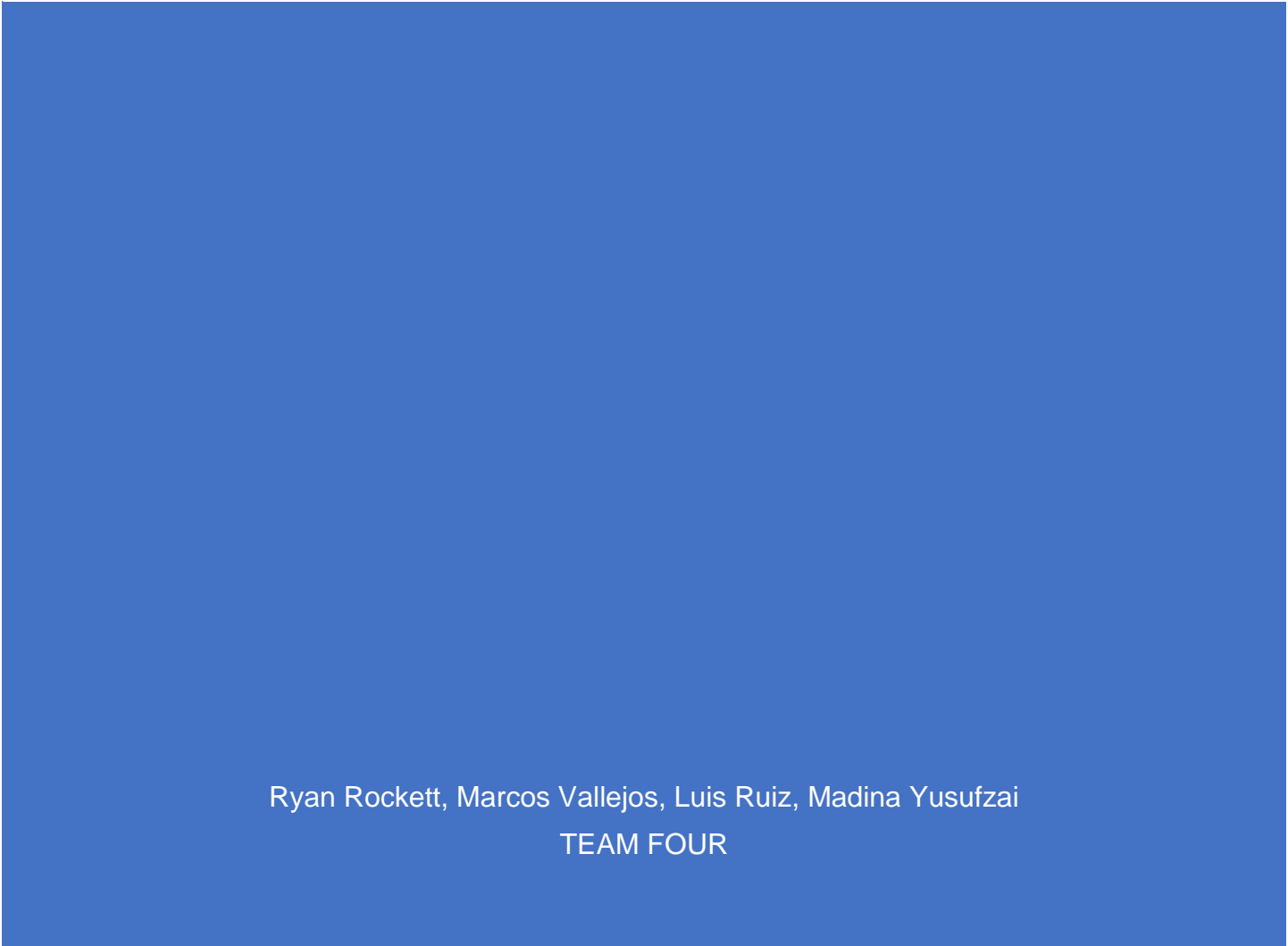




DESIGN OF AN INTEGRATED INTERNAL CONTROL SYSTEM



Ryan Rockett, Marcos Vallejos, Luis Ruiz, Madina Yusufzai
TEAM FOUR

Contents

Introduction	2
COSO Framework Overview.....	2
Internal Controls:	5
Other Frameworks and Standards	9
Integrated Internal Control System Goals Based on PCI-DSS Compliance.....	11
Conclusion.....	13
Works Cited:.....	15

Introduction

The success of a companies in the modern age isn't solely dependent on having the best prices and a high point of sales, there is also name recognition. Customers are smart enough to not only research the product but the company they are buying from as well before they make their purchase. Therefore, reliable companies like Amazon, eBay and Wayfair have gained so much success, not only can they provide their products with a price advantage, but customers are assured that their products are a legitimate purchase, and their data will be secure. An eCommerce company without a strong culture of cardholder data that cannot live up to customer expectations both with delivering their product and protecting their data will never receive name recognition. To become a sustainable and successful eCommerce retailer, S&H Aquariums must take due care to protect cardholder data by using an integrated system which will not only protect S&H Aquariums from audits but also their brand and reputation. The first step towards this goal will be to understand the COSO Framework and its internal control components but also how other frameworks can be integrated to provide the best possible assurance of security.

COSO Framework Overview

The COSO (Committee of Sponsoring Organizations of the Treadway Commission) is a committee composed of representatives from five organizations: American Accounting Association, American Institute of Certified Public Accountants, Financial Executives International, Institute of Management Accountants, and Institute of Internal Auditors. The COSO board develops guidance documents that help

organizations with risk assessment, internal controls, and fraud prevention. The COSO framework is divided into five internal control components with 17 principles that explicitly describe the elements of an effective system of internal controls.

The COSO framework divides internal control objectives into three categories:

Operations – highlights performance goals and securing the organization’s assets against fraud and focuses on the effectiveness and efficiency of your business operations.

Reporting – highlights both internal and external financial reporting as well as non-financial reporting, relate to transparency, timeliness and reliability of the organization’s reporting habits.

Compliance – highlights internal control goals based around adhering to laws and regulations the organization must comply with. The COSO framework lists the following

Internal control component	Principles
Control Environment	<ol style="list-style-type: none">1. Demonstrate commitment to integrity and ethical values2. Ensure that board exercises oversight responsibility3. Establish structures, reporting lines, authorities, and responsibilities4. Demonstrate commitment to a

	<p>competent workforce</p> <p>5. Hold people accountable</p>
Risk Assessment	<p>6. Specify appropriate objectives</p> <p>7. Identify and analyze risks</p> <p>8. Evaluate fraud risks</p> <p>9. Identify and analyze changes that could significantly affect internal controls</p>
Control Activities	<p>10. Select and develop control activities that mitigate risks</p> <p>11. Select and develop technology controls</p> <p>12. Deploy control activities through policies and procedures</p>
Information and Communication	<p>13. Use relevant, quality information to support the internal control function</p> <p>14. Communicate internal control information internally</p> <p>15. Communicate internal control information externally</p>
Monitoring	<p>16. Perform ongoing or periodic evaluations of internal controls</p> <p>17. Communicate internal control deficiencies</p>

Internal Controls:

These internal controls will create the process that S&H Aquariums will use to realize the three control objectives previously mentioned as well as maintaining compliance with laws, policies and regulations and maintaining personal business objectives. The five control components are deliberately broad so that it becomes easier for organizations such as S&H Aquariums to adapt it into their security culture. Additionally, they also provide a sufficient measure of assurance which is emboldened by a constant and ongoing process of maintaining securities. All five components and their principles were designed to be relevant in the present and to also be functioning in relevance in the future. The controls are also meant to perform in an integrated system and operate together to reduce the shortcomings that are present in the company.

The Control Environment:

This component creates the basis and the foundation upon which internal controls will be accomplished and integrity will be maintained throughout S&H Aquariums. The first principle unveils the ethical values that company, from top to bottom, will follow and has established the Standards of Conduct which are to be adhered. This will create an ethical workplace and culture and will hopefully target fraudulent or unethical behaviors that can compromise the longevity of the company. The second principle will create a dynamic in which the board of directors have their

duties separated from management. These directors will then have established responsibilities that include oversight over internal controls. This will target any conflicts of interest that could result in the shared responsibilities of a role constituting as a director and management. The third principle will establish the authoritative role of a director and the responsibilities of management as they establish the structure that the company will follow such as, reporting lines and the assignment and limitations of authority and responsibility. This is crucial so that there remains a clear chain of command that employees can follow when an incident occurs and that they know who to report to as an authority figure. The fourth principle sets up the training policies and practices to develop their employees for success and retain them. Without a standardized and trained workforce S&H Aquariums is liable that employees will be unqualified to maintain the internal controls, this principle resolves those concerns. Finally, the fifth principle will hold individuals accountable to the responsibilities of their position. This will not only include disciplinary actions if an internal control is not adhered to but also clarifies the expectations set forth by them and incentives individuals to achieve their objectives.

The Risk Assessment:

Principle six will identify and define the objects of internal controls in a clear and concise manner. These will include the Operational, Reporting and compliance objectives and the methods to achieve them such as through the guiding the company on how to manage the legalities and regulations to stay compliant with applicable laws. The seventh principle will identify the internal and external risk factors that the company will face. It will also determine the likelihood of occurrence, severity and the how

management should respond to the risks. The eight principles will target fraudulent behavior which could negatively impact the company, such as the behaviors demonstrated by Enron. This principle will give guidance on how to prevent or combat fraud through reviewing the incentives and compensation that a company gives which can lead to fraudulent financial reporting. Lastly, the ninth principle will guide the company on how to access the external and internal changes that contribute to risk. These can include on how to access new hacking techniques, new laws such as the GDPR and new technologies that can increase or reduce the security of the internal controls.

The Control Activities:

These activities are the implemented actions that the company will take to contain the risks identified in the risk assessment component. The tenth principle would consider the risks specific to S&H Aquariums and how they can be mitigated, and example of this would be by identifying how credit card information is stored and how to prevent a breach. The eleventh principle is the designation of information and technology tools to be used in the internal control system to meet objectives. This can be in the form of new technology tools to check for and prevent errors, but it also identifies the risks of these tools such as through false flags or incorrect reports. The twelfth principle establishes the policies that management will use to combat risks. Strong examples of this would be non-disclosure agreements and the employee handbook.

Information and Communication:

This component defines the channels of communication within a company, the quality of information and its flow of information through the control activities. The thirteenth principle identifies the information that is critical for the control activities to function and achieve its objectives. The main concern is whether or not the control activity is actually capable of capturing relevant information and maintaining quality through processing it. The fourteenth principle relates to the internal communication systems that control information and the communication of individuals company wide, through all levels. It is critical that management and the board of directors be able to receive information in a timely manner so that they can make decisions regarding the internal controls. The fifteenth principle establishes the appropriate communication channels with external parties and what information is appropriate or not to disclose with them. It also makes it clear that certain information is required to be communicated by law such as data breaches.

Monitoring:

Even when if the other four components are completed to their fullest, they will not guarantee a secure information system. It is necessary to continuously monitor the system thereafter the other internal processes have been implemented to assure that they are working as expected. The sixteenth principle highlights that concept and identifies those evaluations should give an individual the baseline understands of risks so the company can continuously evaluate the controls in place. The final point gives the company an idea of corrective actions when a deficiency is identified through the evaluation process. This also includes the speed of which management reacts to this deficiency when it is found and future evaluations.

Other Frameworks and Standards

S&H Aquariums can consider the following frameworks and standards for the organization to implement together with PCI DSS.

Frameworks/Standards	
Control Objectives for Information and Related Technology (COBIT)	This framework was created for developing, implementing, monitoring, and improving information technology governance as well as best practices for management.
Service Organization Control (SOC)	The Service Organization Control (SOC) reports provide assurance that service organizations have adequate controls and processes. The requirements of Section 404 of the Sarbanes-Oxley Act results in the SOC audit reports becoming crucial in the process of reporting on effectiveness of internal control over financial reporting.
International Organization for Standardization (ISO)	This is an international framework covering a wide range of controls related to IT security risk management. ISO

	27001 presents a framework for developing and implementing information security management systems (ISMS).
National Institute of Standards and Technology (NIST) 800-53	<p>This framework provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. The controls address the various requirements derived from mission and business needs, laws, regulations, policies, standards, and guidelines.</p> <p>Addressing functionality and assurance helps to ensure that technology products and the systems that rely on those products are trustworthy.</p>

How the 17 Principles of COSO and the 12 Primary Requirements of PCI DSS Correspond

Internal control component	Principles		Principles/Goals	Requirements
Control Environment	1. Demonstrate commitment to integrity and ethical values	1	Build and maintain a secure network This principle involves requirements covering the data center network including firewalls (implementation, lockdown, port justification) and vendor defaults (modification of vendor supplied defaults, configuration standards)	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
	2. Ensure that board exercises oversight responsibility		Protect Cardholder data This principle involves requirements covering protection of stored cardholder data and transmission encryption to and from the data center across public networks	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
	3. Establish structures, reporting lines, authorities, and responsibilities		Maintain a vulnerability management program This principle involves requirements covering anti-virus software (installation, capabilities, functionality) and secure systems/applications (patching, security vulnerability awareness, security in the systems development lifecycle).	5. Use and regularly update antivirus software or programs 6. Develop and maintain secure systems and applications.
Risk Assessment	4. Demonstrate commitment to a competent workforce	2		
	5. Hold people accountable	3		
Control Activities	6. Specify appropriate objectives	4	Implement strong access control measures This principle involves requirements covering cardholder data access restrictions, assigning unique IDs by individual (password requirements, two-factor authentication, password encryption) and physical access restrictions to the data center and the managed servers.	7. Restrict access to cardholder data on a need-to-know basis. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
	7. Identify and analyze risks			
Information and Communication	8. Evaluate fraud risks	5	Regularly monitor and test networks This principle involves requirements covering logging and monitoring access to network resources/cardholder. Regular testing of security systems and processes (wireless analyzer, vulnerability scanning, penetration testing)	10. Track/Monitor all access to network resources and cardholder data. 11. Testing security systems & processes regularly.
	9. Identify and analyze changes that could significantly affect internal controls			
Monitoring	10. Select and develop control activities that mitigate risks	6	Maintain an info security policy Covers the need for an up to date and thorough Information Security Policy (incident response planning, role/responsibility assignments, employee usage requirements)	12. Maintain a policy that addresses information security for employees and contractors
	11. Select and develop technology controls			
	12. Deploy control activities through policies and procedures			
	13. Use relevant, quality information to support the internal control function			
	14. Communicate internal control information internally			
	15. Communicate internal control information externally			
	16. Perform ongoing or periodic evaluations of internal controls			
	17. Communicate internal control deficiencies			

1 Establishes baseline policy, and environment

2 Secures data through the use of tools

3 Maintains program through use of assessments

4 Deployment of controls

5 Establishes how information is shared

6 Ongoing monitoring and testing

Integrated Internal Control System Goals Based on PCI-DSS

Compliance

As technology continues to evolve, our goal is to keep Credit Card systems that store and transmit data safe through the framework. Any organization with a system that processes card payment data directly or indirectly must comply with the PCI DSS standards. PCI DSS has a 12-step procedure that outlines the procedures and how to ensure that the principles are followed. The 12 outlined principles are also updated by PCI DSS to ensure that they conform to the current everchanging security requirements. Heavy fines are levied on an entity or organization that is uncompliant with the PCI DSS standards.

The first step in ensuring compliance with PCI DSS, requires a network must maintain the baseline required security to uphold the CIA triad. The first line of defense to ensure that the data is secure is the proper installation and configuration of a firewall. Card holder data must also be held securely to not compromised data integrity. More importantly the card holder data must be encrypted during transmission to ensure that it is only accessible to authorized persons/entities and cannot be intercepted by third parties or unauthorized persons/entities.

The third aspect is to ensure the integrity and security of the management programs, systems and applications that process the user's data. The strong control policies as mandated by the frameworks and PCI DSS, mandate that software testing needs to be done to ensure that system software is current and up to date. Required patchwork is done in a timely manner and the use of automation on the installation of patchworks make the process seamless.

S&H Aquariums needs to enforce strong security access controls and employ the use of MFA (a 2 or 3 layer of security) and verification to ensure that the person accessing the system is who they are. Constant monitoring of credit card information databases for security breaches needs to be done proactively to ensure that systems are not rendered vulnerable.

Implementation and maintenance of a strong security policy is key for all employees and ongoing training must be enforced so that all employees are aware of the risks and threats that can impact S&H Aquariums. Regardless of the framework that is used, namely NIST, ISO, COSO, SOC, COBIT, all the steps mentioned above can be instituted and attained with due diligence. The ISO framework would identify and prioritize the risks and vulnerabilities that the S & H Aquarium may encounter. SOC framework as a tool, would outline an effective monitoring system to the systems, whereas the COBIT framework would offer a more detailed approach to the implementation of the various controls.

Conclusion

After careful review, our team suggests the following frameworks and standards to S&H Aquariums for further consideration; COSO, COBIT, and PCI DSS. COSO offers the structure to examine risk within the organization and apply risk-based processes. Although being a broad framework, it applies risk management towards functions across the company. In addition to COSO, S&H Aquariums can implement the COBIT framework considering the need to ensure and protect consumer data and personal information. COBIT is useful in aligning IT with the organization requirements by mapping controls to key business requirements, sorting IT activities into a process

model, distinguishing the key IT resources to be regulated. Both the COSO and COBIT framework can be integrated with PCI DSS which additionally can assist S&H Aquariums safeguard cardholder data and provide consumers a sense of trust and confidence. By successfully implementing the COSO Framework and integrating other frameworks as needed not only will S&H Aquariums become PCI DSS compliant with relevant internal controls, but there will also be a reasonable assurance to protect against both internal and external risks that can impact cardholder data.

Works Cited:

Fox, T. (2021, March 12). *COSO week – Objective V: Monitoring activities*. JD Supra.
<https://www.jdsupra.com/legalnews/coso-week-objective-v-monitoring-6050918/>.

Welch, M., & Nagal, E. (2021, June 24). *Internal controls – information & communication*. Johnson Lambert LLP.
<https://www.johnsonlambert.com/insights/internal-controls-information-communication/>.

Everson, M., Beston, C., Jourdan, C., Soske, S., Harris, C., & Posklensky, J. et al. (2021). *Coso.org*. Retrieved 5 August 2021, from
<https://www.coso.org/documents/990025p-executive-summary-final-may20.pdf>.

The 17 Principles of Effective Internal Controls | Weaver | Assurance, Tax & Advisory Firm. (2020, February 12). Weaver. <https://weaver.com/blog/17-principles-effective-internal-controls>

360 Advanced. (2021, April 27). *What is a SOC Report and Why Does My Company Need One?* <https://360advanced.com/soc-report-and-why-my-company-needs-one/>

COBIT | Control Objectives for Information Technologies. ISACA.
<https://www.isaca.org/resources/cobit>

NIST vs. ISO: What's the Difference? AuditBoard. <https://www.auditboard.com/blog/nist-vs-iso-whats-the-difference/>

Payment Card Industry Security Standards Council. (2018, May). *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures*. PCI Security Standards Council.

<https://www.pcisecuritystandards.org>

SOC for Service Organizations: Information for Service Organizations. AICPA.

<https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html>

Weiss, M., & Solomon, M. G. (2015). *Auditing IT Infrastructures for Compliance: Information Systems Security & Assurance* (2nd ed.). Jones & Bartlett Learning.