**Addressing De Nile’s Compliance Responsibilities**

Team 2

IT 472 IT Compliance

City University of Seattle

School of Technology and Computing

Richard Baker, Fernando McKenzie, Jammie Steele

Bachelor of Information Technology, Bachelor of Information Technology, Bachelor of Cyber Security

[Mckenziegoodenferna@cityuniversity.edu](mailto:Mckenziegoodenferna@cityuniversity.edu), [barkerrichard@cityuniversity.edu](mailto:barkerrichard@cityuniversity.edu), [steelejammie@cityuniversity.edu](mailto:steelejammie@cityuniversity.edu)

**Abstract**

Priority ONE Solutions will exert a great deal of effort over the course of ten weeks in order to develop a comprehensive solution for our client, De Nile. This solution will include but is not limited to, the creation of efficient internal control for De Nile's systems. The development of this solution will require a lot of hard work. If De Nile does this, it will have a better understanding of the risks it is taking and the dangers it confronts from both within the company and from outside. It will be Priority ONE's responsibility to carry out risk assessments, during which we will search for potential hazards both within and beyond the organization and figure out ways to reduce or do away with these hazards. Priority ONE Solutions will be of assistance to De Nile in achieving its purpose and goals, as well as achieving full compliance with all of the most recent industry standards and all of the rules and guidelines that are now in effect. Priority One is to set up a compliance process program that will help De Nile understand the requirements and controls of the different frameworks (such as COBIT, ISO, NIST, PCI DSS, SOC, and SOX), take stock of their own internal controls and security measures, and then take steps to fix or change any broken controls or procedures.

**Keywords:** Compliance, Internal Control, COBIT, ISO, NIST, PCI DSS, Family of Risk

**Introduction**

PriorityONE solutions is committed to achieving compliance in the ever-evolving scope of government regulations, as well as working with, developing, and employing the systems sought out by DeNile. In order to meet the standards of today, to stay within regulation of today’s best practices, and to ensure safety standards for both the consumer and the company, PriorityONE Solutions finds it best to work towards and maintain COBIT 2019 Framework

standards, as well as integrating the five NIST functions for additional protection and regulation. The development, implementation, and integration of a working credit card system

implemented upon the DeNile retail platform should be thoroughly scrutinized as to make sure that customers, the company, and auditors feel confident in the solutions that we have created, which is why PriorityOne Solutions works towards exceeding the PCI DSS standards

In order to provide confidence in our product, PriorityOne Solutions would proceed with COBIT 2019 and ensure that all its principles are being met. Working to assure that the company is being delivered a viable, safe product, working product that also satisfies consumers interests and stakeholders needs. We would also work in tandem with DeNile, integrating all the information technology within the company to make sure that the rollout of our credit card implementation is not only synergistic, but to ensure that standards are being met uniformly. Through the complementation of the proprietary DeNile systems and our implementation of the credit card system, we can ensure that our combined vision for providing customers with a great service and pleasing shareholders is met.

**Government Standards – Sarbanes-Oxley Act of 2002**

Governance of IT is a formal framework that provides structure for organizations to ensures IT investments are supporting best business practices (Lindor, cio.com). These frameworks have been influenced by the creation and passing of the Sarbanes-Oxley Act (SOX). The Sarbanes-Oxley Act was created in response to scandals from the early 2000s, so that the auditing process was detailed and outlined, and so that there is public disclosure as to what is going on with a company’s internal procedures to give peace of mind to its investors, as well as its consumers and customers. There are four main internal controls that a company should focus on in order to be SOX compliant. Access, rather, the securing of all digital and electronic access points, Security by demonstrating resilience to data breach attempts, the recording and retention of a company’s data, and being able to respond swiftly to software and data changes impacting record.

PriorityONE solutions is committed to being compliant in the ever-evolving scape of government regulations, as well as working with, developing, and employing the systems sought out by DeNile. In order to meet the standards of today, to stay within regulation of today’s best practices, and to ensure safety standards for both the consumer and the company, PriorityONE Solutions figures it best to work towards and maintain COBIT 5 Framework standards, as well as integrating the five NIST functions for additional protection and regulation. The development, implementation, and integration of a working credit card system implemented upon the DeNile retail platform should be thoroughly scrutinized as to make sure that customers, the company, and auditors feel confident in the solutions that we have created, which is why PriorityOne Solutions works towards exceeding the PCI DSS standards

Utilizing COBIT 5 is a boon in the compliance domain, not only because it is Sarbanes-Oxley compliant, but also because it can work in tandem with other IT governance frameworks. As stated before, with DeNile wanting to incorporate credit card utilization onto their website, the NIST framework would also be a framework to be utilized for the protection of the business and its consumers. Implementing a list of all equipment being used for the company and assigning roles and hierarchies will enforce a standard that will make sure that no abuse of data, whether purposeful or accidental, is happening. It also ensures and encrypts data across the board, making sure that if there is foul play, the companies’ data will not be easily accessible, and can be easily identified as to who the malicious actor could be. The NIST framework would also attempt to keep DeNile and its workers active and informed, by teaching them to scout out any detrimental circumstances as well as how to perform in a situation should the companies’ sensitive data be compromised.

Another way that PriorityOne Solutions works to mitigate data being breached, and maintaining stakeholder and consumer interests, is also to implement PCI compliance. The Payment Card Industry Data Security Standard is a set of requirements mandated to maintain security amongst payment card transactions. We hope to achieve compliance with PCIDSS in order to mitigate any potential infractions sustained with the implementation, as PCI DSS compliance could be observed to be in line with COBIT 5 and NIST framework standards.

**Industry Standards – PCI DSS**

The Payment Card Industry Security Standards Council establishes the technical and operational requirements known as PCI security standards in order to safeguard the information of cardholders. All merchants and organizations around the world that store, process, or transfer this data are subject to these worldwide standards, which also include additional requirements for the software developers and manufacturers of apps and devices used in those transactions. American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. are the five major payment card companies that were responsible for establishing the Payment Card Industry Council and make it a requirement for their respective stakeholders to comply with the PCI set of standards. For this project we will explain in detail the PCI DSS (Payment Card Industry Data Security Standard) which refers to any business that handles credit card information in any way. Everything that is a part of the system that is technically related to cardholder data is covered. All company must adhere to the PCI DSS if it deals with credit card processing or acceptance.

**List of Principles**

* Build and maintain a secure network and systems
* Protect cardholder data
* Maintain a vulnerability management program
* Implement strong access control measures
* Regularly monitor and test networks
* Maintain an information security policy

**PCI DSS 1**: **Install and maintain a firewall configuration to protect cardholder data**

A firewall is a form of access control system that creates a barrier around the network of your company, preventing unauthorized users from gaining access to the data contained within the network. In a nutshell, firewalls provide the function of a barrier. Also set up firewalls inside of your network to protect particularly sensitive data and limit access for different groups or people that are already a part of the organization. After all, not every single member of the workforce or staff will need access to the information about cardholders. This PCI DSS standard also describes how to arrange routers to secure cardholder data on the internal networks. The IT team should continuously monitor the traffic on the firewall, evaluate the configurations of the routers every six months, and update them as needed to comply with the standard.

**PCI DSS 2: Do not use vendor-supplied defaults for system passwords and other security parameters**

Operating systems, servers, firewalls, and other security features have default usernames and passwords. They're easy to guess and could be shared online. This criterion supports industry best practices like NIST password recommendations - users who create accounts to access applications shouldn't be supplied a default password. If DeNile is PCI DSS and NIST compliant, you're good. A hacker or cybercriminal can easily cycle through default passwords to access employee or customer details. PCI DSS recommends removing "any unneeded default accounts before installing a system on the network" to prevent users from using default passwords to access cardholder data.

**PCI DSS 3: Protect stored cardholder data**

In accordance with this rule, no cardholder information may be kept on file unless doing so is required for a legitimate business purpose. If cardholder data must be stored, you must take the following precautions:

1) Keep it for no longer than necessary. 2) Delete old records once a quarter.

3) Make all authentication data unintelligible by encrypting it and "masking" it on display (by revealing only the first or last four digits of the Primary Account Number).

4) Keep track of and secure all encryption keys and tools.

**PCI DSS 4: Encrypt transmission of cardholder data across open, public networks**

It may be more difficult to verify that cardholder data is not compromised while being transmitted via open, public networks, despite the fact that a firewall can assist in keep cybercriminals out of all internal networks. The Payment Card Industry Data Security Standard (PCI DSS) requires all businesses to use measures to encrypt sensitive customer information before it is transmitted or stored. Before a skilled hacker can decrypt the data, the IT administrator has time to take precautions and recover it using encryption.

**PCI DSS 5: Protect all systems against malware and regularly update anti-virus software or programs**

All on-premises computers, as well as mobile and remote devices used by employees, should be equipped with anti-virus software to protect against harmful software (malware). The fifth condition is vigilant monitoring of the ever-evolving malware landscape to stay abreast of new threats and ensure that all necessary systems have anti-malware protection.

**PCI DSS 6: Develop and maintain secure systems and applications**

A risk management strategy for finding vulnerabilities, installing security updates, prioritizing risks, and the order of security actions is fundamentally outlined by PCI DSS requirement 6, which is the sixth requirement in the standard. This criterion requires that security measures must be performed during every stage of the software development process, beginning with the coding stage and continuing all the way through the process of deploying patches to vulnerabilities.

**PCI DSS 7: Restrict access to cardholder data by business need-to-know**

Only those employees who absolutely need to know cardholder data for company operations should have access to that data; this need dictates that employee access be totally restricted as the default setting. This requirement can correspond with your identity and access management methodology. As soon as a user is terminated, changes roles, or quits the firm, access controls should be set as quickly as possible. User roles should also be clearly specified.

**PCI DSS 8: Identify and authenticate access to system components**

In order to comply with Requirement 8, all users who have access to cardholder data must have a unique ID that can be used to track and monitor their movements and any time they log in. Authentication tools (keys, cards, or multi-factor authentication software) should be assigned to individual users, and each user should create a strong password (consider following NIST password rules). The purpose of this rule is to prevent any unauthorized access and make it simple to identify who is responsible for any misdeeds. Requirement 8 can aid in the prevention of internal fraud and the identification of instances where a user's login information may have been compromised by working in tandem with audit logs and audit trails.

**PCI DSS 9: Restrict physical access to cardholder data**

In order to protect customers' credit card information when it is being sent over the network or stored locally, merchants must comply with Requirement 9. Employees who collect a physical card payment must have physical identity, and access to areas where onsite people will be handling cardholder data must be restricted, as discussed in Requirement 7 and Requirement 8. In addition, paper receipts and electronic records containing cardholder data should be rendered unreadable and stored in a safe place.

**PCI DSS 10: Track and monitor all access to network resources and cardholder data**

Guidelines for logging, tracking, and monitoring all user activities are provided in Requirement 10. By maintaining audit logs and audit trails, your IT administrators will be able to spot unusual login behavior that may indicate a hacker is attempting to gain access to cardholder data through compromised credentials. Audit logs and trails should be automated and checked by administrators with limited rights; they should also include user identification, date, and time. This rule also mandates that audit trail information be stored for a minimum of one full year, with the most recent three months' worth of data readily available for inspection. Errors and data breaches can be prevented, and their sources can be identified if audit trails are kept in pristine form.

**PCI DSS 11: Regularly test security systems and processes**

Changing any aspect of the system, even something as seemingly innocuous as a firewall or router setting, can open it up to previously unseen threats. So, even if you do everything by the book with PCI DSS, you can still be putting yourself at danger if you aren't using the most up-to-date security measures. Specific instructions for doing vulnerability scans and penetration testing are outlined in great depth in Requirement 11. This section also includes important contextual information like timetables and schedules. Scanning and testing on a regular basis is crucial for ensuring that the correct security fixes and updates are applied, as new software and malware attacks might present previously undisclosed vulnerabilities.

**PCI DSS 12: Maintain a policy that addresses information security for all personnel**

Because of this requirement, PCI DSS is an important part of IT governance. It talks about training employees, reducing risks, and making a strong security policy that everyone in the company follows. This policy should be written down and given to all employees who need to know about it. PCI DSS says that it should be reviewed "at least once a year." The organization should also plan regular risk assessments (again, "at least once a year") to keep the policy up to date. PCI DSS-compliant businesses should also limit employee misuse and set up internal controls to stop fraud. They can do this by interviewing potential employees, making and distributing usage policies for technologies used to send, store, or access cardholder data, such as computer hardware, email, browsing the web, and messaging, and giving all employees "security awareness" training.

**Design and Implementation of the Management Framework**

Using the guidelines laid out in the COBIT 2019 governance framework, a series of policies and controls can be established to ensure compliance with all industry and government standards. COBIT is designed to be a comprehensive governing framework using a risk-based approach to ensure that all stakeholder’s needs are met. Applying a governing framework is important in IT management, especially when handling PPI and customer financial information. This section will cover the policies, procedures, and controls that will be implemented to ensure compliance with applicable standards. The three areas that will be addressed will be compliance with government standards, industry standards and internal goals. This will require following the requirements in the Sarbanes-Oxley Act and PCI DSS standards set by industry leaders in the payment card field.

**Phase 1-What are the Drivers?**

* Identify current governance context, pain points, events, and symptoms that will trigger a response.
* Identify the business and governance drivers and compliance requirements for improving the enterprise governance of IT (EGIT).
* Identify business priorities and business strategy dependent on IT.
* Align with enterprise policies, strategies, and principles.
* Raise executive awareness of IT’s importance and the value of EGIT.
* Define EGIT policy, objectives and principles
* Ensure executives and board understand and approve the high-level approach and understand the consequences of not taking action on significant issues.

**Phase 2-Where are we now?**

* Identify key enterprise and supporting IT-related goals
* Establish the significance and nature of IT’s contribution (solutions and services) needed to support business objectives.
* Identify key governance issues and weaknesses related to contribution and the enterprise support needed to complete IT goals.
* Identify and select critical processes to support IT related goals.
* Assess risk related to critical IT processes.
* Identify and select processes to ensure that risk is avoided.
* Understand the risk acceptance position defined by management.
* Analyze current level of capability

**Phase 3-Where do we want to be?**

* Define targets for improvement
* Analyze gaps
* Identify potential improvements

By implementing these policies and procedures we can be assured that our IT systems will function effectively and provide the most value possible. Following this framework will ensure that DeNile’s risk profile is minimized. By using the highest security standards and a highly efficient system will provide DeNile’s clients with peace of mind that will improve growth and revenue. The client’s trust is vital to any company that handles financial transactions and information. This system will require regular assessment to ensure that DeNile remains compliant with an ever-changing threat landscape and regulatory environment.

**Immediate Considerations for PCI DSS Compliance**

***Letting the board know that keeping DeNile strictly online is the best thing due to cloud computing resources and compliance regulation its better as an online/ ecommerce platform and that opening a brick-and-mortar store is out of scope.***

Maintaining PCI compliance is not a once-and-done task; rather, it calls for constant work. You, as the shareholders of DeNile, are responsible for a significant portion of this work. When it comes to ensuring compliance, putting all of your attention on the annual review can give you a false sense of safety.

Once DeNile achieves compliance within the organization here are some considerations to keep compliance consistency:

* By segregating various systems, setting up firewalls, and prohibiting point-of-sale terminals from using the internet for any purpose other than processing payments, you may maintain the security of your computer networks.

* Both a vulnerability management program and regular security checks should be maintained. This program should include updating anti-virus software and checking for vulnerabilities on external networks.

* Monthly password updates should be required, and you should implement a rigorous policy that forbids staff members from divulging or discussing their personal passwords.

* Conduct system access audits and confirm that personnel only have the bare minimum of authorization needed to carry out their job duties.

* Provide staff with training on the payment card industry and the best data security procedures.

* Create and maintain a document outlining security policies and procedures, which should cover not only the details mentioned in the previous paragraphs but also additional safeguards for cardholder and payment information.

**Maintaining PCI DSS compliance**

We must remain vigilant to ensure that we maintain compliance with PCI DSS and all regulations. This will require a plan to monitor changes to regulations and threats the networks. To complete this task will establish a plan to audit security controls, changes to PCI DSS, and emerging threats.

The PCI SCC has established a series of recommendations to establish an approach and ongoing review process the service to support the organization’s continual compliance and reduce the risk of heart data compromise. The following eight principles are provided to help implement and maintain compliance PCI DSS:

1. Develop and Maintain a Sustainable Compliance Program- in order for the compliance program to be effective, it needs to be included in business-as-usual activities as part of the overall security strategy. The organization needs to monitor security control effectiveness in an ongoing manner and maintain compliance in between assessments. The security of cardholder data should be the primary objective behind all compliance activities, not just getting a passing report when the assessment is completed.
2. Develop Program, Policy, and Procedures-the PCI DSS compliance program needs to include the people, processes, and technology along with all supporting policies and procedures in order to guide behaviors and maintain business and operational processes.
3. Define Performance Metrics to Measure Success- using a comprehensive metrics program provides the company with useful data to see where potential risks are and to measure the effectiveness of security controls. This will allow the organization to direct its energy towards areas of need and minimize risk. The scope of data collected should be clearly defined and based on the specific needs, goals, and priorities of the business.
4. Assign Ownership for coordinating security activities- a specific management level individual should be assigned responsibility for maintaining compliance. This person will receive all information and data regarding the effectiveness of the compliance program and security controls, they will assign activities to other groups or individuals to ensure that goals are met. These activities might include ordination resources, project management, monitoring compliance, and cost. This person should be able to complete an objective risk reward assessment and communicate business needs to other management personnel.
5. Emphasize Security and Risk Management to Attain and Maintain Compliance- being in compliance with PCI DSS standards does not ensure the security of your data. PCI DSS provides a baseline control but should not be considered the only source for addressing security needs. The organization needs to prioritize protecting the data, infrastructure, and network assets by maintaining a comprehensive security policy and building a security focused culture. PCI DSS compliance will be achieved as a byproduct of implementing security policy and emphasizing the need to follow security policy.
6. Continuously Monitor Controls- strategies to continuously monitor, test, and document the effectiveness of security controls should be developed as part of security policy. This required ensuring that controls are in place and are properly implemented, while checking the efficiency and impact on risk management.
7. Detect and Respond to Control Failures- the company needs to have a process for recognizing and responding security control failures quickly. Any failure could be a security incident and require a more formal incident response as outlined in the security policy. Even if control failure is not a security incident even make sure the controls restored, determine the cause of the failure, and minimize the impact of the failure. Any control that has failed needs to be monitored closely to make sure that its future effectiveness is not impacted.
8. Maintain Security Awareness- more and more we are seeing social engineering attacks leading to data breaches, network damage, and other attacks like ransomware. This leads to the need for an effective program to train employees to recognize risks and report possible attacks. This program should be regularly updated to recognize the emergence of new threads and help maintain security culture in our company.

There are other measures needed to ensure the safety of our data besides these recommendations. Our company may rely on third-party service providers to provide equipment, software, or other resources. We must make sure that any of these vendors that have access to our networks or data are following our security policy. The effectiveness of our security policy can easily be compromised if one of the vendors is using lax security controls. All vendors should understand and be required to follow security and compliance programs in order to ensure compliance. We also need to make sure that our controls and policies evolved to consider changing business landscape, new or changing needs of the business, and take into account technological advancements. Our security policy goals, and security controls should always reflect the needs of the business. By following these recommendations and adhering to the spirit of compliance we minimize the risk to our company and clients.

**Payment Brands**

DeNile’s initial form of payments are Visa and Mastercard ONLY that will change in the future. Compliance with the Payment Card Industry Data Security Standard (PCI DSS) has been mandated by the payment brands (Visa, MasterCard, Discover, and American Express) for any and all businesses that process, store, or transfer payment cardholder data. The capacity to manage cardholder information is a feature that comes standard with a Merchant account. This standard addresses not only the POS (Point of Sale) and computer systems but also the secure processing of data as well as the physical handling of data.

**Transaction Volume**

At a level 3 which is 20k to 1 Million, DeNile Total annual transactions divided by 12 months equals a merchant's average monthly transaction volume. If a merchant has no processing history, they may be requested for an estimate. Processors may use monthly transaction volume to evaluate merchant risk. It can affect merchant account approval or denial. High transaction volume is a danger because every sale could be charged back, making the processor accountable. Some merchant accounts limit monthly transaction volume to reduce risk. The merchant must stay below a processor's monthly transaction limit. In the initial few months of processing, meeting the monthly barrier may be dangerous if many transactions are denied. If a merchant hits the volume maximum, the processor may perform a risk evaluation. The merchant account may be closed if the assessment shows potential liabilities. As a precaution, merchants may choose to set transaction thresholds below the processor's restrictions. Processors may require a merchant account reserve to offset liabilities.

**Merchant Level**

PCI compliance levels are assigned to businesses based on the number of card transactions (credit, debit, and prepaid) they handle annually. The compliance Standard that a store must meet may be raised if a security breach causes sensitive customer account information to be compromised.

The best way for merchants to determine their level of PCI compliance is to consult with their merchant services provider or use the reporting tools provided by their provider. Because of the scale and nature of their operations, Level 1-3 merchants are subject to compliance standards that are more difficult to fulfill. In addition to this, they are more likely to have IT and compliance teams working within the company to develop and monitor their compliance procedures.

The majority of retailers that classify themselves as either small or medium-sized firms are classified as level 4 businesses. In spite of the fact that the requirements for compliance may be simplified to some degree, these retailers frequently discover that it is more difficult to fulfill the standards since they lack an internal IT infrastructure.

**Level 1 merchants**

More than 6 million credit card transactions are processed by Level 1 retailers every year across all channels (card present, card not present, eCommerce). In addition, if a worldwide retailer processes more than 6 million transactions per year across all territories, that may be enough to qualify the entire company.

To qualify as a Level 1 vendor, businesses must:

* Submit a Report of Compliance (ROC) to a Qualified Security Assessor on a yearly basis (QSA)
* Employ a Recognized Scanning Company to do network scans every three months (ASV)
* To attest compliance, fill out the form.

**Level 2 merchants**

Across all sales channels, Level 2 retailers process between 1 and 6 million credit card transactions per year (card present, card not present, eCommerce.)

What Level 2 retailers must do:

* Participate in an Annual Self-Evaluation Survey (SAQ)
* Get an ASV scan of your network done once a quarter.
* Finalize the Attestation of Compliance Form.

**Level 3 merchants**

Level 3 shops handle anywhere from 20,000 and 1,000,000 in yearly credit card sales, all through electronic means.

The following are requirements for Level 3 retailers:

* Fill Out a SAQ Every Year
* Get an ASV scan of your network done once a quarter.
* Finalize the Attestation of Compliance Form.

**Level 4 merchants**

Level 4 retailers accept credit cards and debit cards in-store, over the phone, and online annually at a combined total of up to 1 million, with no one channel accepting more than 20,000. Alternatively, a Level 4 merchant is one who does less than 20,000 card transactions annually, regardless of channel.

The following are requirements for Level 4 retailers:

* Fill Out a SAQ Every Year
* Get an ASV scan of your network done once a quarter.
* Finalize the Attestation of Compliance Form.

**Types of reporting required (any type)**

Consumers, staff, and watchdog groups all adhere to a pretty consistent process when it comes to reporting any violations of PCI compliance. Getting in touch with the company or group that was responsible for the infraction is frequently the first step in the process. A significant proportion of individuals take the information that is presented in these reports extremely seriously and, as a general rule, will handle any issues that arise on their own. The vast majority of organizations can be contacted via the more traditional means of postal mail, as well as via the telephone and electronic mail.

The majority of organizations will report PCI compliance infractions to the credit card processor of the accused organization if the organization that committed the infraction does not reply or refuses to address the non-compliance. Even if they are unaware of which processor was accountable for the transaction, complainants are still able to file reports directly with Mastercard or Visa. Each of these companies provides support via e-mail, over the phone, and via live webchat for its customers.

Get in touch with the financial institution that issued your credit card if you have any reason to fear that the security of the information associated with your credit card may have been jeopardized as a result of a retailer's failure to comply with applicable requirements. Any specific issues relating to non-compliance can be addressed at that moment, when the old card has been deactivated and a new one has been issued. This is the earliest opportunity to do so.

**Implementation of an Integrated Internal Control System**

The development of Internal Control Systems may seem a tall task, however, given the COSO and COBIT 2019 frameworks that we have implemented throughout the creation and integration of the relationship between PriorityONE Solutions and DeNile, we at PriorityONE can utilize our already-established frameworks in order to denote the process for implementing these control systems. By employing these frameworks, as well as the PCI DSS standards, we can safely assume customer and consumer safety.

Establishing a baseline for the internal control system relies on the creation of preventative, detective, automated, and manual controls. With PriorityONE supporting DeNile in its consumer and customer-oriented ventures, we must plan for all unforeseen circumstances.

**Preventative Control Measures**

These measures are in place to prevent one singular entity from having too much unchecked authority and privilege over any and all areas of responsibility.

**Segregation of duties**

By clearly dividing responsibilities and duties, we can make sure that no one singular entity is dictating a department, or the entire company's directions, towards their own benefit.

**Authorization requirements to prevent improper use of university resources**

Developing a hierarchy of roles and responsibilities is important to make sure that no individual or entity can attempt to muscle their status into another area of responsibility. At no point in time should Human Resources demand to have access to customer transaction data, for example.

**Access Controls**

At any given time, no workstation should ever be unlocked, and free to roam around. By restricting access to workstations and terminals, we can ensure that only those who have been deemed responsible are given access with usernames and passwords, who have access and clearance to do so.

**Clear and Enforced Documentation and Record-keeping Procedures**

Record keeping documentation is important to maintaining footprints on employees and users who have access. With physical mediums, having a sign-in sheet/checklist for secure areas will ensure that anyone who is supposed to be there is actually there, and vice-versa. Digital mediums, being administrators receiving notifications any time there are failed attempts to log into a workstation/network, or a notification if there is a foreign network address attempting to log in to a workstation.

**Physical Control Over Assets**

Different departments having separate means of accessing certain proprietary information is important, at no time should there ever be a “master key” that would allow an individual to access everywhere, at any given time, without attaining permission.

Detective Control Measures

Detective control measures are created for finding any discrepancies that may have not been previously identified or encountered through preventative measures.

**Monthly reconciliations of departmental transactions.**

The detective control of reconciliation is the comparison of transactions, or events, from two different sets of data. An example could be trying to see if the remote log-in attempt event coincides with a C-level employee taking a business trip and attempting to check the company email, or if proposed budgets for allocating and preventing security breaches matches with the actual expenditure cost.

**Conducting physical asset counts.**

An effective measure in making sure that all physical means of accessing company data is secure. From making sure identification cards are secured across the board, to making sure that there are no missing workstations that aren’t accounted for.

Automated Control Measures

**Automated alerts can notify an admin of normal or notorious activity**

Having administrative personnel receiving alerts whenever a user is logging into a certain workstation normally or receiving a notification that a user has failed to log in properly after many attempts or receiving a log-in notification from an area that may be suspicious.

**Authentication measures**

There may be a common place for employees to work from, with unassigned workstations that can be used as long as a user has been given the clearance or authority to use said workstations, but not every user should have the ability to authorize or access what could be considered “restricted” transactions if they have not been bestowed the authority.

**Manual Control Measures**

Important or restricted areas, or the transference or retrieval of a physical control device, should be overseen by security officers. Only certain individuals allowed to attend certain areas or be given access to certain items that could be potentially harmful if given to the wrong person.

The integration of all of these control measures being implemented with DeNile will result in the creation of a solid internal control system, and with strict guidelines, the upkeep of industry standards, and proper maintenance amongst systems used, we at PriorityONE are hoping to propel DeNile into the forefront of the online sale industry. However, the frameworks of COSO and COBIT won’t be the only implementations used. Due to the nature of online sales, we have to keep the customers safeties in mind, and incorporate safeguards for their protection based upon the PCI DSS. A good many of these standards are implemented within the control system, such as using custom security parameters for logins (PCI DSS 2) and restricting cardholder data by need-to-know entities, secured by protected locations (PCI DSS 6 and PCI DSS 9) by differentiating different echelons of access and identifying select personnel.

Having a table or other visual assistance with several standards and frameworks might be useful when creating an integrated internal control system (see figure 1). A checklist is one possible format for this. For starters, it's not easy to create an effective internal control system without first having a thorough understanding of the business and how it runs. It's easier for the business and its consumers to exert influence over the system when they have multiple options for doing so. An integrated internal control system is useful for a business owner who wants the assurance that comes from knowing everything is running as it should but who does not have the time or resources to personally oversee every aspect of the operation that has to do with the internal controls. Using a system that incorporates many frameworks and security approaches is one of the most effective ways to achieve this goal.

**Conclusion**

Maintaining compliance with industry and government standards is vital to the continued operations of the DeNile corporation. These rules and regulations are in place to protect consumer's data, company secrets, and business practices. There could be disastrous consequences if the breach were to occur or if the company was found to be out of compliance. The federal government passed the SOX act in 2002 due to the financial shenanigans of companies like Enron and WorldCom. These companies use deceptive accounting and reporting practices that led to the loss of millions of dollars that led to a huge public backlash, forcing Congress to act. This new law places much stricter auditing and reporting rules that are supposed to make companies' financial situation clearer to investors.

There are significant consequences to violating the Sox act, executives that violate these laws can face up to $5 million in fines and 20 years in prison. PCI DSS is an industry-based standard set forth by the major credit card companies that establishes another set of rules that companies need to follow when accepting payments using payment cards. PCI DSS lays out much more detailed and complex guidelines that are intended to provide further protection for consumers and reduce liability for businesses. Violations of PCI DSS can lead to monthly penalties ranging from $5000-$100,000 from the payment card companies. There are several frameworks that guide businesses towards compliance like COBIT 2019 and COSO. Maintaining a secure and transparent environment also protects the business from other risks. If a data breach occurs DeNile could face millions of dollars in losses, lawsuits from affected consumers, and significant damage to public reputation. By following this plan in maintaining future compliance the company can significantly reduce risk or minimize the damage in a worst-case scenario.

**9.** **REFERENCES**

FisGlobal. (2019, July 30). *What you need to know about PCI compliance levels - insights: Worldpay from FIS*. FIS Global. Retrieved September 4, 2022, from <https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/what-you-need-to-know-about-pci-compliance-levels>

Galligan, M. E., & Rau, K. (2015, January). *COSO in the cyber age - Deloitte*. Retrieved July 22, 2022, from <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-coso-in-the-cyber-age-final-01292015.pdf>

Irwin, L. (2022, January 18). *A guide to the 4 PCI DSS compliance levels*. IT Governance Blog. Retrieved September 4, 2022, from <https://www.itgovernance.eu/blog/en/a-guide-to-the-4-pci-dss-compliance-levels>

Lindros, K. (2017, July 31). *What is it governance? A formal way to align IT & business strategy*. CIO. Retrieved August 21, 2022, from <https://www.cio.com/article/272051/governanceit-governance-definition-and-solutions.html>

Orbus. (2021). *COBIT 5 principle 2: Covering the enterprise end to end*. Retrieved August 21, 2022, from <https://www.orbussoftware.com/resources/video/video/cobit-principle-2-covering-the-enterprise-end-to-end#:~:text=This%20is%20what%20we%20mean,views%20and%20developments%20in%20governance>

PCI. (2018, July). *PCI DSS v3.2.1 quick reference guide - PCI security standards council*. Retrieved August 15, 2022, from https://www.pcisecuritystandards.org/documents/PCI\_DSS-QRG-v3\_2\_1.pdf

PCI. (2008). *Payment card industry security standards*. Retrieved August 15, 2022, from <https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf>

PCI. (2013, January). *PCI DSS e-commerce guidelines - PCI security standards council*. Retrieved August 15, 2022, from <https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_eCommerce_Guidelines.pdf>

PCI. (2019, January). *Best practices for maintaining PCI DSS compliance*. Retrieved August 15, 2022, from <https://www.pcisecuritystandards.org/documents/PCI_DSS_V2.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance.pdf>

RSI Security. (2022, March 30). *How to report PCI compliance violations*. RSI Security. Retrieved September 5, 2022, from <https://blog.rsisecurity.com/how-to-report-pci-compliance-violations/>

Staff, the P. N. O., & Staff, D. P. I. P. and C. T. O. (2021, November 9). *Understanding the NIST cybersecurity framework*. Federal Trade Commission. Retrieved August 21, 2022, from <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework>

Weiss, M. (2016). *Auditing IT infrastructures for compliance*. Jones & Bartlett Learning.

*What is Sox Compliance? 2022 requirements, controls and more: Upguard*. RSS. (n.d.). Retrieved August 21, 2022, from <https://www.upguard.com/blog/sox-compliance>

Wright, D. (2017, June 7). *Transaction volumes and merchant level*. PCI Compliance Guide. Retrieved September 4, 2022, from <https://www.pcicomplianceguide.org/how-are-transaction-volumes-calculated-to-determine-merchant-level/>

Zhao, J. (2022, May 5). *How to develop internal controls to mitigate IT security risks*. Hyperproof. Retrieved July 22, 2022, from <https://hyperproof.io/resource/internal-controls-and-data-security/>

Appendix

Figure 1.

**Table COSO-PCI Alignment**

**COSO**

|  |  |
| --- | --- |
| **Internal Control Component** | **Principles** |
| **Control environment** | **1. Demonstrate commitment to integrity and ethical values**  **2. Ensure that board exercises oversight responsibility**  **3. Establish structures, reporting lines, authorities and responsibilities**  **4. Demonstrate commitment to a competent workforce**  **5. Hold people accountable** |
| **Risk assessment** | **6. Specify appropriate objectives**  **7. Identify and analyze risks**  **8. Evaluate fraud risks**  **9. Identify and analyze changes that could significantly affect internal controls** |
| **Control activities** | **10. Select and develop control activities that mitigate risks**  **11. Select and develop technology controls**  **12. Deploy control activities through policies and procedures** |
| **Information and communication** | **13. Use relevant, quality information to support the internal control function**  **14. Communicate internal control information internally**  **15. Communicate internal control information externally** |
| **Monitoring** | **16. Perform ongoing or periodic evaluations of internal controls (or a combination of the two)**  **17. Communicate internal control deficiencies** |

**PCI DSS**

|  |  |
| --- | --- |
| **Build and maintain a secure network** | **Install and maintain a firewall configuration to protect cardholder data**  **Do not use vendor-supplied defaults for system passwords and other security parameters** |
| **Protect cardholder data** | **Protect stored cardholder data**  **Encrypt transmission of cardholder data across open, public networks** |
| **Maintain a vulnerability management program** | **Use and regularly update anti-virus software or programs**  **Develop and maintain secure systems and applications** |
| **Implement strong access control measures** | **Restrict access to cardholder data by business need to know**  **Assign a unique ID to each person with computer access**  **Restrict physical access to cardholder data** |
| **Regularly monitor and test networks** | **Track and monitor all access to network resources and cardholder data**  **Regularly test security systems and processes** |
| **Maintain an information security policy** | **Maintain a policy that addresses information security for all personnel** |