Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

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

Tackling ISO 27001: A Project to Build an ISMS

The ISO 27001/27002 standards for implementing an Information Security Management System (ISMS) often present a challenging set of activities to be performed. When a security professional is tasked with implementing a project of this nature, success hinges on the ability to organize, prepare, and plan effectively. This paper addresses the implementation of an ISO 27001 ISMS using the Project Management Body of Knowledge known as the PMBOK Guide published by Project Management Institute, Inc. This paper explores the ...

Copyright SANS Institute

Author Retains Full Rights

AD

Tackling ISO 27001: A Project to Build an ISMS

GCPM Gold Certification

Author: David Henning, daviddhenning@gmail.com

Adviser: Jim Purcell

Accepted: July 22nd 2009

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Abstract.....3

Introduction.....3

Project Initiation..... 5

Project Planning.....7

Project Execution..... 16

Monitoring and Controlling Project Elements21

Closing the Project.....29

Conclusion..... 30

Appendices.....32

References.....33

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

1.Abstract

The ISO 27001/27002 standards for implementing an Information Security Management System (ISMS) often present a challenging set of activities to be performed. When a security professional is tasked with implementing a project of this nature, success hinges on the ability to organize, prepare, and plan effectively. This paper addresses the implementation of an ISO 27001 ISMS using the Project Management Body of Knowledge known as the PMBOK Guide published by Project Management Institute, Inc. This paper explores the process of implementing an Information Security Management System capable of being certified against ISO 27001. It also provides real world concrete examples of the 44 processes in the PMBOK Guide as applied to an information security project at a satellite broadband ISP.

2.Introduction

The International Organization for Standardization (ISO) is familiar for their standards for business quality 9000/9001, CD-ROM file system format 9660, or controversy over Open Office XML (Rooney, 2008). In the realm of information security, the ISO 27001 standard specifies the requirements for an Information Security Management System (ISMS) while ISO/IEC 27002:2005 Code of Practice for Information Security Management (originally known as ISO 17799:2005) defines the set of best practices or guidelines for implementation. (ISO/IEC 27000, 2009; BS ISO/IEC 27001:2005, 2005; BS ISO/IEC 27002:2005, 2007) While 17799/27002 has been used as a best practices document for many years, it is the 27001 standard which is actually audited and certified against. Put another way, the 27002 Code of Practice details many possible controls which may be selected under the guidance of the risk assessment performed per the 27001 standard.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

The Project Management Institute (PMI) publishes A Guide to the Project Management Body of Knowledge (PMBOK Guide). Where ISO 27002 defines a set of IT security best practices resulting in reduced risk of an information security failure, the PMBOK Guide defines a set of best practices reducing the risk of project failure. According to Jim Johnson, Chairman of the Standish Group, the main reason for project success is "Doing projects with iterative processing as opposed to the waterfall method, which called for all project requirements to be defined up front, is a major step forward." (Software Magazine, 2004, 2) The iterative process is exactly what is prescribed in the PMBOK Guide. Johnson also goes on to say, "People have become much more savvy in project management. When we first started the research, project management was a sort of black art. People have spent time trying to get it right and that has also been a major step forward." (Software Magazine, 2004, 5)

Internet Offerings & Telecommunications (IOT) is a fictional ISP used throughout this paper to illustrate examples of implementing ISO 27001 as a project. A project as defined in the PMBOK Guide is temporary in nature, creates unique deliverables, and develops by a process of progressive elaboration (Project Management Institute (PMI), 2004). In the case of IOT, Internetworking Division (ID) management was presented a business case to use ISO 27001 as the ISMS for their National Network Operations (NNO) Payment Card Industry (PCI) network service offerings by the Project Sponsor (Sponsor) and the ID Security Expert (SE). (Wright, 2008) IOT is considered a PCI complaint provider to various enterprise networks performing credit card processing. ID management have chosen to implement ISO 27001 as the ISMS for their PCI transport network environment as a model for future expansion to manage security for the rest of their network operations. The project manager (PM) is charged with ensuring the SE completes of all the necessary documentation, selection and implementation of controls enabling IOT to have their

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

PCI environment certified against ISO 27001. IOT is considered a 'weak matrix' organization as defined in PMBOK Guide. (Project Management Institute (PMI), 2004) The SE reports directly to the Sponsor, not to the PM. The challenges posed by this type of organization are also illustrated here. Finally, a mapping of the ISO control categories to the PCI requirements and a set of project planning templates are included in the Appendix.

3.Project Initiation

The Initiating Process Group is the first of five process groups in the PMBOK Guide, consisting of the Project Charter and the Scope Statement which both fall under the Project Integration Management knowledge area.

Project Integration Management Knowledge Area

Project Charter

The Project Charter provides the management backing needed to get a project started. It formally documents management support, documents the business reasons for doing the project, and provides a high level view of what the project is designed to accomplish and how it will be accomplished. (Project Management Institute (PMI), 2004) In the case of IOT, the ISO/PCI Project (I/PP) is managed by the security group. The purpose of the project is to implement the ISO 27001 ISMS with regard to the PCI transport network environment. IOT management sees the potential to satisfy the business needs of compliance with PCI and possibly Sarbanes-Oxley and personally identifiable information (PII) laws as well. Other business benefits include an improved ability to address customer contractual requirements with regard to network security and having a marketing differentiator to competing ISPs. The description is kept simple; the ISO/PCI Project will create a functioning, certified ISMS for the PCI transport network environment. Success

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

hinges on the ability of the ISMS to pass certification by an ISO 27001 certifying body. Because of a small group and weak-matrix organizational style, many of the key personnel perform multiple duties including being the project manager, project champion, and selection of security controls. Of the three project priorities (Time, Money, Scope/Quality), the most important to IOT management is to keep costs at a minimum. The scope is seen as being narrowly defined to only applying to the PCI environment. However, the scalability of solutions being considered is a factor if management supports future expansion of the ISMS to include non-PCI portions of the business. Time is the one factor which the project manager has been given the most leeway with a loose guideline of 'sometime this year'. The project manager, using the constraints and assumptions given by management, and some expert judgment by the SE from previous experience with ISO, determines the preliminary budget at $30,000 for certification. Other capital budgetary items fall under other PCI spending projects.

Preliminary Scope Statement

The project scope statement defines the project. It details requirements, deliverables, acceptance criteria, constraints, assumptions, risks, work required, and costs. (Project Management Institute (PMI), 2004) The IOT project manager identified a number of deliverables for a functional ISMS as defined by ISO 27001. (ISO/IEC 27000-series Implementers' Forum, 2009; ISO 27000 Directory, 2007) These included security policy documents, an ISMS scope document, a risk assessment, a risk treatment plan, a Statement of Applicability (SoA), selection of controls, implementation of controls, and certification of the ISMS. The assumptions, constraints, acceptance criteria, and initial budget documented in the Project Charter are carried into the scope. The work required is further broken down into an initial Work Breakdown Structure (WBS). The initial WBS consists of the creation of all the

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

documentation associated with each identified deliverable. The Risk Assessment (RA) is further broken down into the components of identifying the RA methodology, performing the RA, and compiling the results. The risk treatment plan is likewise broken into the components of selecting a risk management methodology and creation of the treatment plan.

4.Project Planning

The Project Planning Process Group is the second of five process groups in the PMBOK Guide, consisting of twenty-one (21) processes in all nine (9) project management knowledge areas, Integration, Scope, Time, Cost, Quality, Human Resources, Communications, Risk, and Procurement.

Project Integration Management Knowledge Area

Project Management Plan

The Project Management Plan is a key document for the success of a project. It defines the various other planning needing to be accomplished for a particular project. Corporate culture and project experience come heavily into play as the Project Manager (PM) makes decisions about what components are needed for a particular project. The defined scope and size of the ISO/PCI Project enable the ID project manager to eliminate some sections such as Human Resources Planning because the implementation will be handled primarily by a single employee skilled in ISO and PCI. There just isn't the need for formalized project team development. The PM makes note of this in the Project Management Plan.

Another key decision in the development of the Project Management Plan is to include the other management sub-plans directly in the main document. The primary purpose of this decision is to minimize the amount of documentation updating required as the project progresses.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

One month after creating various project management documents from scratch using internet resources (Baker, 2009; Gordon, 2009; Reynolds, 2009; Stallsworth, 2009), the PM has a discussion with a member of the engineering division of IOT about using an internal document repository to store the I/PP documentation. The PM discovered the engineering team already has certain templates for project management which ID-IOT management could not provide when requested at the start of the project. This is a prime example of how an organization that does not follow strong project management practices leads to inefficiencies within the organization.

Project Scope Management Knowledge Area

Scope Planning and Scope Definition

The project Scope Management Plan is developed as the result of performing the Scope Planning activity. The PM for the I/PP ensured the plan includes the process of how the scope statement is developed and documented, the process for creating the WBS, how the deliverables are verified and accepted, and how changes to project scope are controlled.

Scope Definition is the activity which produces the Project Scope Statement. The scope of the I/PP is focused on implementing the ISO structure for the PCI transport environment.

The PM created a Preliminary Scope Statement as part of project initiation. This document was revised during Scope Planning and Definition to include details not available at the time of project initiation. The PM included details about change management and approval requirements to manage future changes to the scope. Later in the project, the PM followed this management process to include elements of the IOT service provider network not originally considered part of the PCI transport network.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Creating the WBS

The Work Breakdown Structure (WBS) lists the important tasks for the project. The level of detail is variable and depends on what productivity measurements are planned for the project. The main idea is to define WBS elements in terms of work units, either in terms of dollars or period of time which can then be quantified to provide monitoring of progress and cost of the project. (Heldman, 2007)

Researching the process of getting ISO 27001 certified the PM was able to develop the WBS (figure 1) to represent the major deliverables for the project. (ISO 27001 Directory, 2007; ISO/IEC 27000-series Implementers' Forum, 2009) Using the Deming (Shewhart) 'Plan – Do – Check – Act' cycle (BS ISO/IEC 27001:2005, 2005) favored by ISO, the WBS reflects the work units for the major milestones in the ISO process. As shown in Figure 1 below, element 1 Establish ISMS reflects the Plan phase. Element 2 Implement ISMS is the Do phase. Element 3 Internal Audit is the Check phase. Finally, element 4 External Audit is the Act phase. These milestones have been broken down into major deliverables. Later in the project, these were further broken down. One example would be after the completion of the risk assessment. The knowledge gained performing the risk assessment created requirements to implement selected controls to satisfy ISO 27001. These new requirements were added under section 1.4 Select Controls and implemented under 2.1 Risk Treatment.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

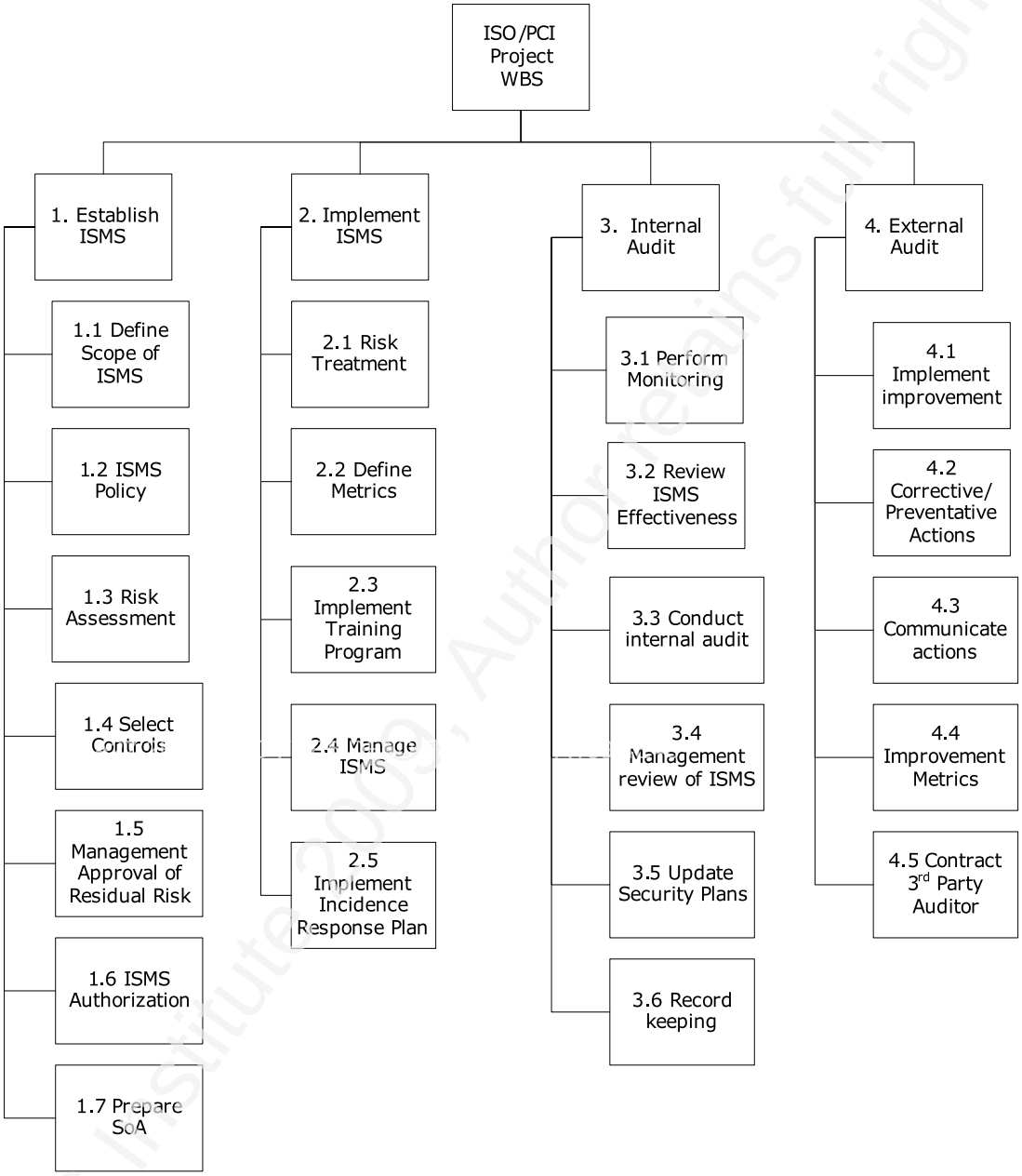

Figure 1

Another item of note is, not all the sub-tasks making up the WBS have to be performed in order. The experience of the project team allowed them to start working on implementing some missing controls before the completion of the risk

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

assessment. This allows parallel work to be performed rather than making resources wait on sequential steps. This is covered further in Activity Sequencing below.

Project Time Management

Activity Definition, Activity Sequencing, Resource Estimating, Duration Estimating, and Schedule Development

"On some projects, especially ones of smaller scope, activity sequencing, activity resource estimating, activity duration estimating, and schedule development are so tightly linked that they are viewed as a single process that can be performed by a person over a relatively short period of time."(Project Management Institute (PMI), 2004)

The PM for the I/PP took this statement to heart and combined these elements to develop the schedule for the project. Based on the WBS, the schedule was broken down by deliverable using estimates based on prior experience. It was clear certain tasks could not be precisely estimated until further into the project because some controls from ISO would be created in whole as opposed to being a refinement of existing PCI controls. The refinement of this schedule is reflected later in the Schedule Control section on the Monitoring and Controlling Process Group.

The PM estimated the major milestones to take approximately one man month each. Two months were also added to the estimated schedule to allow slack for findings from the risk assessment that would add to the overall project task list. The total time to implement the ISMS was estimated to be 6 man months.

As previously mentioned, not all activities for the project have to be run sequentially. While the project was still being planned, the SE was able to research and implement controls known to be required by PCI and able to fulfill ISO prior to the formal risk assessment. Also, some of the policy writing was not completed

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

prior to implementation of technical controls such as the firewall. This allowed the I/PP to integrate scheduling for activities and resource availability with other PCI project work more easily. Time estimates were only documented for specific I/PP activities. Other activities specifically related to the PCI project were not included in the project time estimates.

Project Cost Management Knowledge Area

Cost Estimating and Budgeting

Similar to Project Time Management, Project Cost Management can combine the work of estimating and budgeting costs for small projects. The initial cost estimate of $30,000 for 3rd party audit and project assistance was based on prior experience by the SE. The PM verified this estimate by contacting a qualified ISO certification body and requesting a budgetary quote. The total of the quote was $15,000 to perform the pre-certification audit, application for certification, and Stage 1 and Stage 2 of the certification assessment. Ongoing maintenance of the registration came to another $6,200/year for years 2 and 3 before another full audit of the ISMS would be required.

The project Sponsor was informed of the cost estimate and allocated funding accordingly. In addition to the $15,000 for first year auditing, another $15,000 was allocated for training, materials such as the ISO 27001/27002 standards and policy templates, and consulting services.

Project Quality Management

Quality Planning

The Quality Planning process generates the Quality Management Plan. As mentioned above, this is one of the sub-management plans included in the Project Management Plan. It defines the way in which the project performs quality control,

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

quality assurance, process improvement, and what tools or techniques are used to assess the quality of the project deliverables and ultimately the overall project as a whole. (Heldman, 2007)

The ultimate goal of the I/PP is a binary pass/fail of an audit performed by a 3rd party firm. The PM and Sponsor originally decided they are the arbiters of quality prior to 3rd party assessment. Both the Sponsor and SE have prior experience with PCI assessments and Sarbanes-Oxley (SOX) audits. This experience gives the Sponsor and SE confidence they are able to discern the requirements of ISO 27001 and ensure the ISMS for the PCI environment meets or exceeds them. Additionally, the training budget will pay for a class on the ISO requirements to help the PM understand ISO 27001 implementation and help assess the quality of deliverables. During the Execution phase of the project, the PM enlists the assistance of an internal audit group. This is discussed in the QA section of the Project Execution process group below.

Project Human Resources Management Knowledge Area

Human Resource Planning

Human Resource Planning documents the roles, responsibilities, relationships, and staffing plan. It is more critical based on the scale and relative novelty of the project. For example, when IOT prepared to purchase and launch their first fully owned satellite, many new hires were brought on to the team to manage the operation of the satellite. This required heavy involvement by the IOT HR department.

The I/PP project does not require new hires. The weak matrix nature of the organization also precludes any changes to staffing or management chains. The success of the project relied on the PM to work with other functional group managers to have buy-in and assign their resources to assist where needed. The lack of direct

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

management was noted by the PM in the risk register as a possible risk to the project success.

Project Communications Management Knowledge Area

Communications Planning

The intention of the Communications Management Plan is to document what information needs to be communicated, why it needs to be communicated, when and with what frequency, the format, and who is responsible for communicating the information. (Project Management Institute (PMI), 2004) The plan documents the stakeholder requirements, defines information for communication, the roles and responsibilities of stakeholders, methods (e-mail, phone, signed documents), frequency, escalation, change control of the plan, tools and techniques, and a glossary of terms. (Project Management Institute (PMI), 2004) This planning becomes more important as the number of stakeholders increases but the number is not very large. The number of communication channels is represented by the formula n(n-1)/2 where n=number of stakeholders.(Heldman, 2007) For example, a project with 4 people has 4(3)/2 = 6 communication channels to manage. A general guideline is to keep the number of stakeholders below 10 and communication channels below 45. (The SANS Institute, 2008 525.4 2-45) One method to handle larger numbers is to assign a single contact point for a group of stakeholders. This individual is then responsible to communicate to and from the group they represent.

The PM, SE, and Sponsor are the main communicants for the I/PP project. Using the previous formula gives a total of three communication channels. The PM and Sponsor take it upon themselves to communicate with any other entities such as internal audit or ID management as part of managing the stakeholders.

Project Risk Management Knowledge Area

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Risk Management Plan

In terms of project management, risk is defined as uncertainty. It can be either a positive or negative. (The SANS Institute, 2008 525.5 2-5) For example, a competing project could be terminated due to poor planning. The resources for the competing project are now available for projects being properly managed. A second aspect of risk is the probability of a risk is never absolute. (The SANS Institute, 2008 525.5 2-5) If the probability were zero, by definition it cannot happen and is not a risk. If the probability were 100%, by definition the event will happen and you must be prepared to deal with it when it does. Thirdly, the risks being planned for are directly to the success of the project, not to other aspects of the business or network security.

The Risk Management Plan is created in order to prepare the project for risk events if or when they occur. The plan defines the methodology for assessing project risk. It assigns roles and responsibilities, addresses budgeting and timing, documents stakeholder risk tolerances, as well as the reporting and tracking of risks and responses. (Project Management Institute (PMI), 2004)

The Risk Management Plan developed by the PM assesses risk to the project qualitatively and not quantitatively because the PM felt the difficulties of quantitative assessment outweighed the benefits of putting dollar amounts of risk to a project of only $30,000. The PM created a risk matrix using probability values (0.1, 0.3, 0.5, 0.7, and 0.9) and impact of High (5), Medium (3), and Low (1). The risk categories identified by the PM are Personnel, Technological, Services, and Organizational. These categories are later used when developing the risk registry that identifies specific project risks.

Project Procurement Management Knowledge Area

Purchases, Acquisitions, and Contracts

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

The Procurement Management Plan defines the types of contracts the company is willing to consider such as fixed price or time and materials. The plan details the authority of project team members in the purchasing process. It also covers how vendors are selected, integration of purchasing into the scheduling of project work, and standard processes the company uses when purchasing goods or services. (Project Management Institute (PMI), 2004) The level of integration varies from company to company. Some organizations have the project team handle procurement while other companies employ dedicated purchasing groups to handle all the negotiations with vendors.

IOT has a dedicated purchasing department. The process is tightly controlled with little variation. The PM documents the process in the Procurement Management Plan. IOT only negotiates firm fixed price contracts for services. The SE and PM researched up to four vendors for the 3rd party assessment and send request for proposal (RFP) to them. The RFP responses lead the SE and PM to request two vendors to perform on-site presentations. The SE and PM then rank each vendor according to a criteria matrix with categories of RFP Response, Vendor Presentation, and Price. The data from this assessment along with a recommendation of one vendor is given to the IOT purchasing group to negotiate price and contract details.

5.Project Execution

The Project Execution Process Group is the third of five process groups in the PMBOK Guide, consisting of seven (7) processes in five (5) project management knowledge areas, Integration, Quality, Human Resources, Communications, and Procurement. The Execution Process Group is the phase of the project where the most activity producing deliverables is accomplished.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Project Integration Management Knowledge Area

Managing Project Execution

Managing the execution of a project requires using the project management plan, approved corrective or preventive actions, change requests, defect repairs, and administrative closure procedures to generate the requested changes, deliverables, and performance information. (Project Management Institute (PMI), 2004) More simply, this is the macro level of project activity accomplishing the bulk of project productivity. While other aspects of a project have more narrowly defined interactions, this process interacts with every other individual process in the PMBOK Guide.

Because this process is so central to the activities of a project, there are many examples to choose from to illustrate this group. A prime example is the change management process. Requests for changes can feed in from twenty-three of the forty-four processes. While the SE is busy performing the work during the execution phase, the PM must manage the changes coming in. For this project, the PM had to update the WBS after the ISO 27001 Risk Assessment allowed for more details to be added to the work required. Updates to the schedule flowed from this as well. The addition of assistance from internal audit required some project management to coordinate the activity. Even the risk registry required an update after the PM learned of the purchasing issue illustrated below in the Soliciting and Selecting Sellers process.

Project Quality Management Knowledge Area

Performing Quality Assurance

The act of Performing Quality Assurance (QA) results in requested changes, corrective actions, and updates to assets and the project management plan. (Project

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Management Institute (PMI), 2004) It is the managed implementation of planned quality control (QC) activities to ensure the product meets the standards described in the project management plan. If a defect is found during quality control (QC) the reason for the defect is corrected by the actions taken in QA.

During this Execution phase, the PM attended training on ISO 27001. One item the PM learned was about performing internal auditing prior to hiring a 3rd party firm for the formal audit. IOT has an internal audit group (IAG) for SOX and other auditing functions. The PM contacted the head of IAG and got commitment for up to 10 man days of assistance with the I/PP internal audit once the project team felt prepared. The PM then put this addition through Change Control to formalize it into the project.

Project Human Resources Management Knowledge Area

Acquire Project Team

Acquiring the Project Team involves getting the personnel needed to accomplish the various tasks of a project assigned to do the work. It may involve outside contractors or consultants. In that case, the process must also interact with the procurement process to ensure contracts are established clearly defining the work to be performed and the expected output.

As previously mentioned, this phase was not performed in a formal way during the I/PP project at IOT due to perceived lack of need. Rather, the PM worked with group managers for system support, audit, and development, to get small resource commitments as needed during the project. For system support and development, the work performed for the I/PP project dovetailed with work being performed for other PCI initiatives within IOT and only 5 man days (3 from system support, 2 from development) were needed. The bigger commitment came from IAG spending a number of days to familiarize with the ISO 27001 standard and then performing the

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

internal audit for a total of 10 man days.

Develop Project Team

Developing the project team helps project performance by making the team members work together more efficiently. The tools consist of general management skills, training of team members, team building exercises, clear ground rules, recognition and rewards, and possibly co-location. Results of this process should be improvements to project team effectiveness and reduced staff turnover. Again, for the I/PP project, there was no formal team development. For an organization with new people, this could hinder productivity and efficiency as the team members learn to interact and work together effectively. The team at IOT has already been working together for over a year so team cohesiveness was already well established.

Project Communications Management Knowledge Area

Information Distribution

This process is the activity of reporting information to stakeholders according to the Communications Management Plan. It involves using written and oral communication skills, the ability to gather information, appropriate distribution media, and a lessons learned process. (Project Management Institute (PMI), 2004) The results of this process are updated organizational assets and requested changes.

The PM handled most of the project communication efforts with some assistance from the Sponsor. The assistance was primarily due to the Sponsor having a longer standing presence in the company and established working relationships, especially with the ID management chain. Numerous meetings were required throughout the life of the project to discuss planning and any change requests. E-mail was used to follow up with meeting notes, plan future meetings, and send documents to stakeholders. The team also made use of an internal

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

documentation system which allowed for tight document revision management in an automated manner. The documentation system enabled feedback to be given at the convenience of individual schedules. Once feedback was collected, follow-on meetings to discuss changes were kept efficient by not getting bogged down in discussions of mutually accepted items.

Project Procurement Management Knowledge Area

Soliciting and Selecting Sellers

The PMBOK Guide separates the solicitation and selection of sellers into two distinct processes. However, common practice is to combine these activities under a single process. Solicitation involves contacting vendors of a particular product or service. In very formal situations, a Request for Proposal (RFP) or similar document is generated to elicit responses from a variety of vendors. The responses to the RFP become inputs into the selection process. Clearly documented evaluation criteria in the Procurement Management Plan make the task of selection more efficient.

As previously mentioned, the SE and PM worked to identify vendors and create an RFP. The RFP responses were evaluated based on how well the vendors responded to individual components of the RFP. For example, the RFP requested the names and work experience of the proposed auditors. One vendor chose not to submit the actual names or detailed history. Subsequently, the SE and PM both gave a lower score to that section of the response.

Another purchasing issue arose after a discussion between the PM and an IOT employee outside of the ID division. The employee had been working with a vendor for weeks to buy server equipment. After the recommendation had been sent to the purchasing group, he had assumed the vendor of choice would be selected. Instead, purchasing found another vendor selling the same equipment cheaper and made a deal. The employee only found out after the purchase order was sent to the new

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

vendor. The PM decided this was a potential risk to the I/PP project and updated the risk registry through the change control process. The PM and Sponsor then worked out a mitigation strategy to increase the regular communication with the purchasing agent in an effort to prevent surprise changes.

6. Monitoring and Controlling Project Elements

The Project Monitoring & Controlling Process Group is the fourth of five process groups in the PMBOK Guide, consisting of twelve (12) processes in all nine (9) project management knowledge areas, Integration, Scope, Time, Cost, Quality, Human Resources, Communications, Risk, and Procurement. The Monitoring & Controlling Process Group is the phase of the project where project performance is evaluated. Feedback from the performance evaluation goes back into the Project Execution cycle until moving into the project closing phase.

Project Integration Management Knowledge Area

Monitoring Project Work

This continual process is focused on improvement to the performance of the project. It can be thought of as performing QA against the other four process groups (Initiating, Planning, Executing, and Closing) to check the project is performing according to the plan. The main tools are the chosen project management methodology, a project management information system (PMIS) to automate aspects of project management, the earned value technique (EV), and expert judgment. (Project Management Institute (PMI), 2004) The results of this process are recommended improvements to increase project performance and better forecast future project work.

The PM primarily performed this process to assess the need for taking action to keep the project moving forward, to assess risk, and maintain project

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

documentation. There was little value to performing the earned value technique. EV compares completed work to the budget. The formula is EV=Budget x Completion where Budget is in dollars and Completion is a percentage. (Heldman, 2007) For the I/PP, if completion is 50% and budget is $30,000 then the EV=$15,000.

However, EV alone does not tell enough about the performance of the project. Cost variance (CV) can give an indication of how the project is performing in regard to spending. CV is equal to EV minus the actual cost (AC, the money spent so far). (Heldman, 2007) However, since the I/PP will not spend much budget until the actual audit, this number would be skewed to look like the project was performing perfectly as AC would be zero. To illustrate, CV=EV-AC at 50% project completion would be equal to EV. There is no variance. On a project spending budget over time, this variance can be either a positive or negative number. When CV is positive, the project has spent less than planned. When CV is negative, the project has spent more than planned to this point. An experienced PM knows variance does not necessarily mean the project is doing well or poorly. It means things are not going as planned and the reason for the variance should be analyzed to see if corrective actions need to be taken.

Likewise, another measure using EV is to calculate schedule performance using Schedule Variance (SV). SV is equal to EV minus the Planned Value (PV) which is the amount of budget planned to be spent at this point in the project. (Heldman, 2007) In this case, because there is no planned spending PV=0 for most of the project. Again, SV is equal to EV until very late in the project when the spending occurs on the assessment. Also, because there are no hard deadlines for scheduling, there is little value in formal project performance review. Rather, the Sponsor and management team follow the project progress and evaluate performance based on steady progress being shown by the PM and SE.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Finally, there are other performance indexes and forecasting that make use of EV as well. The cost performance index (CPI), schedule performance index (SPI), estimate to completion (ETC), and estimate at completion (EAC) can give indications of performance (CPI and SPI) or forecasts (ETC and EAC). The performance indexes represent the values as a percentage where 1.00 (100%) is performing exactly as expected. Anything higher than 1 is generally good (i.e. the team really is performing at 110%) and below 1 is not. ETC and EAC give dollar amounts on how much money is yet to be spent on the project while taking variances into account. Again, because there was little value to formal performance analysis on the I/PP, these were not used by the PM.

Integrated Change Control

Integrated Change Control is another continual process in project management. Having strong change controls prevents scope creep and incorporates alterations to the project plan. As previously mentioned, project management is an iterative process. A project is rarely defined with 100% accuracy at the start with every detail known up front and accounted for, preventing a need for changes. Rather, a project gets enough information to get the ball rolling while the re-iteration of the project plan allows the path to be laid out as needed.

The PM for the I/PP had to put a number of changes through the change control process. The change requests that came about through the Manage Project Execution process were fed into the Integrated Change Control process. Manage Project Execution worked to identify the needed changes and implement approved changes. Integrated Change Control is how requested changes were approved or rejected and any updates to project scope or management plans were created. Being a small project made this simpler than projects with larger numbers of stakeholders to consider. Larger projects make use of a change control board with

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

representatives from major components working together to assess the impact of changes.

Project Scope Management Knowledge Area

Scope Verification and Control

Scope Verification and Scope Control are two processes in PMBOK which can be combined as well. Verification gets formal acceptance of scope by the stakeholders. Control is the process by which any changes to scope are fed back through the overall Change Control process. If verification results in requested changes rather than acceptance, the changes must go through change control and be accepted. Changes to scope can result in what is known as scope creep.

The I/PP project scope had one major change (and a few minor) during the life of the project. The PCI approved transport network makes use of microwave frequencies in the Ku spectrum. Recently, IOT had launched an upgraded service using Ka frequencies initially for consumer based customers. The Ka system had not yet been assessed for PCI compliance when the sales force at IOT sold the upgraded system capabilities to an existing enterprise customer using Ku based PCI compliant transport. This meant the Ka system now had to become PCI compliant. The original scope of networks and devices included into the I/PP was changed to accommodate the Ka system.

Project Time Management Knowledge Area

Schedule Control

Performing Schedule Control focuses on monitoring when the project schedule is not performing according to plan and managing any changes to the schedule. The result may be a change to the expected completion date or recommendation for corrective actions to get the schedule back on track. The schedule variance and

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

schedule performance index (SV and SPI) explained previously in Monitoring and Controlling Project Work are typically applied here.

The open ended schedule for the I/PP meant the PM did not perform formal schedule performance measurements or variance analysis. Rather, the PM made use of project management software to monitor completion of tasks and milestones. Elements of the project having dependencies were followed more closely to ensure work on a predecessor is completed satisfactorily before having the SE continue on to the successor activity. Ultimately, the project did take two months longer than the initial schedule estimate. This was due to certain ISO controls like business continuity planning and disaster recovery taking longer to implement.

Project Cost Management Knowledge Area

Cost Control

The Cost Control process is tightly linked to Integrated Change Control. The importance of cost control is directly related to the overall project budget. The purpose of cost control is to assess the monetary impact of changes and ensure the project costs do not exceed budget without being approved overruns. (Heldman, 2007)

The PM did not run into any cost overrun issues during the I/PP. The expansion of scope to include the new Ka product offering did not change the level of effort for the 3rd party ISO audit which was the largest budget item of the project. Again, due to the small budgetary size and lack of continuous spending during the project, no formal performance measurement of earned value or forecasting were performed.

Project Quality Management Knowledge Area

Quality Control

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

The Quality Control (QC) process checks the project deliverables meet the specifications originally described in the Quality Management Plan. QC also checks the project is being managed effectively by analyzing schedule or cost performance. Any variances are documented and methods to eliminate them are identified. The recommended fixes are then fed into Change Control for review and approval.

As already mentioned, schedule and cost performance were not performed for this project. Deliverables from the SE were reviewed by the PM and Sponsor initially. Once all the documentation and selected controls were implemented, the IOT internal audit team performed an audit. Findings from the audit included employees not following the clear desk policy, weaknesses in contracts with 3rd parties, and portions of the business continuity plan were deficient. These findings lead to change requests processed per Manage Project Execution and Integrated Change Control as mentioned previously.

Project Human Resources Management Knowledge Area

Managing the Project Team

This process monitors and appraises the performance of individual team members, manages conflict, and resolves issues. The type of organization (Functional, Projectized, Matrix, or Composite) plays a large role in the effective management of a project team. In cases like a Matrix organization, team members are not accountable to the project manager which increases the difficulty of prioritizing team member activity.

Formal management of the team is not something a PM in a weak-matrix organization typically does. Also, for IOT, the PM and SE were essentially peers in the organization both managed by the Sponsor. This can present a challenge if team members choose to ignore the direction of the PM in favor of other priorities. A successful PM finds ways to keep the project work moving forward. At IOT, the PM

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

communicated regularly with the Sponsor to ensure the Sponsor saw the importance of the required work. The PM also requested the Sponsor task the SE rather than trying to task the SE directly.

Project Communications Management Knowledge Area

Performance Reporting

Performance Reporting collects baseline performance data and distributes it to stakeholders. (Project Management Institute (PMI), 2004) It covers scope, schedule, cost, quality, and may include risk handling or procurement. Communication of the reports follows the Communications Plan established during the planning phase.

The majority of performance reporting occurred informally between the PM and Sponsor during weekly face to face meetings. The results of these meetings were corrective actions such as updates to the WBS, requested changes, or a push by the PM to have the Sponsor task the SE. After completion of the 3rd party audit, a formal presentation was made to management showing how the project had been accomplished and the newly certified environment could be marketed.

Managing Stakeholders

This process is part of the communications process to ensure stakeholders are informed of issues as they arise during the project. Keeping stakeholders informed improves the chances the project stays on track. Issues are typically resolved by the project manager holding face to face meetings with stakeholders.

Throughout the project the PM held stakeholder meetings to keep them informed about progress, changes, and issues. The biggest change was the addition of the Ka product line into the scope of the project. Luckily for the PM and IOT, the Ka product line had been developed with strong security controls from the ground up. The increased scope did not result in increased workload or cost disruptive to

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

the project.

Project Risk Management Knowledge Area

Risk Monitoring and Control

Risk Monitoring and Control manages existing risks, monitors for newly discovered risks, and feeds updates or recommendations through Change Control to the Risk Register or Risk Management Plan. It is accomplished via risk reassessment, audits, trend analysis, performance measurements, reserve analysis, and status meetings. (Project Management Institute (PMI), 2004) It supplements planned responses to identified risks that are part of the initial Risk Management Plan.

During the project, the PM tracked the items in the risk registry. One item was scope creep which the PM originally listed as a low impact of 1 and a probability of 0.1 resulting in a score of 0.1, the lowest possible risk score. Realizing the new Ka system needed inclusion caused the PM to reassess this particular risk. Before assigning a new risk score, the PM and SE worked through a PCI Self Assessment Questionnaire (PCI Security Standards Council, 2008) to determine the level of effort required to incorporate the new system. This resulted in a change to the impact from 1 to 5 and probability changed from 0.1 to 0.3. This resulted in a new score of 1.5 which was considered medium. The change was also put through the change control process and documented.

Project Procurement Management Knowledge Area

Contract Administration

Performing Contract Administration ensures the contracted vendor meets the terms established by the contract. It manages the financial obligation of the organization by sending payments on time. It also reviews and documents the performance of the vendor which may impact the qualified vendor list used to select

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

vendors for future projects.

The vendor for the 3rd party assessment was chosen after following the Procurement Management Plan and having the IOT purchasing group negotiate the deal. Administering the contract entailed communication from the PM to the purchasing group announcing satisfaction of the contract terms for the initial audit. The purchasing group then sent payment to the auditor per the negotiated terms.

7. Closing the Project

The Project Closing Process Group is the last of five process groups in the PMBOK Guide, consisting of two (2) processes in two (2) project management knowledge areas, Integration and Procurement. The Closing Process Group is the phase of the project where the most activity gets done.

Project Integration Management Knowledge Area

Close Project

Closing the project involves the administrative work of collecting documentation of formal product acceptance, associated project files, and any activities needed to transfer the project into a production or operations environment. (Project Management Institute (PMI), 2004) It should list specific activities required for formal acceptance and exit criteria for the project.

The IOT I/PP maintained a very simple exit criteria of attaining certification of the ISMS. The PM, SE, and Sponsor worked with the vendor to perform an initial two day ISO-pre audit. This was followed by seven days of auditing split between one-and-a-half days for documentation review and five-and-a-half days for auditing of implemented controls. The PM and Sponsor made certain the auditor was given access to all the required documentation. The SE worked to show the auditor examples of required controls. The vendor then formally registered the IOT ISMS

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

and a certificate was granted, fulfilling the success criteria laid out in the Project Scope Statement.

Project Procurement Management Knowledge Area

Closing Contracts

Contract closure verifies all work and deliverables have been accepted. Payments have been delivered. Records are updated and saved for future projects. When a project is completed successfully, this process is typically straightforward. However, should a contract need to be terminated early, either by mutual agreement or default on the part of one of the parties, this process can become much more complicated. (Heldman, 2007)

Once the contracted work was complete and the ISMS certified and registered, the Sponsor confirmed with purchasing the auditing terms of the contract had been satisfied. However, the contract includes two follow on years of registration maintenance. Because the maintenance of the ISMS is an ongoing operation, the follow-on portions of the contract were managed by the operations team. This allowed for the project to be formally closed.

8. Conclusion

This paper has shown one set of choices for performing project management to implement the ISO 27001:2005 standard. Certainly there are many factors unique to an organization influencing the decisions when choosing which project management processes to implement and which to avoid. The experience of the project manager, the corporate structure and culture, and the needs of the project are all important factors to weigh when performing project management.

Ultimately, the foundations of success stemmed from a combination of management support and a project manager able to plan, communicate, negotiate,

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

and step up to lead the team from inception to completion. IOT now has a functioning Information Security Management System for their PCI transport environment. Seeing success on a smaller, manageable scale encouraged IOT management to expand their ISMS capabilities into other aspects of the organization. The successful implementation of ISO 27001:2005 also enabled IOT to further differentiate itself from competitors in the broadband over satellite marketplace.

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

9.Appendices

ISO 27001 to PCI 1.2 mapping

Included below is a mapping of ISO 27001:2005 control objectives and matching controls from PCI version 1.2. This is provided as educational reference. Note implementing **only** the controls listed in version 1.2 of the PCI standard is not likely to warrant certification under ISO and the author makes no claims as to the appropriateness or effectiveness of these controls for the reader's environment.

ISO-PCI_v1.2_mappi
ng.xlsx

Sample Templates

Included here are sample templates of the Charter, Preliminary Scope, Scope, Project Management Plan, WBS, and Risk Register for the IOT I/PP project.

ISO_27001_PCI_Cha
rter GIAC Appx.docx

Preliminary Scope
Statement GIAC App

Scope Statement
GIAC Appx.docx

ProjectMgmtPlan
GIAC Appx.docx

WBS_GIAC
Appx.docx

RiskRegister GIAC
Appx.xlsm

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

10.References

Baker, Natasha (2009). Project Charter Example for Every Project Manager. Retrieved 2009, from Bright Hub Web site: http://www.brighthub.com/office/project-management/articles/5159.aspx

BS ISO/IEC 27001:2005 (2005). Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2005).London, England: British Standards Institute.

BS ISO/IEC 27002:2005 (2007). Information technology – Security techniques – Information security management systems – Code of practice for information security management (BS ISO/IEC 27002:2005 incorporating corrigendum no. 1). London, England: British Standards Institute.

Gordon, Ann (2009). What is a Work Breakdown Structure? Retrieved 2009, from Bright Hub Web site: http://www.brighthub.com/office/project-management/articles/2645.aspx

Heldman, Kim (2007). PMP Project Management Professional Exam Study Guide Fourth Edition. Indianapolis, Indiana: Wiley Publishing, Inc..

ISO 27000 Directory (2007). The ISO27001 Certification Process. Retrieved 2009, from The ISO 27000 Directory Web site: http://www.27000.org/ismsprocess.htm

ISO/IEC 27000-series Implementers' Forum (2009). ISO27k Toolkit. Retrieved 2009 from http://iso27001security.com/html/iso27k_toolkit.html.

ISO/IEC 27000 (2009, May 1). Information technology – Security techniques – Information security management systems – Overview and Vocabulary (ISO/IEC 27000:2009). Geneva, Switzerland: ISO/IEC.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

PCI Security Standards Council (October, 2008). PCI SSC New Self-Assessment Questionnaire (SAQ) Summary V1.2. from PCI Security Standards Council Web site: https://www.pcisecuritystandards.org/saq/instructions_dss.shtml

Project Management Institute (PMI). (2004). A Guide to the Project Management Body of Knowledge (PMBOK Guide). Philadelphia, Pennsylvania: PMI.

Reynolds, Deanna (2009). Free Project Management Forms & Templates You Can Download. Retrieved 2009, from Bright Hub Web site: http://www.brighthub.com/office/project-management/articles/26131.aspx

Rooney, Paula (2008, April 1). Ubuntu's Shuttleworth blames ISO for OOXML's win. Retrieved from ZDNet Technology News Web site: http://blogs.zdnet.com/open-source/?p=2222

Stallsworth, Eric (2009). How To Write A Scope Statement. Retrieved 2009, from Bright Hub Web site: http://www.brighthub.com/office/project-management/articles/2491.aspx

Software Magazine (2004, Jan 15). Standish: Project Success Rates Improved Over 10 Years. Retrieved 2009, from Software Magazine Web site: http://www.softwaremag.com/L.cfm?doc=newsletter/2004-01-15/Standish

The SANS Institute, (2008). Management 525 Project Management And Effective Communications For Security Professionals And Managers: Quality And Risk Management. Bethesda, MD: The SANS Institute.

Wright, Steve (2008). Using ISO 27001 for PCI DSS Compliance. Retrieved 2009, from http://www.insight.co.uk/files/whitepapers/Using%20ISO%2027001%20for%20PCI%20DSS%20Compliance%20(White%20paper).pdf

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 1st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced