnerability Management (OP2.5): Contextual Information** | | | | | | |
| **Organizational Level** | **Protection Strategy Practices** | | **Organizational Vulnerabilities** | | | |
| Senior Management |  | |  | | | |
| Operational Area Management |  | |  | | | |
| Staff |  | |  | | | |
| IT Staff |  | |  | | | |

## A8.1.OP2.6 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| **Encryption (OP2.6): Survey Results** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Survey Statement** | | **Senior Managers** | | **Operational Area Managers** | **Staff** | **IT Staff** |
| Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology). | |  | |  |  | Yes |
| Encrypted protocols are used when remotely managing systems, routers, and firewalls. | |  | |  |  | Yes |
| **Encryption (OP2.6): Contextual Information** | | | | | | |
| **Organizational Level** | **Protection Strategy Practices** | | **Organizational Vulnerabilities** | | | |
| Senior Management |  | |  | | | |
| Operational Area Management |  | |  | | | |
| Staff |  | |  | | | |
| IT Staff |  | |  | | | |

## A8.1.OP2.7 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnerabilities, Security Requirements, and Risk Information

| **Security Architecture and Design (OP2.7): Survey Results** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Survey Statement** | | | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| System architecture and design for new and revised systems include considerations for   * security strategies, policies, and procedures * history of security compromises * results of security risk assessments | | |  |  |  | Yes |
| The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology. | | |  |  |  | Unclear |
| **Security Architecture and Design (OP2.7): Contextual Information** | | | | | | |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** | | | | |
| Senior Management |  |  | | | | |
| Operational Area Management |  |  | | | | |
| Staff |  |  | | | | |
| IT Staff |  |  | | | | |

## A8.1.OP3.1 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnera1ilities, Security Requirements, and Risk Information

| **Incident Management (OP3.1): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Unclear | Unclear | Unclear | Yes |
| Incident management procedures are periodically tested, verified, and updated. | Unclear | Yes | Unclear | Unclear |
| There are documented policies and procedures for working with law enforcement agencies. | Unclear | Yes | Unclear | Yes |

| **Incident Management (OP3.1): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management |  |  |
| Operational Area Management |  |  |
| Staff |  |  |
| IT Staff |  |  |

## A8.1.OP3.2 | Review Vulnerabilities, Protection Strategy Practices, Organizational Vulnera1ilities, Security Requirements, and Risk Information

| **General Staff Practices (OP3.2): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Unclear | No | Unclear | Yes |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Unclear | Yes | Unclear | Yes |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Unclear | No | Unclear | Yes |

| **General Staff Practices (OP3.2): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs, they may struggle to develop and maintain a strong security posture | Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs, they may struggle to develop and maintain a strong security posture. |
| Operational Area Management | Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs, they may struggle to develop and maintain a strong security posture | Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs, they may struggle to develop and maintain a strong security posture. |
| Staff |  |  |
| IT Staff |  |  |

## A8.2 | Consolidate Protection Strategy Information

| **Organization Protection Strategy** | |
| --- | --- |
| **Strategy Area** | **Strategy** |
| Security Awareness and Training | IT Staff should meet with management to discuss security roles and responsibilities and disclose verified documentation for approval and improved understanding from management.  IT Staff should check-in with management to ensure services, mechanisms, and technologies are being managed by a capable or available staff member.  Ensure IT Staff are receiving Security ATE too at an appropriate level. |
| Security Strategy | IT Staff should meet with management to discuss security topics for approval of current and future mechanisms, improved management understanding on Swisher security policies and posture, and to encourage manager buy-in. |
| Security Management | IT Staff should meet with management to discuss security topics for approval of current and future mechanisms, improved management understanding on Swisher security policies and posture, and to encourage manager buy-in. |
| **Strategy Area** | **Strategy** |
| Security Policies and Regulations | Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs, they may struggle to develop and maintain a strong security posture.  Operational Managers do not know if its evaluating and ensuring compliance with major security requirements but is certain that they enforce them.  Staff should be aware of policies, how to locate them, and the importance of them. |
| Collaborative Security Management | Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs, they may struggle to develop and maintain a strong security posture  Staff should be aware of policies, how to locate them, and the importance of them.  Swisher should ensure their servicing bank is meeting regulatory standards and has strong public facing policies. |
| Contingency Planning/ Disaster Recovery | Disaster recovery planning is not being maintained or developed to meet current organizational needs. |
| Physical Security | Staff should be made aware of policies regarding guests or physically handing hardware or modifying software.  Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs, they may struggle to develop and maintain a strong security posture  Operational Management should audit and verify IT Staff are performing audits and are monitoring logs.  There is only one IT Staff, having confirmation that this task is being done should be supported by management. |
| Information Technology Security | IT Staff should ensure regular backups and encryption of this data.  Documentation of IT hardware changes must be made, approved, and recorded for future reference.  IT Staff should ensure that anti-malware software is regularly updated and tested to ensure compliance with organization and regulatory compliance.  Access control management policies should be developed, implemented, and maintained to ensure unauthorized access cannot be made to Swisher systems |
| Staff Security | Management are responsible for spear-heading the organization into making positive and effective efforts towards the organizations success. If management is not on the same page about its programs, they may struggle to develop and maintain a strong security posture. |
| Issues |  |

## A8.3a | Create Mitigation Plans

| Intellectual Property and Proprietary Information | |
| --- | --- |
| **Threat Type** | **Actions** |
| Human actors using network access | IT Staff will configure and enforce SSL protocols or equivalent encryption protocols on Swisher data servers.  IT Staff will develop, implement, and enforce password requirements on Swisher data server.  IT Staff will enable and monitor Swisher data servers to ensure regular updating of firmware and software.  IT Staff will enable and monitor Swisher routers to ensure regular updating of firmware and software.  IT Staff will develop, implement, and enforce password requirements on Swisher networks.  IT Staff will ensure administrative accounts are not connected to routers when these privileged accounts are not actively in use.  IT Staff will disable unused ports on network switches.  IT Staff will develop, implement, and enforce optimized port security settings on Swisher network switches.  IT Staff will implement anti-malware software to secure Swisher switches.  IT Staff will implement anti-malware software to secure Swisher access points. |
| Human actors using physical access | IT Staff will implement and enforce policies that will timely remove all access of terminated employees to desktop workstations.  IT Staff will implement and enforce screen saver policies on desktop workstations.  IT Staff will implement and enforce application control policies on laptops.  IT Staff will implement and enforce restricted personal use policies on laptops.  IT Staff will timely remove terminated employee’s access to laptops.  IT Staff will implement and enforce screen saver policies on laptops.  IT Staff will update and maintain accurate documentation and tracking of external hard drives.  IT Staff will maintain accurate documentation of all data and software stored and managed on external hard drives. |
| System problems | IT Staff will ensure regular updates to software and firmware of swisher systems and will develop, implement, and enforce policies to regularly test and maintain software and hardware for defects.  IT Staff will ensure anti-malware software is effectively implemented to secure Swisher systems. Data stored and data in transit will be encrypted and managed on a secure environment to minimize risk of malware threat actors. |
| Other problems | Physical data storage will be maintained of all business and personnel essential information to support disaster recover procedures, or business continuity in the event of limited or total system or power failures. Documentation of physical data storage will be secure, its location will be disclosed to authorized staff, and will continue useful information including emergency contact information, fire exit routes, procedures for protecting Swisher employee safety and business continuity, etc. |
| Measures | ATE training will be documented and records will include information including date, time, personnel attending, topics covered, educator information, and certification fulfillment or failures to complete training.  Password requirements will meet with regulatory compliance and security best standards, or whichever is stronger.  Screen Savers will activate after 5 minutes of inactivity.  All user activities will be monitored and logged and personal activity on workstations will alert IT Staff.  IT Staff will update firmware and software on Swisher systems when they become available and are tested to ensure interruptions to services do not occur or no later than 1-month after they are available. |

## A8.3b | Create Mitigation Plans

| Confidential/Protected Data (PII, Financial Records, etc.) | |
| --- | --- |
| **Threat Type** | **Actions** |
| Human actors using network access | IT Staff will configure and enforce SSL protocols or equivalent encryption protocols on Swisher data servers.  IT Staff will develop, implement, and enforce password requirements on Swisher data server.  IT Staff will enable and monitor Swisher data servers to ensure regular updating of firmware and software.  IT Staff will enable and monitor Swisher routers to ensure regular updating of firmware and software.  IT Staff will develop, implement, and enforce password requirements on Swisher networks.  IT Staff will ensure administrative accounts are not connected to routers when these privileged accounts are not actively in use.  IT Staff will disable unused ports on network switches.  IT Staff will develop, implement, and enforce optimized port security settings on Swisher network switches.  IT Staff will implement anti-malware software to secure Swisher switches.  IT Staff will implement anti-malware software to secure Swisher access points. |
| Human actors using physical access | IT Staff will implement and enforce policies that will timely remove all access of terminated employees to desktop workstations.  IT Staff will implement and enforce screen saver policies on desktop workstations.  IT Staff will implement and enforce application control policies on laptops.  IT Staff will implement and enforce restricted personal use policies on laptops.  IT Staff will timely remove terminated employee’s access to laptops.  IT Staff will implement and enforce screen saver policies on laptops.  IT Staff will update and maintain accurate documentation and tracking of external hard drives.  IT Staff will maintain accurate documentation of all data and software stored and managed on external hard drives. |
| System problems | IT Staff will ensure regular updates to software and firmware of swisher systems and will develop, implement, and enforce policies to regularly test and maintain software and hardware for defects.  IT Staff will ensure anti-malware software is effectively implemented to secure Swisher systems. Data stored and data in transit will be encrypted and managed on a secure environment to minimize risk of malware threat actors. |
| Other problems | Management will review SSAE or equivalent service organization public facing audits to address any security concerns regarding the security of its clients credit card information. |
| Measures | ATE training will be documented and records will include information including date, time, personnel attending, topics covered, educator information, and certification fulfillment or failures to complete training.  Password requirements will meet with regulatory compliance and security best standards, or whichever is stronger.  Screen Savers will activate after 5 minutes of inactivity.  All system activities will be monitored and logged and personal activity on workstations will alert IT Staff.  IT Staff will update firmware and software on Swisher systems when they become available and are tested to ensure interruptions to services do not occur or no later than 1-month after they are available. |

## A8.3c | Create Mitigation Plans

| Documentation and Storage of Operational Data (Hardware and Software Profiles, Scheduling Data, Inventory, etc.) | |
| --- | --- |
| **Threat Type** | **Actions** |
| Human actors using network access | IT Staff will configure and enforce SSL protocols or equivalent encryption protocols on Swisher data servers.  IT Staff will develop, implement, and enforce password requirements on Swisher data server.  IT Staff will enable and monitor Swisher data servers to ensure regular updating of firmware and software.  IT Staff will enable and monitor Swisher routers to ensure regular updating of firmware and software.  IT Staff will develop, implement, and enforce password requirements on Swisher networks.  IT Staff will ensure administrative accounts are not connected to routers when these privileged accounts are not actively in use.  IT Staff will disable unused ports on network switches.  IT Staff will develop, implement, and enforce optimized port security settings on Swisher network switches.  IT Staff will implement anti-malware software to secure Swisher switches.  IT Staff will implement anti-malware software to secure Swisher access points. |
| Human actors using physical access | IT Staff will implement and enforce policies that will timely remove all access of terminated employees to desktop workstations.  IT Staff will implement and enforce screen saver policies on desktop workstations.  IT Staff will implement and enforce application control policies on laptops.  IT Staff will implement and enforce restricted personal use policies on laptops.  IT Staff will timely remove terminated employee’s access to laptops.  IT Staff will implement and enforce screen saver policies on laptops.  IT Staff will update and maintain accurate documentation and tracking of external hard drives.  IT Staff will maintain accurate documentation of all data and software stored and managed on external hard drives. |
| System problems | IT Staff will ensure regular updates to software and firmware of swisher systems and will develop, implement, and enforce policies to regularly test and maintain software and hardware for defects.  IT Staff will ensure anti-malware software is effectively implemented to secure Swisher systems. Data stored and data in transit will be encrypted and managed on a secure environment to minimize risk of malware threat actors. |
| Other problems | Physical or virtual back up files including all business critical data pertaining to operational data such as production specifications, profiles, and data will be securely stored off-site to ensure recovery is possible in the event of the loss of site and damage to assets stored on-site from fire, tornado, flood, etc. |
| Measures | ATE training will be documented and records will include information including date, time, personnel attending, topics covered, educator information, and certification fulfillment or failures to complete training.  Password requirements will meet with regulatory compliance and security best standards, or whichever is stronger.  Screen Savers will activate after 5 minutes of inactivity.  All system activities will be monitored and logged and personal activity on workstations will alert IT Staff.  IT Staff will update firmware and software on Swisher systems when they become available and are tested to ensure interruptions to services do not occur or no later than 1-month after they are available. |

## A8.3d | Create Mitigation Plans

| Documentation and Procedures for Accounting Systems/Order Processing | |
| --- | --- |
| **Threat Type** | **Actions** |
| Human actors using network access | IT Staff will configure and enforce SSL protocols or equivalent encryption protocols on Swisher data servers.  IT Staff will develop, implement, and enforce password requirements on Swisher data server.  IT Staff will enable and monitor Swisher data servers to ensure regular updating of firmware and software.  IT Staff will enable and monitor Swisher routers to ensure regular updating of firmware and software.  IT Staff will develop, implement, and enforce password requirements on Swisher networks.  IT Staff will ensure administrative accounts are not connected to routers when these privileged accounts are not actively in use.  IT Staff will disable unused ports on network switches.  IT Staff will develop, implement, and enforce optimized port security settings on Swisher network switches.  IT Staff will implement anti-malware software to secure Swisher switches.  IT Staff will implement anti-malware software to secure Swisher access points. |
| Human actors using physical access | IT Staff will implement and enforce policies that will timely remove all access of terminated employees to desktop workstations.  IT Staff will implement and enforce screen saver policies on desktop workstations.  IT Staff will implement and enforce application control policies on laptops.  IT Staff will implement and enforce restricted personal use policies on laptops.  IT Staff will timely remove terminated employee’s access to laptops.  IT Staff will implement and enforce screen saver policies on laptops.  IT Staff will update and maintain accurate documentation and tracking of external hard drives.  IT Staff will maintain accurate documentation of all data and software stored and managed on external hard drives. |
| System problems | IT Staff will ensure regular updates to software and firmware of swisher systems and will develop, implement, and enforce policies to regularly test and maintain software and hardware for defects.  IT Staff will ensure anti-malware software is effectively implemented to secure Swisher systems. Data stored and data in transit will be encrypted and managed on a secure environment to minimize risk of malware threat actors. |
| Other problems | Not Relevant |
| Measures | ATE training will be documented and records will include information including date, time, personnel attending, topics covered, educator information, and certification fulfillment or failures to complete training.  Password requirements will meet with regulatory compliance and security best standards, or whichever is stronger.  Screen Savers will activate after 5 minutes of inactivity.  All system activities will be monitored and logged and personal activity on workstations will alert IT Staff.  IT Staff will update firmware and software on Swisher systems when they become available and are tested to ensure interruptions to services do not occur or no later than 1-month after they are available. |

## A8.3e | Create Mitigation Plans

| Network Access and Use | |
| --- | --- |
| **Threat Type** | **Actions** |
| Human actors using network access | IT Staff will configure and enforce SSL protocols or equivalent encryption protocols on Swisher data servers.  IT Staff will develop, implement, and enforce password requirements on Swisher data server.  IT Staff will enable and monitor Swisher data servers to ensure regular updating of firmware and software.  IT Staff will enable and monitor Swisher routers to ensure regular updating of firmware and software.  IT Staff will develop, implement, and enforce password requirements on Swisher networks.  IT Staff will ensure administrative accounts are not connected to routers when these privileged accounts are not actively in use.  IT Staff will disable unused ports on network switches.  IT Staff will develop, implement, and enforce optimized port security settings on Swisher network switches.  IT Staff will implement anti-malware software to secure Swisher switches.  IT Staff will implement anti-malware software to secure Swisher access points. |
| Human actors using physical access | IT Staff will implement and enforce policies that will timely remove all access of terminated employees to desktop workstations.  IT Staff will implement and enforce screen saver policies on desktop workstations.  IT Staff will implement and enforce application control policies on laptops.  IT Staff will implement and enforce restricted personal use policies on laptops.  IT Staff will timely remove terminated employee’s access to laptops.  IT Staff will implement and enforce screen saver policies on laptops.  IT Staff will update and maintain accurate documentation and tracking of external hard drives.  IT Staff will maintain accurate documentation of all data and software stored and managed on external hard drives. |
| System problems | IT Staff will ensure regular updates to software and firmware of swisher systems and will develop, implement, and enforce policies to regularly test and maintain software and hardware for defects.  IT Staff will ensure anti-malware software is effectively implemented to secure Swisher systems. Data stored and data in transit will be encrypted and managed on a secure environment to minimize risk of malware threat actors. |
| Other problems | Business continuity and recovery procedures should be developed to allow for continued production or resumption of normal production following the event ISP, power failure, hardware failure, software failure, or any other issues that may cause temporary network outages or network outages that last longer than 5 minutes. |
| Measures | ATE training will be documented and records will include information including date, time, personnel attending, topics covered, educator information, and certification fulfillment or failures to complete training.  Password requirements will meet with regulatory compliance and security best standards, or whichever is stronger.  IT Staff will update firmware and software on Swisher systems when they become available and are tested to ensure interruptions to services do not occur or no later than 1-month after they are available. |

## A8.4 | Create Action List

| Action List | |
| --- | --- |
| **Action Item** | **Information** |
| * IT Staff will configure and enforce SSL protocols or equivalent encryption protocols on Swisher data servers. * IT Staff will develop, implement, and enforce password requirements on Swisher data server. * IT Staff will enable and monitor Swisher data servers to ensure regular updating of firmware and software. | *Responsibility:* IT Staff  *Completion date:* Within 30 Days  *Required management actions:* Ensure the development, implementation, and enforcement of policies for security protocols, passwords, and regular updates on Swisher servers. |
| * IT Staff will enable and monitor Swisher routers to ensure regular updating of firmware and software. * IT Staff will develop, implement, and enforce password requirements on Swisher networks. * IT Staff will ensure administrative accounts are not connected to routers when these privileged accounts are not actively in use. * IT Staff will disable unused ports on network switches. * IT Staff will develop, implement, and enforce optimized port security settings on Swisher network switches. | *Responsibility:* IT Staff  *Completion date:* Within one week, no later than 30 days.  *Required management actions:*  Ensure the development, implementation, and enforcement of policies for security protocols, passwords, and regular updates on Swisher network components. |
| * IT Staff will implement anti-malware software to secure Swisher switches. * IT Staff will implement anti-malware software to secure Swisher access points. | *Responsibility:* IT Staff  *Completion date:* Complete within 30 days  *Required management actions:* Ensure a current budget is maintained to ensure licensing for anti-malware is available. |
| * IT Staff will implement and enforce policies that will timely remove all access of terminated employees to desktop workstations. * IT Staff will implement and enforce screen saver policies on desktop workstations. | *Responsibility:* IT Staff  *Completion date:* Complete within 30 days  *Required management actions:* Management should follow and check-in with IT Staff to ensure all policies implemented and enforced by Swisher to advocate and promote shareholder buy-in and compliance. |
| * IT Staff will implement and enforce application control policies on laptops. * IT Staff will implement and enforce restricted personal use policies on laptops. * IT Staff will timely remove terminated employee’s access to laptops. * IT Staff will implement and enforce screen saver policies on laptops. | *Responsibility:* IT Staff  *Completion date:* Complete within 30 days  *Required management actions:* Management should follow and check-in with IT Staff to ensure all policies implemented and enforced by Swisher to advocate and promote shareholder buy-in and compliance. |
| * IT Staff will update and maintain accurate documentation and tracking of external hard drives. * IT Staff will maintain accurate documentation of all data and software stored and managed on external hard drives. | *Responsibility:* IT Staff  *Completion date:* Complete within 30 days  *Required management actions:* Nothing |

# Conclusion

In conclusion, the security professionals conducting this OCTAVE will identify the assets, relative priorities, security requirements, and knowledge of current security strategies and known vulnerabilities from each department of Swisher Manufacturing. Each department identified for interview and analysis are Senior Management, Operational Area Management, Operational Staff, and IT Staff. The systems that were identified within Swisher are Administrative, Human Resources, Accounting, Lab (Research and Development), and Production. The staff included in this OCTAVE process include President and CEO, V.P. of Sales – North America, Site Manager, Plant Production Manager, Site Safety Manager, Engineering Manager, Site Accounting Manager, Site Human Resources Manager, secretary to the site manager, Inventory Planning and Purchasing Agent, Production Engineer, Production Worker, and System Administrator. Next, the OCTAVE process identified Intellectual Property and Proprietary Information, legal and regulatory compliance protected information such as PII and financial data, operational critical data such as software and hardware profile, and schedule data, accounting and order processing systems, and the Swisher network as critical assets and systems of interest to conduct this OCTAVE assessment. Critical infrastructure was identified and includes Swishers data server, anti-malware software, external hard drives, desktop workstations, laptops, and network components. An approach to addressing possible vulnerabilities was detailed including information on what to conduct an audit for and an evaluation and development of necessary actions and recommendations to consider for addressing them was provided. Additionally, OCTAVE will identify impacts of these threats to Swishers critical assets and analysts will help identify levels of impact based on Swisher’s security, financial, and operational needs. A review of surveys and threat trees was conduct and identified vulnerabilities and protection strategies to produce mitigation plans and action lists for Swisher to improve security posture and mitigate risks to its critical assets.