Bringing the Dawn of Security & Compliance to Project Teams

Vivek Sahai Mathur

mathurvs@outlook.com

Abstract

The majority of outsourced work is piecemeal: phases of the SDLC are carved out and Service Provider companies deliver the output to the customer as per the Statement of Work. The Customer then integrates all the deliverables together. The Service Provider's focus is on speed, and ensuring that the business requirements are covered. This approach leaves out contract compliance and data protection, Different nations around the world are adopting data security and privacy regulations. Violations are penalized, so customers are transferring the risk through stricter enforcement of contractual penalty clauses.

While the legal framework and insurance is being put in place by the Service Provider's corporate teams, trying to "Inspect in" or "Audit in" contractual compliance is time consuming and ineffective for the project delivery teams. Typically project management does not appreciate the root causes and impact of the risk. Process quality and delivery quality teams also do not cover these aspects a priori.

This paper walks through my experience in creating, piloting, and rolling out an org-wide initiative to awaken the PM community to non-functional requirements and customer's implicit security and privacy expectations. A lightweight framework for early detection of gaps, tracking of corrective actions, and feedback on residual risk for the project was designed to be easy to administer, and quick for the PM to respond, with most information available in the project definition.

Biography

Vivek S Mathur started his IT career in 1997. With 30+ years of varied work experience ranging from the Government to software product and service companies, his focus has always been on setting up robust processes, and seeing their impact on the quality of deliverables and productivity. Making changes that delivery teams internalize and adopt, and add value to the organization.

Vivek has set up core software development processes for product and service companies like McAfee, Intelligroup & Altisource Labs, and has set up and led large delivery teams for multiple customers.

Vivek has always tried to give back to the community, and has been associated with STeP-IN Forum (www.stepinforum.org) actively for the past 11 years. He is currently the President, STeP-IN Forum

Experienced in Information Security and Software Quality, and in leveraging these to achieve highest productivity and predictable project delivery while leveraging the partner ecosystem.

1 Introduction: The Blinkered PM

The typical IT outsourcing deal pursuit crosses multiple stages and has many handoffs. Teams with different responsibilities review the documentation and participate in the negotiation rounds. As the proposal process winds towards its conclusion, multiple aspects of the deal are accepted by these teams.

The result is a signed Statement of Work (SOW), and a project team is assigned to deliver the software application to the customer. When the project is ready to begin, the chosen Project Manager builds the team. At this point in time, the PM is aware of:

- Technology in use (and therefore skills to include in the team)
- Estimated effort and proposed schedule (therefore team size and onboarding duration available)
- Location of the documents (covering requirements and architecture)

And, in certain more mature organizations:

- Expected project contribution margin (and profitability targets for the Business Unit and company as a whole)

As the PM works to get the project started, the focus is on the immediate needs, while other aspects of the deal that have been accepted are not communicated, nor prioritized. The PM begins the project with incomplete appreciation of these expectations and commitments. Primary among these are:

- Information Security and Data Privacy
- Regulatory and Compliance commitments
- Non-functional requirements

The focus of this paper and the assessment it explains, is on the first two topics. Non-functional requirements need to be elicited as part of the project discovery stage, and taken care of as part of the deliverables.

2 The Background Scramble

As mentioned briefly above, Information Security and Data Privacy are implicit customer expectations and an unidentified risk for complete project delivery. These two aspects have taken on greater importance in the current global environment.

2.1 Elevated Cyber Security Risks

2.1.1 Setting the Context 1: The Changed Attack Landscape:

In the current cyber environment, cyber defense needs and the scope of control mechanisms are very fractured, while at the same time requiring continuous attention throughout the SDLC. In short:

- Perimeter Defense is no longer adequate
- 'Fit and Forget' defense is no longer adequate
- Retrofit after Deployment is no longer adequate
- All environments are open to breach

To counteract these risks, we need to adopt a Defensive Security stance that:

- Aligns security to business requirements

- Designs for minimal attack surface
- Builds in security
- Deploys for defense in depth

The earlier we start to Build in Security and inculcate a defensive mindset in the entire team, the less risk will remain at the time of project delivery. We can incorporate the design, implementation, and review effort into the proposed solution, or raise these aspects during initial ideation discussions with the customer.

2.1.2 Setting the Context 2: The Competitive Landscape:

In a competitive industry, customers are looking for a partner to advise, guide and keep their best interests front and center. The best partner will be one to use historic and concurrent experience and industry knowledge, leveraging exposure to multiple industries and cross-leveraging to help identify new solutions and industry leading best practices.

Since Cybersecurity is a growing risk in an increasingly mobile and connected world, applying the ability to proactively reduce cyber disasters for the customers will increase credibility as a trustworthy and worthwhile partner.

2.2 Forced Risk Acceptance

The Service Provider must balance the revenue imperative with the risk of a security incident, and as such is faced with a dilemma. While risk transfer through the use of insurance policies is available, it is an expensive solution, and the customer specifications for insurance terms and conditions make it more complex with every passing year. Inevitably, risk is accepted, and the pressure is on the delivery team to implement the risk mitigation to the maximum extent possible. However, without prior information and understanding of the risks that have been accepted by the company, it is very difficult for the project team to come up with any cogent and useful approach to manage and control the risks.

Therefore, it is imperative to unearth expose the risks at the earliest. For this purpose, we created a risk assessment framework.

3 The Risk Assessment

3.1 Background

The risk assessment application was based on a request from Senior Management to create a corporate security and compliance risk landscape for all in-flight and upcoming projects. During the design stage, the following decisions were taken:

a) Design an end-to-end framework for proactive project risk assessment:
    a. Keep the process simple enough to be quick, but provide indicators to all or most potential problems.
    b. Integrate with preexisting ticketing workflow and management reporting process
    c. Provide a visual aid to the assessees to track progress. This shows how much controllable risk remains, and keeps the team motivated to complete the assigned interventions.
    d. Add the risk assessment as a part of the project initiation process.
    e. Structure the intervention as a self-assessment for scalability, using simple language and concepts.
    f. Definitely NOT to follow the ISO certification audit approach. The initial clauses of the standard focus on organizational mandates and structures, which are beyond the scope and responsibility of the PM, who is busy in the daily project delivery tasks.
b) Monitor the desired outcomes
    a. Expose hidden improvement opportunities in project delivery related to information and data security risks

b. Educate the project leadership to contractual and regulatory aspects of their work, and how cyber security risk that the project team adds to the deliverables can have a much larger impact on the company. Risk may not be limited to the next billing amount, but could have real financial consequences if a penalty clause is triggered.

The Assessment Model was designed to add value to multiple stakeholders:

- Technical team members: Implementable & clear, prescriptive directions
- Project Managers: Delivery interventions during the project timeline
- Portfolio Managers: Risk Governance and Corrective recommendations
- CXO level: Corporate Strategy inputs and portfolio risk management

To try and address this spread of detail and abstraction, and differing focus areas and objectives, the following options were evaluated to achieve the quickest start and roll out.

3.2 Options evaluated:

3.2.1 Leveraging Standard Security Audits:

Existing models for Security Assessment such as ISO27k, etc. are designed with an Outside-in perspective, and are useful for 2 sets of users:

- Internal Auditors looking at their internal software development processes
- Third party auditors identifying lacunae in software development process and abilities

Security Audits are fundamentally “After the Fact”. This is a result of the implicit expectations for the audit, and part of the “Nature of the Beast”:

a) ISMS has to be defined and implemented
b) Projects should already be following the ISMS recommendations, or in process of adoption. In most cases, conformance with the ISMS is not complete, and is always in a state of flux for the Service Provider.
c) Defining, Deploying, and Monitoring the ISMS is typically the responsibility of a specialized Task Force.
d) All project teams cannot participate in the task force
e) Projects end and knowledge is lost
f) New projects start constantly
g) New projects often follow the customer’s processes.

Security Audits also define desired states, but do not recommend actions to be taken by the project team An audit is typically driven across the company, and focus on individual projects and project teams is limited to closure of non-compliance reports (NCRs). Ensuring adequate technical depth and rigor of the solutions becomes secondary to meeting the audit schedule.

3.2.2 Utilizing Standard Risk Frameworks (e.g. OWASP/ SAMM/ CIS):

They are mostly derivative from the ISO standards in terms of the areas covered.

a) As in the case of the external audit-based approach, the frameworks do not have a practitioners viewpoint to guide how to avoid security issues or build a secure product.
b) Cannot be used to assess new projects, but need some deliverables for review.
c) Structured as maturity models, and yield a score that talks about the capability of the project to deliver secure output, rather than interventions that are needed to improve deliverables.
d) Do not address the project delivery process at all. The standard framework was modified with delivery related aspects such as Training & Education, Organization & Reporting, and Process implementation.

3.2.3 Custom-built model:

The Service Providers need is to ensure that existing and future projects and work products are made compliant with security best practices. For this purpose, a custom-made framework works best to provide project teams with a simple, quick assessment mechanism, a convenient method to submit their results, and an automated data ingress and analysis mechanism.

- Risk areas are limited to those under the project manager's control
- Project delivery aspects are covered
- Information about the risk areas is available as part of the project initiation process and the assessment questions can be answered by the PM and project architect within the first 20 days of the project start date.
- The solution also provides senior management with a comprehensive dashboard to show overall metrics and provide click-through to project level details and the ability to slice and dice across multiple dimensions.

3.3 Criteria for Evaluation

The assessment model was assessed for ease of implementation and adoption, using the following evaluation criteria:

3.3.1 Effective

- Identifies maximum risks in one pass.
- Forces evaluation of individual risks
- Triggers an analysis of the risks caused by interaction of different aspects of the project characteristics.

3.3.2 Easy to incorporate in the project life cycle

- Aligned with and synergistic to existing project management and portfolio governance processes
- Intervention Triggers clearly defined and monitored externally
- Learnings can be easily transferred to the next project(s)

3.3.3 Clear and prescriptive

- Understood by tech and non-tech project roles
- Clear actionable Recommendations applicable at project level
- Inculcating risk awareness and risk management focus in the team
- Discussion based; all doubts cleared during the assessment

3.3.4 Simple to administer

- Self-explanatory
- Completed in ½ to 1 hour
- Easy to track
- Clear visualization of results and progress

3.3.5 Comprehensive

- Technology agnostic
- SLDC agnostic
- Delivery type agnostic: Design, Dev, test, deploy, maintain/ support
- Covering code and 'Beyond Code' aspects of project delivery (Not just the SDLC)
- Covering project and portfolio governance aspects: Corporate context means that projects impact not only the immediate deliverable but also the customer relationship, market reputation, and ability to acquire new leads once the client contacts move to other corporates.

    - Providing opportunities to advise the client: Showcase thought leadership and cross leverage learnings, with business domain focus
- Robust & Industry Leading
    - Aligned to Global Best Practices
    - Capable of evolving and staying relevant

3.4 Self-Assessment Design & Implementation

The application was implemented using standard collaboration and analytics tools: Microsoft Teams for meetings, and PowerBI for reporting. An Excel spreadsheet was created for data entry, sent as an email attachment. The combination of tools provides an easy way to conduct the assessment with geographically distributed teams who may not have access to the corporate network.

3.4.1 Core Excel App

a.) Assessment Entry sheet

14 factors in 3 areas were identified as being typically in the blind spot of the PM when evaluating Information security risk. An indicative response spectrum was defined for each as a guideline for rating selection.

1. Technology related:

a. SDLC span: stages of the SDLC covered

b. Tech Stack depth: business logic to server management

c. Non-production environment control: the extent to which management of code promotion was in the project's control

d. SDLC model: time available to fix findings

e. COTS integration: the extent to which the business logic was self-coded.

f. Security Requirements: Whether customer has explicitly noted down security aspects to be addressed.

2. Demographic factors:

a. Industry Sector: Inherent complexity and focus on security

b. Regulatory Requirements: Compliance to regulations and standards

c. Data Privacy impact: applicability of data privacy regulations from various countries

d. Data Components: Personal and non-public information being processed in the application

e. Usage/ Impact: extent of control on the user base behavior

3. Contractual Factors:

a. Deliverable responsibility: The extent of accountability for outcome vs effort

b. Project duration/ iterations: availability of time to fix issues

c. Direct Financial Impact: Penalty amounts and clauses

Each factor is assessed by the project team along with the representative from the delivery quality team. In the initial stages, the author would participate in person, along with his team, later the assessment was conducted by the project team and delivery quality teams.

Scores were assigned from a non-linear scale to assist in clearer prioritization. Based on the score, the author mapped the factor scores to the relevant security controls.

Focal areas for corrective action were identified for each factor and rating

b.) Typical values

To assist the PM and project architect choose the correct score, two guidelines were provided:

- Typical values for each factor, from least to most risk, giving the team a mapping to typical project situations and SOW characteristics.
- A strong suggestion to pick the more severe rating value in case of any disagreement.

c.) Map to Action items

Each rating value was mapped to actionable interventions that were in the control of the project manager and team. The assessment was conducted within the first 20 days of project initiation and for projects with an expected duration of more than 3 months to give the team sufficient time to implement the changes and realize benefits.

- 2 globally accepted models were used:
    - CIS: The Center for Internet Security (CIS) is a nonprofit organization with members including large corporations, government agencies, and academic institutions. Initially nurtured by NIST and OWASP, CIS is now independently managed to provide a free and fair assessment and responsiveness to changing cyber landscape.
    - BSIMM: Industry benchmark body monitoring the actual cyber-security actions undertaken by the member companies. BSIMM controls are constantly being reviewed and mapped to other cyber security standards
- In addition, to provide a compilation and easy reference to standards and controls, we included a reference site from the University of California, Irvine, which has been made Open Source.

The Action items identified were raised as tickets in the Delivery quality Ticketing Tool (initially in-house and later using a third-Party Software), and subject to the same severity classification, closure timelines and escalation process as all other tickets, ensuring that the security assessment received the same attention as any other ticket raised.

d.) Integration to Executive Dashboard

Data from each assessment was added to the database and used as input to the Executive Dashboard portraying the Security Risk Landscape for the company. Accumulation was at different levels of abstraction, from project code, Service line, Business Unit and up to the corporate security risk profile. The dashboard highlighted the common areas of concern, like secure development lifecycle, data privacy, and contractual commitments.

e.) Action tracker

To avoid surprises, the assessment repeats every quarter, and on any change in scope.

To make the process usable and ensure the team's engagement on an ongoing basis, especially for long running "steady-state" projects where there is little or no change in scope, technology or vendor responsibility, a visual aid was created in Microsoft Excel to track the progress and showcase how close the team is to reaching the end state of "no more interventions available." This tracker gets the inputs from the database and is refreshed after every assessment meeting.

3.5 Building Capability & Capacity for Rollout

The implementation of the assessment across all new projects has two challenges: Capability and Capacity

3.5.1 Imparting the skills to review the assessments

The Delivery Quality team was chosen as the ideal team to participate in the assessment because of their frequent interactions with the project teams throughout the project duration. Most of these interactions take the form of data gathering and information capture, into standardized formats for audit and reporting purposes. The Risk assessment falls seamlessly into the same category, albeit with a different focus and requirement of rating evaluation.

Delivery quality team also has follow up meetings to close on the Action Items that were raised in the project ticket tracker.

A training session was conducted by me to sensitize the team to the following factors:

- How not to accept exemption requests from PMs: If there is data being used, and algorithms being applied, some form of SDLC will be in use, and Information Security Risk or Data Privacy considerations will be applicable
- Trends in code development and application deployment environments, and the impact on the exposed risk surface. (This evolution was covered in my paper from PNSQC 2023: https://pnsqc.org/vivek_mathur_2023.php)
- To insist on risk identification: Threat Modeling approach using STRIDE
- The 14 factors and their inter-relationship. How the factors cover almost all aspects of software delivery that the PM and project team can understand and control.
- Talk through the sample ratings and help the team relate to their project reality
- Show the relevance of the factor -> action items mapping
- How not to accept the self-ratings by the project teams, how to be skeptical and get a more realistic rating.
- Technical debt will persist, leading to repeated high risk ratings, and a higher residual risk score.

3.5.2 Ensuring capacity to cover all new projects

Monthly, the number of new projects to be covered by the assessments was substantial. With the assistance of delivery quality team, and my dedicated handful, we were able to address all fresh starts where the assessment was found to be applicable. Renewals, short term, small and POC projects were exempt.

Each assessment took less than an hour, and meetings were held after the information pack (assessment worksheet, instructions, and FAQs) was sent to the PM one week in advance, and both PM and architect were available to participate in the meeting with the self-ratings filled in.

3.6 Process & Governance

The steps in the process towards a born secure Company are:

- Company Project Portfolio Survey - Identify existing projects and New Starts
- Risk Identification & Quantification - Focus on the relevant factors for each project. This is the core of the process and requires active participation from the project management and technical teams.
- Apply security controls - Risk based prescribed controls have to be implemented during the course of the project to fix weak areas and enhance security stance
- Monitor and repeat - every project milestone or half yearly
- Review and Improve - Conduct retrospective meetings and feed back the learnings into the process for continuous improvement

3.6.1 Risk Identification & Quantification Meeting:

We need to identify the influencing factors for the project. The scope and depth of security activities will depend upon the characteristics of the project, or based on the information provided in the RFP documents.

3.6.2 Control Implementation Status Meetings:

Once the relevant controls are identified and being implemented, the residual risk is assessed periodically at project milestones and quarterly/ half-yearly. Completion of the controls implementation is tracked and status is updated to the Teams workspace for progress tracking, analysis and reporting. One assessment just before final delivery of the project ensures that all possible actions have been completed, and the attack surface is minimized.

The assessment values are appended to the database at the granularity of Project – Date – type of assessment (Initial, Ongoing, Pre-delivery), and latest status is reflected in the Excel Action Tracker.

3.6.3 Process Review Meetings:

For the purposes of process improvement, a retrospective meeting is used to capture the final project status and the "Stop/ Start/ Continue" analysis of the process itself, including updates to the List of values in the dropdowns, the file handling, and the reporting improvements.

4 The Wide-Angle View

4.1 The Payoff to the PM

- The primary payoff to the PM is a better, more secure deliverable, with lowered chances of a in-Production firefight to add a security Band-aid.
- Secondary payoff (longer term) is better credibility as a security-oriented delivery personnel.
- Being able to think in terms of risk makes the PM much more likely to have a seat at the table for architectural discussions in the future., having a say in the future direction of the application roadmap.
- Reduced technical debt in the product backlog and ability to speed up the feature delivery.

4.2 The Benefits to the Company

- A better understanding of the cyber threat landscape and ability to prioritize corrective action.
- Quantified financial impact due to project security risks and ability to steer sales negotiations towards less risky
- Knowledge of the risk exposure and reduction in the residual risk after directed corrective action by the project management teams.
- Competitive advantage with the ability to show alignment with imperatives to “Build Security and Privacy in”.

References

Acronyms

- SDLC: Software Development Life Cycle
- PM: Project Manager
- IT: Information Technology
- SOW: Statement of Work
- ISO: International Standards Organization
- CXO: Chief x Officer (X may be replaced by the initial letter for any of multiple corporate responsibilities
- ISO27k: ISO 27001 – ISO defined standard for Information Security Management System (ISMS)
- ISMS: A company's Information Security Management System
- NCRs: Non-Compliance Reports created as a result of an audit showing non-compliance with the standard.
- OWASP: Open Worldwide Application Security Project
- SAMM: Security Assurance Maturity Model
- CIS: Center for Internet Security
- COTS: (for software applications) Commercial Of The Shelf
- NIST: National Institute of Standards and Technology
- BSIMM: Building Security In Maturity Model
- STRIDE: Acronym for the various malware impacts: Spoofing/ Tampering/ Repudiation/ Information Disclosure/ Denial of Service/ Elevation of Privilege
- FAQs: Frequently Asked Questions