Considerations for Information Security in Projects[1]

By Neelov Kar

Abstract

Use of information in our daily life has become essential in the 21st century. Projects are planned and executed based on a plethora of information that has accumulated in the past or has been generated during the process. Information processing has become a part and parcel of any project, whether it is constructing a high rise condo, building a nuclear submarine, developing a new application, building a new hospital or manufacturing a self-driving car. On one hand information helps us to develop a sophisticated service but at the same time it becomes our responsibility to protect it from unauthorized access.

We deal with sensitive information such as intellectual property or personally identifiable information. For example, we cannot think of building a new hospital without an integrated information processing system that is interfaced with the medical devices used in different departments such as radiology or pathology etc., as well as the front office where patient registration happens. At every step of the way we are either receiving sensitive information from the patient or generating new information during the service or storing the information for future use.

During the project planning we must analyze the security exposer and should plan to protect the information. Some of the international standards define this as mandatory requirements. The author would like to provide the basic requirements from different international standards such as ISO 27001, ISO 27018, PCI, SSAE16 and CSA STAR that are relevant for project initiation, planning, execution, control and closing phases.

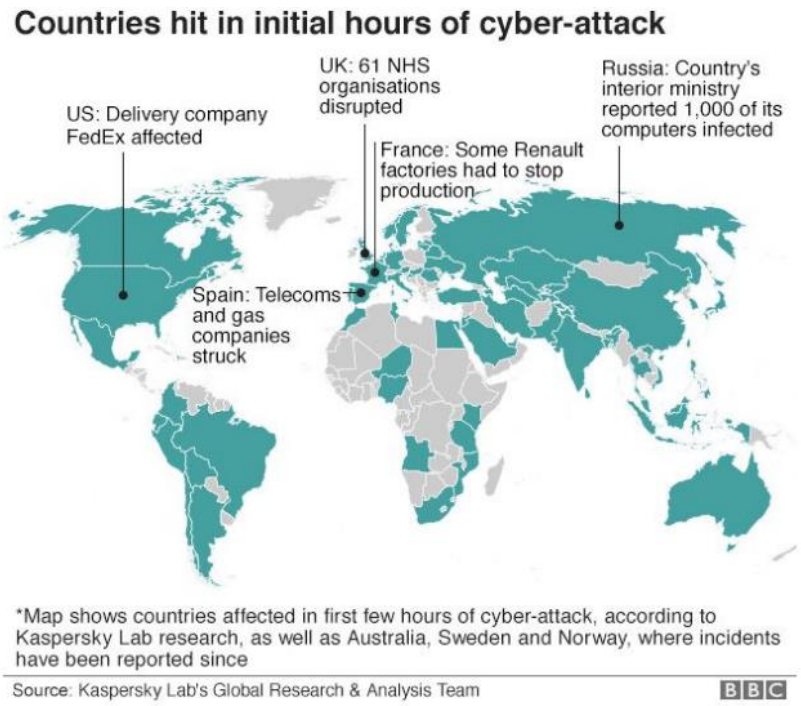
Introduction

Information technology is part of our daily life. As a project manager we use social media, web based application and other IT tools to manage our projects. People are biggest risk for information security. We need to be careful about who we recruit and how we maintain the information security discipline in the team. We not only have to protect the project information but also need to analyze if there is any security vulnerability that can impact information security of the project. Here are some examples that can happen to your projects.

[1] *Editor's note: Second Editions are previously published papers that have continued relevance in today's project management world, or which were originally published in conference proceedings or in a language other than English. Original publication acknowledged; authors retain copyright. This paper was originally presented at the 11th Annual UT Dallas Project Management Symposium in August 2017. It is republished here with the permission of the author and conference organizers.*

This exhibit demonstrates how a disgruntled employee can damage the operation of an organization

Pic 1: Disgruntled employee



This exhibit demonstrates how cyber-attack damage can be so extensive. People in the project should be trained on information security awareness which should include:

- Not to open any phishing email
- Not to respond to suspicious emails
- Not to download unlicensed software
- Using anti-malware on their computers
- Not to visit obnoxious sites

Pic 2: Recent issue with Wannacry

Security Vulnerability in Projects

Information security shall be addressed in project management, regardless of the type of the project. - *ISO 27001:2013 A.6.1.5*

It is recommended to review the information security impact of all projects and identify action to mitigate the risks. Let us look at what are the vulnerabilities that a project may be exposed to.

Following table provides the specific actions that maybe taken at project, program and portfolio levels to address the security vulnerabilities. The PMO should have resource to identify the information security impacts to the organization executing the projects and to the organization the project is implemented for. An information security expert may be appointed

at PMO whose responsibility will be to provide expert advice at the project, program and portfolio level to assess the information security impact of projects. It may be a good idea to have a section in the Project Charter where the presence/absence of information security will be detailed. It is recommended that no projects should be initiated without a sign off from InfoSec SME and no projects should be implement without a sign off form him/her. This person will also review the artifacts at different stages of the project to verify that proper due diligence has been used.

Aspects of Information Security	Project Management	Program Management	Portfolio Management
Impact on Confidentiality, Integrity & Availability (CIA)	Understanding the Impact of Information Security in Projects	Combine projects with similar information security requirements	Keep a watch in the industry regarding Threats and Vulnerabilities
InfoSec Resource	Applying Information Security in Different Knowledge Areas	Share InfoSec Expert across projects	CISO screens the projects for Information Security exposure
Protection	Protecting the Project Information	Protecting the Program Information	Protecting the Portfolio Information
Governance	Applying Information Security in Different Knowledge Areas	Oversee that information security practices followed across the projects	Consider Information Security criticality as one of the prioritization criteria

Table 1

Sensitive Information Type

In projects we deal with various different types of information. The type of information depends upon the kind of project that is being implemented. Following are some information type that may be involved in your projects that may be vulnerable for security attacks:

- PII/ PCI/ PHI

  In a project we may be dealing with personal data like an individual's name, address, SSN, MMN, DOB or we may be implementing a project that will process individual's credit card information or it could be handling individual's health information.

- Customer Data

  Customer data is always considered as confidential and proper care should be taken to protect it from loss and unauthorized modification.

- Company Internal

  There are host of company information that needs to be protected from unauthorized access such as product pricing, information about key resources, or customer list etc.

- Intellectual Property

  More often than not organization will have their own intellectual properties like copyrights or patents which need to be protected from theft.

- Project Critical Milestones

  Sometimes the critical milestones are kept as confidential information.

- Project Database

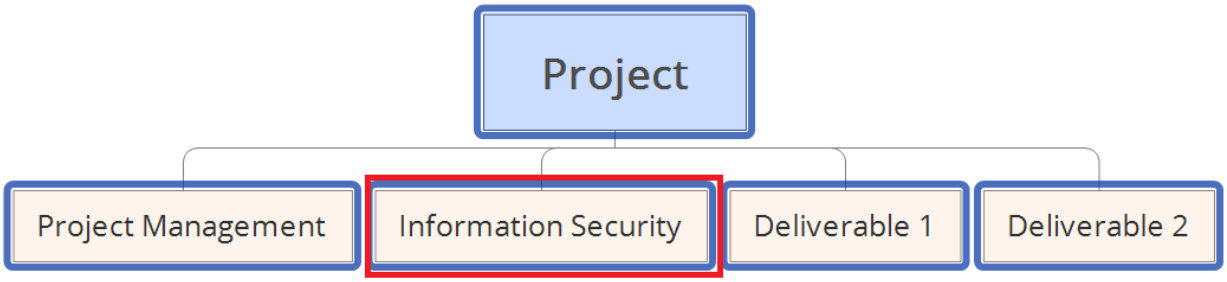
  Project database is a very valuable information that is created based on implementation of multiple projects in past. This database is the source of risks, estimates, project templates, resource skillsets and various other information which is used to configure future projects. This database must be protected from not only unauthorized access but also any malicious actions or natural disasters.

Addressing Information Security in Projects

In the following section we will find out how the information security can be applied at various stages of projects. Information security has direct impacts on Scope Management, Risk Management, HR Management, Stakeholder Management, Communication Management, Procurement Management and Integration Management (Change).

Scope Management:

As we all practice project management we always by default use one of the deliverables of WBS as “Project Management”. Because of importance of information security it may be beneficial to have another mandatory deliverable as “Information Security”. As mentioned above it is required to evaluate the impact of information security on the project at the beginning. The InfoSec Expert will determine if the project requires a deliverable as information security to be included.



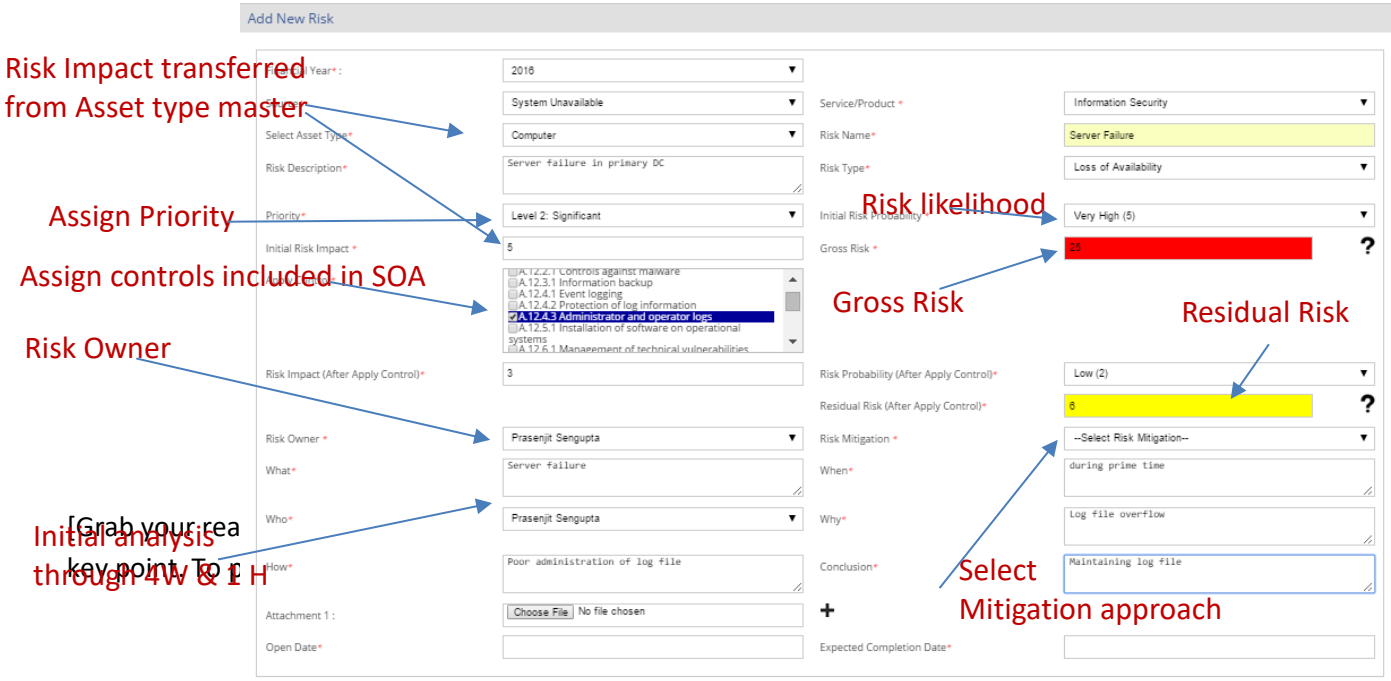
Pic -3

Risk Management:

Risk management is a very important area of information security. As we discussed above there could be various possibilities of security breaches during the implementation of a project. Typically, risk management aspect of PMBOK focuses on unexpected events that can impact the projects scope, schedule and resources. It will be beneficial to evaluate risks from information security angle that can disrupt the project or it can bring it to a standstill situation if we do not mitigate the risk arising from security breaches.

> ***ISO 27001:2013 6.1.3 Information security risk treatment***
> *The organization shall define and apply an information security risk treatment process to:*
> *a) select appropriate information security risk treatment options, taking account of the risk assessment results;*
> *b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;*

The following screenshot from ISO-Metrics demonstrates how a risk can be documented and how controls are applied to process the risk by adopting risk mitigation approaches like avoid, transfer or reduction of risk.



Pic - 4

Communication Management

ISO 27000 also suggests to identify all the possible communications in a project similarly as defined by PMBOK. Here the focus is from information security perspective.

ISO 27001:2013, Clause7.4 Communication

The organization shall determine the need for internal and external communications relevant to the
information security management system including:
a) on what to communicate;
b) when to communicate;
c) with whom to communicate;
d) who shall communicate; and
e) the processes by which communication shall be effected

Following table provides some communication example that can happen from information security perspective.

Message	Target	Media	Description Purpose	Frequency	Owner	Comments
System outage notices	Employees of affected department, involved supplier	Phone call, Email	Updates on if they should go home and ETA	As needed	IT Department, Upper management	IT updates on the fix or ETA of fix and will call the involved supplier. Management will decide if employees need to go home.
ISMS Document changes	Employees	Meeting, Email	Informs staff and employees about new policies	Yearly	Upper management	Communicated from managers to their staff
Security Breaches	Client impacted, Management, employees	Email, phone call, person to person	To stop the breach. Make affected clients aware of possible data loss	As Needed	All	

Table 2

Procurement Management

Supplier Selection

Most of the times we use suppliers in our projects and it is common to share information with them about the project. As we have seen above projects deal with sensitive data, it is possible that some of it is also shared with our suppliers.

We have to be careful in selecting our suppliers. It is a good idea to address the risk associated with suppliers accessing our information.

> *A.15.1.1 Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.*

Supplier Evaluation

In a typical organization we use the suppliers on a long term basis and we have some service level expectations. It is a good practice to document these expectation and agree with the supplier.

A.15.1.2 All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

Information Exchange with Third Parties

Suppliers are considered as third parties. It is a good practice to mention the secured mode of transfer of information in the agreement.

A.15.1.3 Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

A.13.2.2 Agreements shall address the secure transfer of business information between the organization and external parties.

Undertaking from Suppliers that they will run the test in safe mode

It is pretty common to have our suppliers provide services like review of the work or testing some artifacts or sometimes provide some technical support in the project. It is very important to make sure they are aware of the criticality of the system, especially the production system. Therefore, it is a good idea to take an undertaking from them stating that they will perform the tests in a safe mode and no way disrupt the production system.

A.12.7.1 Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

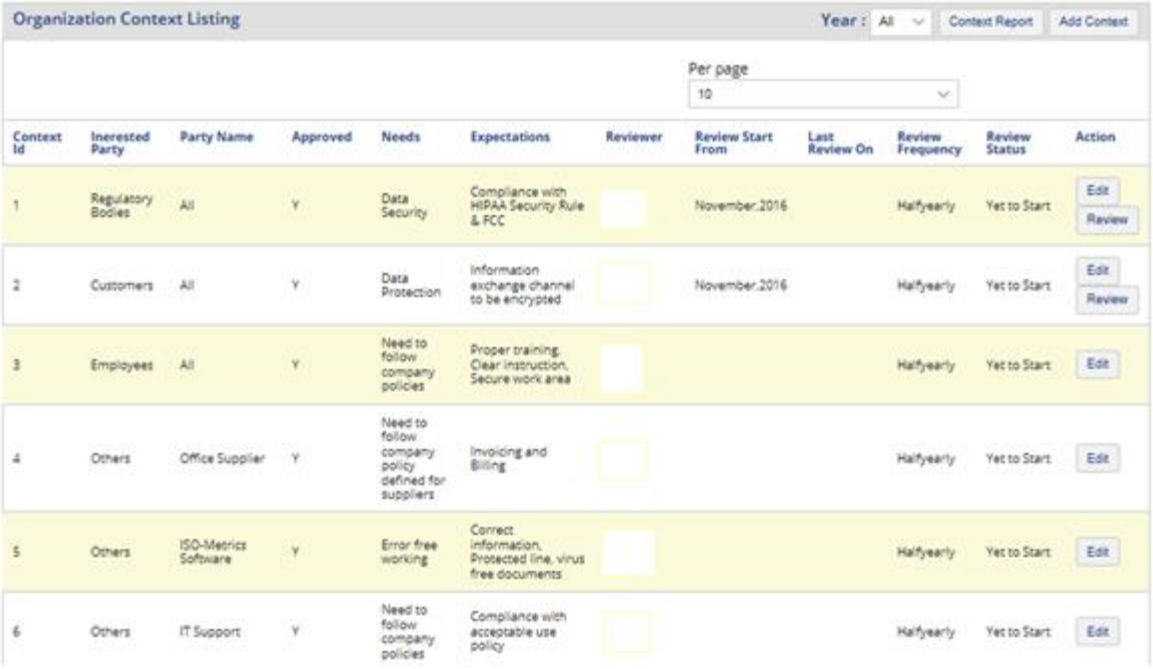
Stakeholder Management:

Stakeholder analysis is a very important activity in project management. We generally perform the project for the stakeholders. When we identify the stakeholder we should also identify their needs and expectation from the project from the information security perspective.

ISO 27001:2013 Clause 4.2 Understanding the needs and expectations of interested parties

The organization shall determine:
a) interested parties that are relevant to the information security management system; and
b) the requirements of these interested parties relevant to information security.

Following screenshot from ISO-Metrix provides some example of such requirements of interested parties.



Organization Context Listing

Year : All | Context Report | Add Context

Per page 10

Context Id	Interested Party	Party Name	Approved	Needs	Expectations	Reviewer	Review Start From	Last Review On	Review Frequency	Review Status	Action
1	Regulatory Bodies	All	Y	Data Security	Compliance with HIPAA Security Rule & FCC		November 2016		Halfyearly	Yet to Start	Edit Review
2	Customers	All	Y	Data Protection	Information exchange channel to be encrypted		November 2016		Halfyearly	Yet to Start	Edit Review
3	Employees	All	Y	Need to follow company policies	Proper training, Clear instruction, Secure work area				Halfyearly	Yet to Start	Edit
4	Others	Office Supplier	Y	Need to follow company policy defined for suppliers	Invoicing and Billing				Halfyearly	Yet to Start	Edit
5	Others	ISO-Metrics Software	Y	Error free working	Correct information, Protected line, virus free documents				Halfyearly	Yet to Start	Edit
6	Others	IT Support	Y	Need to follow company policies	Compliance with acceptable use policy				Halfyearly	Yet to Start	Edit

Pic 5

Human Resource Management

HR Security

It is a well-known fact that people are the biggest risk as far as the information security is concerned. In most of the projects we recruit people from outside. It is becoming a standard practice to get the background screening done for these employees.

Recruiting

> *A.7.1.1 Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.*

During Employment

It is a good practice to remind people constantly about the importance of information security. Most of the organizations have a standard Information Security Awareness Program which every employee has to undergo at least once a year.

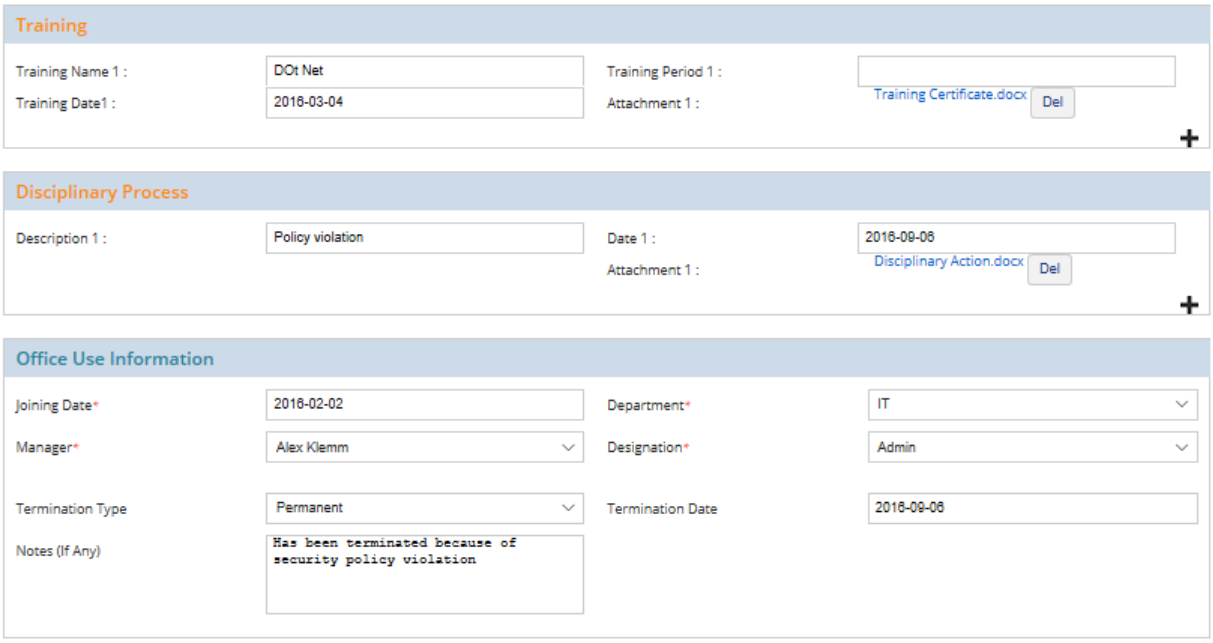
> *A.7.2.2 All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.*

Termination

It is important to retrieve the device assigned to the employee and revoke their network access and physical access so that they cannot access the information system after their departure.

> *A.7.3.1 Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.*

Following screenshot shows how all the information about an employee can be documented and tracked to make sure proper care has been taken during employment and termination.



Pic 6

Integration Management (Change)

Security Analysis

Changes in the organization are an ongoing phenomenon. Some of the changes could be a mini project but sometimes it can be a big project as well.

It should be a standard practice to analyze the change for any security exposure.

> *A.14.1.1 The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.*

Performing Test

As we have experienced earlier that InfoSec Expert is required to perform the security analysis for all the changes. If a security exposure is identified then some mitigation action is designed. To make sure that the security loop hole has been plugged properly, it is required to test to verify that the solution is working. The InfoSec Expert is required to give a "go" sign off on the change before moving it to production.

> *A.14.2.8 Testing of security functionality shall be carried out during development.*

Information Security Standards

- ISO 27001:2013

An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

It can help small, medium and large businesses in any sector keep information assets secure.

- ISO 27018

ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

- PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.

- NIST

The National Institute of Standards and Technology (NIST) is a measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness.

- SSAE16

Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, was finalized by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) in January 2010. SSAE 16 effectively

replaces SAS 70 as the authoritative guidance for reporting on service organizations. SSAE 16 was formally issued in April 2010 and became effective on June 15, 2011.

SSAE 16 was drafted with the intention and purpose of updating the US service organization reporting standard so that it mirrors and complies with the new international service organization reporting standard – ISAE 3402. SSAE 16 also establishes a new Attestation Standard called AT 801 which contains guidance for performing the service auditor's examination.

- CSA STAR

CSA STAR is the industry's most powerful program for security assurance in the cloud. STAR encompasses key principles of transparency, rigorous auditing, and harmonization of standards. STAR certification provides multiple benefits, including indications of best practices and validation of security posture of cloud offerings.

STAR consists of three levels of assurance, which currently cover four unique offerings all based upon a succinct yet comprehensive list of cloud-centric control objectives in the CSA's Cloud Controls Matrix (CCM). CCM is the only meta-framework of cloud-specific security controls, mapped to leading standards, best practices and regulations. CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to cloud computing.

- FISMA

The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002.

- FedRAMP

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that saves an estimated 30-40% of government costs, as well as both time and staff required to conduct redundant agency security assessments. FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

Conclusion

Project Managers are required to understand the importance of information security. They should identify tasks and activities within the project to meet the requirements. This will ensure safe keeping of sensitive information, safe exchange of information and taking necessary care to protect the information from human and environmental factors.

References

- ISO 27001:2013 Standard
- 5th Edition PMBOK® Guide

About the Author

Neelov Kar

Dallas, TX, USA

Neelov Kar has been working as Account Manager (Client Executive) in Perot Systems since 1998, where he has been instrumental in opening new accounts and managing and expanding existing accounts at different client sites with different technologies and domain expertise. As an Account Manager/ Program Manager he has implemented multiple large projects on mainframe and client server environment. He was also involved in recruiting and training/ mentoring the project managers and helped them in their career progression.

He is a PMP, RABQSA certified ISO 9000 Lead Auditor, ISO 14001 Lead Auditor, ISO 27000 Lead Auditor, ISO/IEC 20000 certified, Six Sigma Certified, CSA STAR certified and a Certified Quality Analyst. Neelov can be contacted at Neelov.kar@gmail.com