SANS Institute
Information Security Reading Room

Information Security Best Practices While Managing Projects

Dallas Smith

Copyright SANS Institute 2019. Author Retains Full Rights.

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Information Security Best Practices While Managing Projects

GIAC (GSEC) Gold Certification

Author: Dallas Smith, dallas.smith@outlook.com
Advisor: Rajat Ravinder Varuni
Accepted: March 24th, 2019

Abstract

To maximize long-term return on investment (ROI) with a project's delivery, taking information security into account with all aspects of an environment is essential. Fortunately, there are opportunities for project managers to incorporate the application of information security best practices with their projects. The goal of this paper is to bring a deeper understanding of why information security should be front and center to all project stakeholders. The article will discuss ways that project managers can incorporate information security best practices by the use of (1) vendor selection and management, (2) risk assessments, (3) contract negotiation and business associate agreements, and (4) how information security plays a significant role in all phases of a project's life cycle (initiation, planning, execution, monitoring and controlling, and closure). By understanding and following these information security practices, project managers ensure that their projects do not introduce their organization to unneeded risk, thereby saving the organization time and money.

© 2019 The SANS Institute, Author Retains Full Rights

© 2019 The SANS Institute Author retains full rights.

1. Introduction

Project managers have one goal – to finish a project on time, under budget, and within scope. As projects become increasingly integrated with information systems, it becomes critical that project managers put information security first in all aspects of project management. If they do not, the result could be detrimental to the organization (not just the project itself) and the project manager's future (professional reputation, employability, and so on).

Consider the following example. James Smith works as a project manager for a relatively large hospital in Florida (500-bed facility; 5,000 employees). One day, his supervisor informs James that he is about to lead a relatively sizable multi-departmental project working with a relatively unknown vendor, Provisioning Quest, an information technology consulting firm specializing in the implementation of software that saves organizations money through efficiencies realized with account provisioning and identity and access management systems. James eagerly accepts the assignment and begins to perform research on the vendor. To his dissatisfaction, James is unable to find any information about Provisioning Quest except that the age of their website is only one-year-old.

James meets with his supervisor to discuss his next steps on this effort and learns that the project schedule needs to be reduced from six months to five, due to other project prioritization and delays in this project's contract signing. James meets with Provisioning Quest and decides that they can crash some of the tasks in the work breakdown structure in a move to reduce the number of weeks that the project will take. The project's tasks appear fine; the presentations that James give to his supervisor and stakeholders are well received.

Months pass by, and James is halfway into the project schedule, working with the organization's Identity and Access Management team to conduct end-user testing of the solution when he receives a call to come to Greg's office (the Chief Information Officer of the organization). James hurries to Greg's office and finds that there is an already-in-progress meeting with the information security team. A sense of dread comes over James. What has happened? What is going on?

© 2019 The SANS Institute Author retains full rights.

James quickly learns that ransomware compromised the majority of the critical systems in the organization. Essentially, the electronic health record (EHR) is inoperable in its current state. A full restore of the impacted systems could take weeks, potentially months. The hospital is on diversion with patients moving to other hospitals for patient care. The hospital is at a standstill, losing thousands of dollars a minute, and is currently in the process of standing up a command center to conduct a computer incident threat response to contain and eradicate the threat. There is no time estimation of this getting resolved.

How could this happen? The hospital traced the ransomware virus back to the project that James was managing. The virus infected removable media (a USB drive) that were used by the vendor to install its software on enterprise systems. Since the installation was performed with a privileged account on a system within the hospital's data center, the spreading of the virus occurred rapidly and without detection. The virus also compromised Provisioning Quest's systems and two other client locations.

While sitting in the office of the CIO, James begins to recount his previous interactions with Provisioning Quest and starts conducting a mental post-mortem of the situation. Could James have prevented this from happening? The answer is simple - yes. The scenario described above is not far of an exaggeration from what happens in projects across the globe. Processes get loose, procedures do not get followed, and some oversights occur. Put these together, and any organization is at tremendous risk.

This paper aims at providing project managers with the tools and techniques to prevent situations such as the one James experienced from happening in a real-life case. By understanding and integrating information security best practices in the project management life cycle, a project can be a success, as denoted as being delivered on time, within budget, and within scope.

This paper is structured in each of the main phases of a project as defined by the Project Management Institute, with detail from an information security management point of view. At the end of most sections, an included checklist provides a summary of the information security based suggestions.

© 2019 The SANS Institute Author retains full rights.

2. Information Security in the Project Management Framework

The Project Management Institute has created the project management framework that many project managers use today. The framework contains five phases: (1) Project Initiation, (2) Project Planning, (3) Project Execution, (4) Project Monitoring and Controlling, and (5) Project Closure. Following the project management framework enhances the probability of project success. Similarly, incorporating the appropriate sub-controls listed in the Center for Internet Security (CIS) Controls improves a secure implementation of the project. Proactively hardening the organization's security posture ensures that the organization positions iteself in a good place in the event of an audit. Doing so avoids the likelihood that a company has to take steps to provide remediations when an audit finding comes to light. By preparing in advance, the organization is fully aware of what the project risks are and how those risks impact the organization. By proactively resolving audit findings, the organization would be able to focus their attention on other matters.

2.1. Project Initiation

Before a project can truly begin, there is a lot of work that must be done "behind the scenes," also known as Project Initiation. Here, business case creation, vendor selection, stakeholder identification, and creation of the project charter build the foundation of a successful project. These activities can be referred to and revisited throughout the project in an ongoing effort to ensure the project stays on track and that project information remains current.

2.1.1. Business Case Creation

An organization generally starts by planning to fulfill a business need or some objective. For instance, a hospital has to satisfy a regulatory requirement that it needs to meet by the end of the year. Organizations create business cases to help with the decision making process. Business cases are comprised of costs (implementation, infrastructure, licensing, and so on) and benefits (revenue generated or cost savings), thus producing a return-on-investment (ROI) (Duranti, 2016). Since applying information security practices serves as a benefit to the organization, find ways to include these in the business case. Some potential benefits in the business case include the enforcement of

© 2019 The SANS Institute Author retains full rights.

organizational policies and a need to fulfill regulatory requirements (Nemati, 2008, p. 2649). On the other hand, security-based solutions may present ROI benefits quantitatively by proposing cost avoidance. For example, the implementation of a security appliance reduces the number of full-time employees (FTEs) needed in an organization through the use of automation (Purser, 2004, p. 203).

Table 1: Business Analysis Checklist

Item	Question	Purpose	Methods	CIS Sub-Control
1	*Does the project or solution bring the organization any qualitative information security benefits?*	Includes meeting audit and regulatory requirements or fixing security based issues.	Business Analysis	1.4
2	*Does the project or solution bring the organization any quantitative information security benefits?*	Includes gaining cost savings through automation or other security-specific benefits.	Business Analysis	1.4

2.1.2. Vendor Selection

There are some projects where different vendors are jockeying for the same contract. Choosing the right vendor is critical. To select the right vendor, consider the following list of questions. *What is the vendor's organizational history?* Has the organization been around for several years with a history of repeated success or is this their first or second major contract? If the former, the project plan is going to most likely be well designed, taking experience gained from previous projects. There is also the likelihood that the vendor will have the resources to respond to a computer incident. On the other hand, if the latter, the experience would most likely focus on the core elements of just getting the project completed, thus not being able to focus on any information security management practices. Finding the answer to this question can be done with interviews with the vendor, asking colleagues, or performing queries on the Internet.

Has the organization dealt with the vendor before? Previous dealings can help with decision making, especially if the project is similar in scope. If there have been past business dealings, then there should be an understanding of how important the vendor views information security in its practices.

© 2019 The SANS Institute Author retains full rights.

Where is the vendor based? If the organization resides within the same country, this indicates that the same laws govern both firms. On the other hand, if the vendor operates outside of the country, there could be different laws about how data is to be used, stored, and transmitted, which can pose a significant security risk if not handled appropriately.

Legelis and O'Brien suggest other criteria to look out for including: *what partnerships does the vendor have? What technology does the vendor use? What features does the vendor offer? Does the vendor possess the capability to detect breaches? Does the organization integrate well or seamlessly with other information security products* (Legelis & O'Brien, 2018)*?*

By performing this exercise for each candidate vendor, the firm can then rank order the vendors and select the vendor that meets the most criteria. Doing this is a necessity. Vendors need to have the knowledge, resources, and like-mindedness to ensure that the project will deliver on all targets.

Table 2: Vendor Selection Checklist

Item	Question	Purpose	Methods	CIS Sub-Control
1	*What is the vendor's history?*	Ensure the vendor's ability to provide delivery of a successful project while ensuring information security practices aligns with the organization.	Interviews with the vendor, asking colleagues, Internet search	N/A
2	*Has the organization dealt with this vendor before?*	History predicts future performance; this can indicate expectations from the organization.	Reviewing previous contracts, assessing past project's lessons learned	1.4, 1.5, 2.1, 2.2, 2.5
3	*Where is the vendor located?*	Determines what laws the vendor follows.	Interviews with the vendor, Internet search	N/A
4	*What partnerships does the vendor have?*	Provides another source of credibility to the vendor's capabilities.	Conversation with the vendor, Internet search	N/A
5	*What technology does the vendor use?*	Determines potential integration issues.	Conversation with the vendor, Internet search	1.4, 2.4, 2.5

© 2019 The SANS Institute, Author Retains Full Rights

© 2019 The SANS Institute Author retains full rights.

Item	Question	Purpose	Methods	CIS Sub-Control
6	*What features does the vendor offer?*	Provides information about additional integration points.	Interviews with the vendor, Internet search	1.4, 2.4, 2.5
7	*Does the vendor have the ability to detect breaches?*	Indicates the priority the vendor places on information security related issues and the ability to respond when an event occurs.	Interviews with the vendor, Internet search	1.4, 2.2, 2.4, 2.5
8	*Does the vendor's product or solution integrate well or seamlessly with other information security related products?*	Indicates to the organization how well the vendor's product or service integrates with the organization's previously implemented product or services.	Interviews with the vendor, Internet search	1.4, 2.5

2.1.3. Stakeholder Identification

The process aimed at determining whom to include on a project is known as stakeholder identification. Ensure that the project team consists of members of information security, the owners of impacted applications, appliances, or systems (whether upstream or downstream), members responsible for interfacing the data between the systems, members of the risk and legal team, and a member from the records information management team. Each of these team members plays a vital role in ensuring the project team makes the best decisions for the organization. Information security members bring their expertise with the organization as a whole, the latest trends in information security, and will most often assist in completing the risk assessment questionnaire (RAQ). Impacted application owners provide valuable insight into their system or systems and help the project team understand the organization's current state with their areas of responsibility.

Similarly, a member of the interface team brings a broader view of the organization, thereby assisting the project in making good decisions for project success. The risk and legal teams provide clarity with what type of risks the organization is willing to take. The records information management team assists with best practices in the process of storing information within the organization. Leaving any of these groups

© 2019 The SANS Institute Author retains full rights.

out of the decision-making process in a project runs the chance of the project team making a poor decision thus negatively impacting the organization.

Table 3: Stakeholder Identification Checklist

Item	Question	Purpose	CIS Sub-Control
1	*Is a member of the information security team involved?*	Will typically bring awareness of organizational goals to the project; assists with leading the risk assessment questionnaire (RAQ).	1.4, 2.1, 2.5
2	*Are members of impacted solutions included?*	Ensures the team can discuss all systems and determine the reasoning behind previous design decisions.	1.4, 2.1, 2.5
3	*Is a member of the interface team involved?*	Provides a broad view of how the systems will integrate.	1.4, 2.1, 2.5
3	*Is a member of the risk management team involved?*	Provides insight into what risk the organization is willing to take.	1.4, 2.1, 2.5
4	*Is a member of the records information management team involved?*	Provides information on how the organization stores information.	1.4, 2.1, 2.5

The stakeholder identification process should be done at the beginning of the project and reviewed periodically throughout the life of the project. Throughout a project, discoveries made can change the trajectory of a project – for better or worse. For example, if the project identifies another appliance being affected during the planning phases of a project, then it is critical to incorporate that appliance and all impacted team members to the project as soon as possible to determine what the impact is to the organization and the project's implementation. Discoveries such as this impact the scope, timeline, and resources required to complete the project. Examples of this put into action include the project manager having a stakeholder identification workshop after the completion of each major milestone and having the stakeholder identification topic occur periodically as an agenda item in standing project meetings.

2.1.4. Project Charter

The project charter is one of the most important documents of a project. The Project Management Institute defines it as the document that outlines the project's purpose, identifies success criteria, lists key deliverables, states project risks, captures a high-level overview of the project milestone schedule, provides information regarding

© 2019 The SANS Institute Author retains full rights.

financial resources, and grants authority to the project manager for this project (Project Management Institute, 2017, p. 81). Since the project charter provides the project with the resources it needs to be successful and gives the project manager authority over the project, it is essential to integrate information security elements in some of the major categories.

Information security based success criteria and a critical deliverable include the logging of the network's assets that process or store information in the organization's inventory solution. Hardware asset information that should be captured consists of the following: application name (and any aliases); workstation or server name; network address (IP address); hardware address (MAC address); data asset owners (whose responsible for the handling of information within the system); primary support personnel (the party that is engaged when an issue is encountered); the business process that is utilized by the asset; the date the asset was introduced in the environment; the end users of the asset; and a short description for the asset. This type of information will prove invaluable once the project ends and the organization has stopped making asset discovery a priority. Knowing who is responsible for the asset and who supports the asset will also help in future projects where the asset interfaces with other assets (upstream or downstream). These parties will serve as critical stakeholders in those future projects.

Once the project manager finalizes the project charter and receives sign-off from the project sponsor, the project work can truly begin. Including the information security elements mentioned above prior will ensure that the project manager has the right and authority to take an information security-centric approach in subsequent project phases.

Table 4: Project Charter Checklist

Item	Question	Purpose	Methods	CIS Sub-Control

© 2019 The SANS Institute Author retains full rights.

1	*How does the project's purpose align with information security principles?*	Provides security focused value-add benefits to the project.	Solution review	N/A
2	*What information security criteria and deliverables can be listed to ensure success?*	Including network asset inventory ensures that the organization is kept up-to-date with the introduction of new solutions.	Asset review workshop, architecture diagrams	1.4

2.2. Project Planning

The project planning process group contains all of the knowledge areas within the PMI Project Management framework. This paper covers the following knowledge areas: scope, communications, risk management, procurement planning, and conducting a project kickoff. The other knowledge areas contain limited information security practices.

2.2.1. Plan Scope Management

Information technology-based projects generally need a minimum of one server for their solution to be implemented. Vendors provide specification lists that inform what is needed for their product to run in an operational state. Unfortunately, this information contains minimal or no security requirements. Vendors commonly rely on the organization itself to make security decisions.

To best prepare the organization for the introduction of a new server, it is best to follow a build, harden, test, and signoff process. The build step refers to the process of the server resource building out the server based on the vendor's recommendations. It is a good idea to increase the storage to ensure that there is enough for logging purposes. The project manager can have the vendor perform a preliminary check on the server to ensure build accuracy.

Hardening refers to the preliminary steps the organization takes to ensure the server is secure. Examples include changing default passwords, closing unneeded ports, enabling system auditing, uninstalling unnecessary applications, disabling external (USB) auto-run features, patching systems to the latest stable version, and keeping security applications up-to-date with the latest signatures. Organizations typically create a working image for each of the operating systems that they deal with; this is recommended

© 2019 The SANS Institute Author Retains Full Rights

to ensure standardization, avoid any gaps in the measures taken by the server resources, and to reduce the amount of time it takes to create a working system.

Testing refers to running the completed system through a vulnerability scan. The report that generates from this exercise will indicate what remaining security vulnerabilities are outstanding. Here, it is a good idea to fix all the issues that are on this list. There are, however, times when this is not possible. Document the compensating controls for the flagged items that are impossible to remediate. Once the team completes remediating the reported security vulnerabilities, run another vulnerability scan to confirm there are no new issues.

Once the system completes the hardening process and vulnerability scans generate no unknown vulnerabilities, proceed with having the vendor test the previously tested functionality. If the system is working as designed, continue with signoff for this activity. If there is a problem with the system (processes are failing, communications are not delivering, and so on), work with the vendor to determine the root cause, provide the appropriate remediation, and then seek signoff.

Now that the server has been created, hardened, and is known to work and have no vulnerabilities, it is crucial to document these efforts. Creating a document that lists the decisions on specific actions will help in future efforts (OS upgrades, audit findings, and so on). Creating an architectural diagram will serve as an exercise that will increase the knowledge of the systems and will serve as an invaluable document during security incidents or production-related issues.

Password complexity should vary based on use case. For accounts that are to be used by systems (for example, service accounts and interactive login accounts), passwords should be at least 25 characters long, using alphanumeric characters (upper and lower), and symbols (if the system will allow it). These passwords should be set to expire periodically (365 days). Service accounts should be reviewed and determined if enrolling in Microsoft's Security Account Manager (SAM) is a possibility.

User account passwords should follow a slightly different password complexity requirement. Passwords should be at least eight characters, using alphanumeric characters (upper and lower) and symbols (if the system will allow it). The passwords should be set to expire on an accelerated basis (90 days). Depending on the system's configuration,

© 2019 The SANS Institute, Author Retains Full Rights

© 2019 The SANS Institute Author retains full rights.

there are also other password settings that are worth mentioning: account lockout should be set to five (the number of times an incorrect password can be entered without locking the system); account lockout duration set to 30 minutes (once a password has been entered enough times incorrectly to enter a lockout, this is the amount of time before the system will automatically unlock the system); and reset account lockout threshold set to 20 minutes (this is the amount of time is needed for the system to reset its incorrect password counter).

Access control (also commonly referred to as privileges) relates to the rights and functionality a user account has once in the system. It is a best practice that the system is configured to take a role-based access control (RBAC) approach. Here, each position type has its security set; user security matches their job function.

Other scope management items that should be reviewed include if the solution is able to leverage multi-factor authentication; ensuring that data is only sent through encrypted channels; segmenting the server on the network through VLANs if data is considered sensitive or protected; if the server's network can function correctly with whitelisting; and ensuring that the system is configured to conduct backups on a scheduled basis.

Table 5: Project Charter Checklist

Item	Question	Purpose	Methods	CIS Sub-Control
1	*Has the server been created?*	Fulfills the technical requirements of the project.	Building the server based off of a specification sheet (including the capacity for logging purposes).	18.3

© 2019 The SANS Institute Author retains full rights.

2	*Has the server been hardened?*	Ensures that the server is robust in the environment.	Following organizational hardening procedures (for example, changing default passwords, closing unneeded ports, and so on).	18.11
3	*Has the server been tested?*	Validates the system is secure and develops a plan of action for those that are not complete.	Vulnerability scans, remediating found issues, providing compensating controls for unchanged items.	3.1, 3.6, 3.7
3	*Has the server received vendor signoff?*	Brings the vendor into the process to ensure functionality and their approval with the system.	Vendor review	N/A
4	*Are all account types using an approved password complexity structure and contain the correct privileges?*	Ensures that the project aligns any account passwords with the organization's best practices.	Reviewing accounts by type (administrator, user) and ensuring the policy matches the organization. Implement role-based access controls for account types.	4.4, 16.7
5	*Are there any other security features that can be reviewed with the solution? Examples include incorporating multi-factor authentication, using encrypted only channels, and so on.*	Ensures that the solution can provide long-term success and acceptable maintenance within the organization.	Technical review workgroup	2.7, 10.1, 14.1, 16.3, 16.5

2.2.2. Plan Communications

In this context, communications planning refers to answering the following question – *What can I do to ensure that the information that I have about this project is kept secure?* The answer varies depending upon the maturity the project team has regarding following information security standards. During or near the time of the project kickoff, the project team may benefit from attending information security-based classes

© 2019 The SANS Institute Author retains full rights.

regarding how to handle sensitive project data, what steps are needed to prevent unintended data breaches, and how to report a security incident. Having a project manager plan these events and communications signals to the project team just how important they are to the organization.

Once the project planning has ended, a project kickoff meeting is conducted to align the expectations of the project to the project team. The meeting agenda generally consists of stating the goals of the project, any assumptions the project may be making, a timeline for key milestones, and the team members involved. By communicating all of this information, the project kickoff meeting is aimed at instilling a commitment to the project (Project Management Institute, 2017, p. 86).

Table 6: Plan Communications Checklist

Item	Question	Purpose	Methods	CIS Sub-Control
1	*What can I do to ensure that the information that I have about this project is kept secure?*	Ensuring that all communications answer this question to enhance the security posture of the project and organization.	Project kickoff meetings, project meetings, emails	17.x

2.2.3. Plan Risk Management

How much risk is the organization willing to take with the implementation of this project? Do the positives outweigh the negatives? Answer these questions by conducting a risk assessment questionnaire (also known as a "RAQ"). Risk assessments are performed to ensure that the organization's definition of security aligns with the vendor's. An information security resource typically conducts a risk assessment for the project and vendor. Once complete, the risk assessment is sent to the project manager and member of the information security office for review and sign off.

Risk assessments vary by organization but generally contain contact information for the project and the questionnaire itself. Each of these items needs to be carefully reviewed to ensure the organization is comfortable with how the data is generated and managed throughout the solution. Contact information can be categorized by the organization and vendor. Organizational contact information includes the following: the project manager, the team responsible for the solution, data steward(s), system, and

© 2019 The SANS Institute, Author Retains Full Rights

business owner. Vendor-related contact information includes the following: company name, contact at the company (with their title), address and telephone of the company, email address, and hours of operation.

Now that the contact information has been obtained let's go through some of the central questions of a risk assessment. *Where is the solution hosted? Is the solution hosted on-premises and supported by the organization?* These questions indicate that the organization needs to think about how to support the solution and its security requirements for its entire life. *Is the solution hosted on-premises and supported by the vendor?* If this is the answer, the organization needs to think about how the vendor will access the systems and if accounts will be created for every support personnel. *Is the solution hosted off-site?* The support model changes and additional questions will need to be answered (where, who is responsible for maintenance, and so on).

What is the data classification for this solution? Classifying data is needed for the proper handling of data. There are a variety of classification types depending upon the nature of the organization. An example set of data classifications includes company data (human resources sensitive information, intellectual property files, system architect diagrams), consumer data (personally identifiable information, credit card information), and medical data (protected health information) (Woody, 2013, pg. 138-139). Data classification can also be as simple as listing all of the types of data within the system. Common data elements used include social security numbers, credit card information, electronic protected health information (e-PHI), electronic medical record (EMR) data, photographic images, and so on. Making selections during the completion of a questionnaire indicates how to handle the data. For instance, health information is protected using the guidance outlined in the Health Insurance Portability and Accountability Act (HIPAA); the handling of credit card data is protected using the Payment Card Industry (PCI) data security standard (DSS) (Broad, 2013, pg. 173).

What is the solution's provisioning strategy? In other words, how do the solution's accounts integrate with the organization's identity and access management process? Work towards developing a strategy that takes a look at the following areas: account creation (centrally managed or provisioned by a specific team), account usage (single sign-on, attribute sharing), account update activities (account change history),

© 2019 The SANS Institute Author retains full rights.

account revocation (eliminating access for terminated employees), and governance (ensuring these identity-related transactions are following predefined organizational policies) (Bertino & Takahashit, 2010, p. 30-35). Developing a clear understanding of the identity and access management process ensures that users can continue to use the new system without any interruption.

What are the solution's backup and disaster recovery strategy? With the increase in ransomware attacks to organizations, it is essential for both organizations and vendors alike to have robust and adequate backup and disaster recovery plans. Is the backup going to be done using a full (backing up all the files in a system) or incremental (backing up only the data that have been changed since the latest backup thereby saving time) backup? Is this considered a hot backup (can users use the system and make edits while the data is being backed up)? What is the return-to-operation (RTO)? What is the recovery point objection (RPO) (how far back in time is the data recovery configured to go) (Stier, 2015, p. 50)? If the vendor is unsure, the project manager should refer to the organization's data management and backup policy and provide this as a point of reference for the vendor to work towards.

Does the vendor need to use external media (USB, CD, or floppy disk) for any reason throughout the life of the project? The use of external media threatens the organization through the potential for pre-installed malware to be on the media; and external media poses as a method for unknown data loss by avoiding egress filtering monitoring (Vladimirov, Michajlowski, & Gavrilenko, 2014, p. 162). With this posing as an enormous risk to the organization, the organization should prohibit the use of external media at an enterprise-wide level. If this decision substantially hinders the vendor's progress on completing project deliverables, there are creative ways to bypass this. For example, a vendor could provide the organization with the external media drive before the installation. The organization scans the external media on a workstation that is not able to connect to the Internet. From there, the organization transfers the contents on the vendor's external media drive to an organization's pre-approved external media drive. The vendor is to then use the pre-approved external media drive for software installation and data transfer. Once the installation process is complete, the organization and vendor can each return their external media drives to the other party. Following this process achieves two significant objectives – it ensures that the contents on the vendor's external

© 2019 The SANS Institute Author retains full rights.

media drive were safe and the vendor is unable to deceive the organization and steal confidential or sensitive information.

Can the vendor provide on-demand audit requests such as the Standards for Attestation Engagement No. 16 (SSAE 16)? Since the organization is outsourcing some of its processes, the Sarbanes-Oxley Act requires that the vendor provide this to their customer (the organization). This report yields a couple of benefits to the organization: time and money savings through a reduction in audit costs; and the organization receives an outside opinion of the vendor's security controls (Gonsalves, 2011, p. 34).

Is the data protected at rest and in transit per guidelines outlined in Federal Information Processing (FIPS) 140-2? FIPS 140-2 is a standard that was created collaboratively from the National Institute of Standards Technology (NIST) and Communications Security Establishment Canada (CSEC) (Bomgar Receives FIPS 140-2 Level 2 Validation, 2014, p. 6). Meeting this indicates that the vendor meets a regulatory standard in information security. Doing so demonstrates that the vendor has taken the time and effort to strengthen their solution to a particular degree.

It is important to state that while the plan risk management plan is technically in the planning phase of a project, it benefits the project to get started as soon as possible. Being provided with potential risks before the start of a project will give the organization an opportunity to appropriately respond (eliminating the threat, accepting the risk, or canceling the project).

Table 7: Plan Risk Management Checklist

Item	Question	Purpose	Methods	CIS Sub-Control
1	*Where is the solution hosted? Is the solution hosted on-premises and supported by the organization? Is the solution hosted off-site?*	Determines what security controls are needed for the solution.	Risk assessment questionnaire	N/A
2	*What is the data classification for the solution?*	Determines what laws govern the data.	Risk assessment questionnaire	N/A
3	*What is the solution's provisioning strategy?*	Determines who is responsible for creating accounts for the solution.	Risk assessment questionnaire	16.2

© 2019 The SANS Institute, Author Retains Full Rights

Item	Question	Purpose	Methods	CIS Sub-Control
3	*What is the vendor's backup and data recovery strategy?*	Provides insight into how the solution can restore its files in the event of an incident or disaster.	Risk assessment questionnaire	10.x
4	*Does the vendor need to use external media (USB, CD, or floppy disk) for any reason throughout the life of the project?*	Determines what security controls the organization needs to take.	Risk assessment questionnaire	13.7
5	*Can the vendor provide on-demand audit requests such as the Standards for Attestation Engagement No. 16 (SSAE 16)?*	Provides the organization assurances in the event of an audit.	Risk assessment questionnaire	N/A
6	*Is the data protected at rest and in transit per guidelines outlined in Federal Information Processing (FIPS) 140-2?*	Demonstrates that the vendor meets regulatory standards.	Risk assessment questionnaire	N/A

2.2.4. Plan Procurement

Once the vendor selection is complete, it is necessary to plan the procurement process with contract development. Contract development ensures that the vendor and organization are accountable towards one another throughout the life of the engagement (Kubitscheck, 2014, p. 54). Similar to service level agreements (SLAs), contracts should contain several items that should be reviewed meticulously. These items include: purpose of the agreement, estimated time needed for the effort, security requirements, the process for change control, criteria that parties can use to get out of the contract, pricing (cost plus), post-conversion strategy, and any other project support agenda items (Hiles & Noakes-Fry, 2014, pp. 129-130).

It is often a good idea to have the pending contract reviewed by some of the senior members of the project team. These members serve as a fresh set of eyes on the effort and can provide discipline-specific insight into how to interpret the contract

© 2019 The SANS Institute, Author Retains Full Rights

language and if there are any noticeable gaps. Contract review workshops are a conventional vehicle to have this activity done.

Table 8: Plan Procurement Checklist

Item	Question	Purpose	Methods	CIS Sub-Control
1	*Have the basic requirements of the contract been reviewed? Examples include the purpose of the agreement, estimated time for effort, security requirements, pricing, conversion (pre/post) strategy, and so on.*	Provides the organization the statement of work that is needed to complete the effort; this is important in the event issues arise.	Contract review	N/A
2	*Have other subject matter experts (SMEs) reviewed the contract?*	Provides oversight into the project review process.	Contract review workshops	N/A

2.2.5. Business Associate Agreements

If the organization is a health care provider, it is most likely going to create and execute a Business Associate Agreement (BAA) if there is any transmitting of PHI between the two organizations. The BAA is a legally binding document that has the business associate (vendor) pledging to the covered entity (organization) that it will not use obtained health information for inappropriate purposes (Maintaining Privacy Is an Everyday Task, 2005, pp. 3-4). If the business associate discovers that the covered entity is violating the BAA, the business associate is responsible for providing a reasonable effort in resolving the violation, or to terminate the BAA with the covered entity and report to the Secretary of HHS. BAA violations could result in civil penalties ($100 to $1.5 million) or criminal sanctions (up to 10 years in prison, fines up to $250,000) to the organization or persons committing the violation (Classen, Fogarty, Mier, 2012, p. 7).

The BAA's language should include elements of the HIPAA's security rule (the technical, administrative, and physical safeguards) and privacy rule (limitations about use and disclosure) (American Dental Association, 2017, p. 109) and should clearly explain each of the parties' obligations. Covered entity obligations include: (1) providing the organization's "Notice of Privacy Practices" (NPP); (2) notifying the business associate if

© 2019 The SANS Institute, Author Retains Full Rights

individuals change or modify the permission of their PHI; (3) notifying the business associate if there are any restrictions that impact the use or disclosure of the PHI; (4) stating that the business associate should not engage in actions that violate what is outlined in the HIPAA/HITECH acts; (5) indicating that the business associate is able to rely on any instructions; (6) following the notification breach process in the event of a breach; and (7) any transaction-specific concerns (Classen, Fogarty, Mier, 2012, pp. 6-7). Business associate obligations include: (1) stating the permitted use and disclosures of using PHI; (2) ensuring that any sub-contractors and third-party agents adhere to the same obligations outlined in the BAA; (3) how to handle PHI; (4) the safeguards to be used (administrative, technical, and physical); (5) the right to audit to ensure compliance with the BAA; (6) applying to laws (in addition to what is outlined in HIPAA/HITECH); (7) the requirements when reporting breaches (relating to privacy and/or security); and (8) complying with the covered entity's related policies (Classen, Fogarty, Mier, 2012, pp. 8-72).

Table 9: Business Associate Agreement (BAA) Checklist

Item	Question	Purpose	Methods	CIS Sub-Control
1	*What are the technical, administrative, and physical safeguards written in the agreement?*	Provides the elements outlined in HIPAA's Security Review.	BAA Creation and Review	N/A
2	*Are there limitations about use and disclosure?*	Provides the elements outlined in HIPAA's Privacy Rule.	BAA Creation and Review	N/A

© 2019 The SANS Institute, Author Retains Full Rights

3	*Does the BAA discuss obligations by the Covered Entity?*	Provides answers to essential questions including but not limited to: (1) providing the organization's "Notice of Privacy Practices" (NPP); (2) notifying the business associate if individuals change or modification of permission of their PHI; (3) notifying the business associate if there are any restrictions that impact the use or disclosure of the PHI; (4) stating that the business associate should not engage in actions that violate what is outlined in the HIPAA/HITECH acts; (5) indicating that the business associate is able to rely on any instructions; (6) following the notification breach process in the event of a breach; and (7) any transaction-specific concerns.	BAA Creation and Review	N/A
4	*Does the BAA discuss obligations by the Business Associate?*	Provides answers to essential questions including, but not limited to, the following: (1) providing the organization's "Notice of Privacy Practices" (NPP); notifying the business associate if individuals change or modification of permission of their PHI; (3) notifying the business associate if there are any restrictions that impact the use or disclosure of the PHI; (4) stating that the business associate should not engage in actions that violate what is outlined in HIPAA/HITECH acts; (5) indicating that the business associate is able to rely on any instructions; (6) following the notification breach process in the event of a breach; and (7) any transaction-specific concerns.	BAA Creation and Review	N/A

2.3. Project Execution

This phase of the project is where project deliverables are made. To complete the project with information security principles being applied, the project manager has to ensure everyone follows the strategy outlined in the project management plan. In other words, consider the following perspective: a project is generally seen as delivering the scope as described in the statement of work; this is what the project team thinks of as well. Project team members are usually not thinking about following a process a specific way to ensure they are following information security best practices. It is, therefore, imperative for the project manager lead in the information security domain by example, because if not, the area could be left unattended, resulting in long-term costs to the organization.

© 2019 The SANS Institute Author retains full rights.

2.4. Project Monitoring and Controlling

To keep the project managed appropriately throughout all phases of a project, the project manager should practice the activities described in the project monitoring and controlling phase. The following activities ensure that a project can deliver on time, within budget, and as defined in the scope statement, while still being information security minded.

Keeping project data secure should be a priority for the project team. Frequently, the project manager should ensure that the project team is placing files only in authorized locations. If files need to be sent to another individual, this should be done using the approved organizational methods. Email encryption or large file distribution solutions are used at organizations to send sensitive information. If the project manager encounters a deviation to any of these processes, the project manager should notify the offending project team member of the infraction and the correct way to do things. If a pattern emerges with a particular team member, escalating the matter to the team member's manager may be necessary.

Changes to the project need to follow the organization's change management process. There are times in a project where the initial scope is insufficient, and a new scope has to be defined to satisfy the customer. It is critical that the project manager process all changes through the same project change control process. The change control process generally defines the impacts on the project's timeline, budget, and scope. It is important to review each of these change requests and determine if it can negatively impact the organization's security climate. If it does, then the change request needs to be escalated to the project governance committee for review and approval.

If the project is in collaboration with a vendor, configure scheduled access reviews with the vendor team. People come and go with any organization. It is vital to ensure that the vendor's staffing list is kept current and that there are no terminated employees with access. Reviews can be scheduled as a function of the duration of the project. For example, if the project is 16 weeks, the project manager could host access reviews with the vendor every four weeks.

Involve project members (including vendors) in information security exercises (such as phishing campaigns). Periodically execute phishing campaigns to ensure staff remains aware and vigilant throughout the life of the project. For those that fail the phishing

© 2019 The SANS Institute Author retains full rights.

campaign, have them enroll in another phishing campaign to ensure that behaviors have been modified.

Table 10: Project Monitoring and Controlling Checklist

Item	Objective	CIS Sub-Control
1	Keeping project data secure should be a priority for the project team.	17.x
2	Changes to the project need to follow the organization's change management process.	14.9
3	If the project is in collaboration with a vendor, configure scheduled access reviews with the vendor team.	16.7
4	Involve project members (including vendors) in information security exercises (such as phishing campaigns).	17.x

2.5. Project Closure

Now that the project has had a successful conversion and the project is ready to close, the project manager should commit to completing the tasks outlined in the project closure phase. All documents should be saved and stored; this is helpful with future projects and contract disputes (McLaughlin & Olson, 2017, p. 127). A lessons learned session held with the project team and key stakeholders to identify what went right and what could have been done better in relations to implementing an information security-centric project. Doing this will help reinforce the right behaviors needed for project success. Other important closure activities include modifying vendor access to reflect an operational state – network and badge access.

3. Conclusion

Implementing information security in project management does not have to be hard work. By following the recommendations listed above, an organization is primed with the tools needed for a successful and safe project implementation.

The checklists documented above have been uploaded into a GitHub repository which can be found at https://github.com/moogs37/InfoSec-Project-Management

© 2019 The SANS Institute, Author Retains Full Rights

References

American Dental Association (2017). Managing the Regulatory Environment: Guidelines for Practice Success: Best Practices. Chicago: American Dental Association.

Bertino, E., & Takahashi, K. (2010). Identity Management: Concepts, Technologies, and Systems. Boston, MA: Artech House, Inc.

Bomgar Receives Fips 140-2 Level 2 Validation. (2014). Computer Security Update, 15(5), 6–7.

Broad, J. (2013). Risk Management Framework: A Lab-Based Approach to Securing Information Systems. Amsterdam: Syngress.

Classen, H. W., Fogarty, M., & Mier, B. (2012). Anatomy of a Business Associate Agreement, Part I. Journal of Health Care Compliance, 14(4), 5–73.

Classen, H. W., Fogarty, M., & Mier, B. (2012). Anatomy of a Business Associate Agreement, Part II. Journal of Health Care Compliance, 14(5), 5–12.

Duranti, G. (2016). Best practices from a business analysis telco project. Paper presented at PMI® Global Congress 2016—EMEA, Barcelona, Spain. Newtown Square, PA: Project Management Institute.

Gonsalves, N. S. (2011). The New Standard. Collector (0010082X), 76(11), 33–37.

Hiles, A., & Noakes-Fry, K. (2014). Business Continuity Management: Global Best Practices (Vol. 4th ed). Brookfield, Conn: Rothstein Publishing.

Kubitscheck, V. (2014). Integrated Assurance: Risk Governance Beyond Boundaries. Farnham: Routledge.

Legelis, K., & O'Brien, L. (2018, December 18). Simplifying the ICS Cyber Security Vendor Selection Process. Retrieved February 19, 2019, from https://www.nozominetworks.com/2018/12/18/blog/simplifying-the-ics-cyber-security-vendor-selection-process/

Maintaining Privacy Is an Everyday Task. (2005). Receivables Report for America's Health Care Financial Managers, 20(7), 3–4.

McLaughlin, D. B., & Olson, J. R. (2017). Healthcare Operations Management (Vol. Third edition). Chicago, Illinois: Health Administration Press.

Nemati, H. R. (2008). Information Security and Ethics : Concepts, Methodologies, Tools and Applications. Hershey PA: IGI Global.

© 2019 The SANS Institute, Author Retains Full Rights

© 2019 The SANS Institute Author retains full rights.

Project Management Institute. (2017). A Guide to the Project Management Body of Knowledge: (PMBOK guide).

Purser, S. (2004). A Practical Guide to Managing Information Security. Norwood, MA: Artech House, Inc.

Stier, K. (2015). Data Backup in the Age of the Cloud. University Business, 18(9), 49–51.

Vladimirov, A. A., Michajlowski, A., & Gavrilenko, K. (2014). Assessing Information Security : Strategies, Tactics, Logic and Framework (Vol. Second edition). Ely, Cambridgeshire: IT Governance Publishing

Woody, A. (2013). Enterprise Security : A Data-Centric Approach to Securing the Enterprise. Birmingham: Packt Publishing.

© 2019 The SANS Institute, Author Retains Full Rights

© 2019 The SANS Institute Author retains full rights.

Last Updated: May 24th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS San Antonio 2019	San Antonio, TXUS	May 28, 2019 - Jun 02, 2019	Live Event
SANS Atlanta 2019	Atlanta, GAUS	May 28, 2019 - Jun 02, 2019	Live Event
Security Writing NYC: SEC402 Beta 2	New York, NYUS	Jun 01, 2019 - Jun 02, 2019	Live Event
Enterprise Defense Summit & Training 2019	Redondo Beach, CAUS	Jun 03, 2019 - Jun 10, 2019	Live Event
SANS Zurich June 2019	Zurich, CH	Jun 03, 2019 - Jun 08, 2019	Live Event
SANS London June 2019	London, GB	Jun 03, 2019 - Jun 08, 2019	Live Event
SANS Kansas City 2019	Kansas City, MOUS	Jun 10, 2019 - Jun 15, 2019	Live Event
SANS SEC440 Oslo June 2019	Oslo, NO	Jun 11, 2019 - Jun 12, 2019	Live Event
SANSFIRE 2019	Washington, DCUS	Jun 15, 2019 - Jun 22, 2019	Live Event
Security Operations Summit & Training 2019	New Orleans, LAUS	Jun 24, 2019 - Jul 01, 2019	Live Event
SANS Cyber Defence Canberra 2019	Canberra, AU	Jun 24, 2019 - Jul 13, 2019	Live Event
SANS ICS Europe 2019	Munich, DE	Jun 24, 2019 - Jun 29, 2019	Live Event
SANS Cyber Defence Japan 2019	Tokyo, JP	Jul 01, 2019 - Jul 13, 2019	Live Event
SANS Munich July 2019	Munich, DE	Jul 01, 2019 - Jul 06, 2019	Live Event
SANS Paris July 2019	Paris, FR	Jul 01, 2019 - Jul 06, 2019	Live Event
SANS London July 2019	London, GB	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Cyber Defence Singapore 2019	Singapore, SG	Jul 08, 2019 - Jul 20, 2019	Live Event
SEC450 Security Ops-Analysis Beta 1	Crystal City, VAUS	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Pittsburgh 2019	Pittsburgh, PAUS	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Charlotte 2019	Charlotte, NCUS	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Rocky Mountain 2019	Denver, COUS	Jul 15, 2019 - Jul 20, 2019	Live Event
SANS Columbia 2019	Columbia, MDUS	Jul 15, 2019 - Jul 20, 2019	Live Event
SANS San Francisco Summer 2019	San Francisco, CAUS	Jul 22, 2019 - Jul 27, 2019	Live Event
SANS Pen Test Hackfest Europe 2019	Berlin, DE	Jul 22, 2019 - Jul 28, 2019	Live Event
DFIR Summit & Training 2019	Austin, TXUS	Jul 25, 2019 - Aug 01, 2019	Live Event
SANS Riyadh July 2019	Riyadh, SA	Jul 28, 2019 - Aug 01, 2019	Live Event
SANS Boston Summer 2019	Boston, MAUS	Jul 29, 2019 - Aug 03, 2019	Live Event
SANS July Malaysia 2019	Kuala Lumpur, MY	Jul 29, 2019 - Aug 03, 2019	Live Event
Security Awareness Summit & Training 2019	San Diego, CAUS	Aug 05, 2019 - Aug 14, 2019	Live Event
SANS London August 2019	London, GB	Aug 05, 2019 - Aug 10, 2019	Live Event
SANS Crystal City 2019	Arlington, VAUS	Aug 05, 2019 - Aug 10, 2019	Live Event
SANS Melbourne 2019	Melbourne, AU	Aug 05, 2019 - Aug 10, 2019	Live Event
SANS Krakow May 2019	OnlinePL	May 27, 2019 - Jun 01, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced