AGILE RISK MANAGEMENT FOR BUILDING RISK DRIVEN SECURITY

Abstract

Dealing effectively with risks involved in the project is difficult and requires management interventions to successfully handle project completion. Now days, being agile will definitely help you to satisfy your clients and at the same time your business objectives. Therefore, implementing risk management in agile way will help you to imrpovise your mitigation plans as per the iteration andminimize threatened revenues and business reputation.

Kulkarni, Mr. Shantanu Vinayak

Sk34800n@pace.edu

Dec 12, 2016

Agile Project Management Principles:

Agile Project Management is an iterative process that focuses on customer value first, team interaction over tasks, and adapting to current business reality rather than following a prescriptive plan. It is based on the same organizational practices and key principles found in the Agile Manifesto. It is how you deliver high value and technical quality within your time and budget constraints. However, the principles go beyond software development. It's a mindset for people who need a management approach that builds consensus quickly in a fast-paced environment. Scrum is widely used and popular framework for agile software development process.

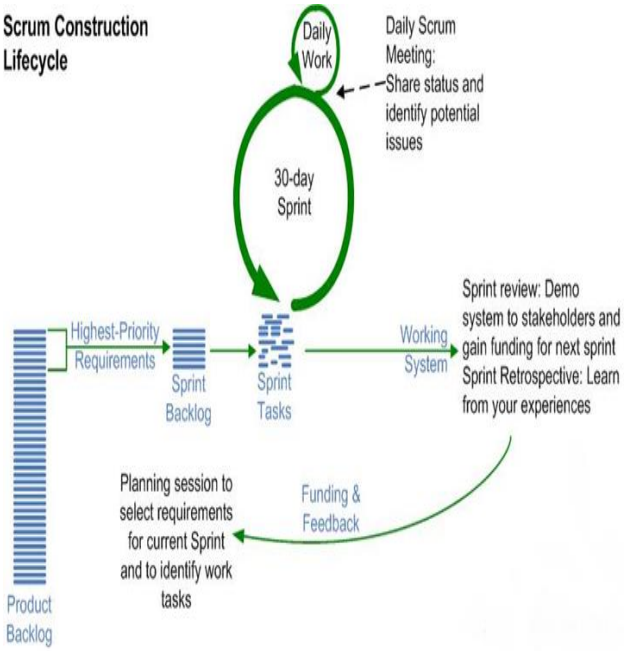
Scrum includes three important roles for project participants:

Product owner: The person responsible for business value of the project and deciding what work to do and in what order.

Scrum master: The person who ensures that the team is productive, facilitates the daily Scrum, enables close cooperation across all roles and functions, and removes barriers that prevent the team from being effective. Scrum masters have authority over the process but not the people on the team.

Scrum team/ Development team: A cross-functional team of people who organize themselves and the work to produce the desired results for each sprint.

The principles of Scrum capture both humanist and business values such as courage, openness and respect, as well as focus and commitment. Its set of official practices is limited to iterative development (referred to as sprinting), planning, daily scrum meetings and review and retrospective exercises. These are frequently augmented with other optional techniques such as Scrum-ban (essentially the use of a Kanban board) and burndown charting. Although iterative development and incremental delivery are not as clearly delineated as in other agile methodologies, it is clear from the descriptions of planning activities that there is at least an implicit division between the two. Scrum teams are organized into the roles of Scrum Master, Product Owner and the Development Team. The Scrum Master is in essence both a process owner and a process manager who ensures that practices are understood and supports them through facilitation and coaching. The Product Owner is the sole custodian of the project requirements and is accountable for their clear expression and value alignment within the organisation. Finally, the Development Team is responsible for transforming requirements into deliverables that constitute potentially releasable functionality. Typically, the Development Team is a small, self-organizing and cross-functional unit that is jointly accountable for its work. It relies on neither titles nor substructures in order to operate.



Fixed length iterations, referred to as Sprints, constitute the primary arena for all Scrum events, each of which enables inspection and adaptation of the process. Chronologically, the first of these is the Sprint Planning event, during which deliverables and the work required to deliver them are determined. Thereafter the team meets on a daily basis (the Daily Sprint) to briefly (i.e., no more than fifteen minutes) discuss their contribution towards the Sprint goal, the planned activities for that day and to declare any impediments that lie in their path. At the end of a Sprint there is a Sprint Review meeting to determine the state of affairs of items on the Product Backlog and propose any necessary adaptations, gather feedback on the iteration itself and review other details related to the project (e.g., budget, timelines, next steps).

Finally, the Sprint Retrospective is an opportunity for continual process improvement (e.g., by taking a closer look at relationships within the team, use of processes and tools) and how it can be implemented in the next Sprint. Requirements are derived from the Product Backlog (an open-ended list of welldefined and understood requirements, enhancements and fixes that are estimated and assigned value) and used to create the Sprint Backlog that communicates, forecasts and monitors activities in greater detail on a daily basis. Much of the work at this stage is focused on gaining consensus regarding understanding of the requirements and how they should be implemented (incl. design) and tested during the course of which a well-defined and coherent Sprint goal is determined and formulated.

Alternatively, the Scrum process can be represented as an agile chart in which movement around each circle implies multiple iterations of its inner circle (see our website for more information about the agile charting technique). Thus in the figure below, which depicts a simplified version of the Scrum process, each release comprises of one or more Sprints each of which involves one or more days

For Agile development model, Risk is a big factor and which should be considered at the earliest during planning sprints. Let's take a look to understand exactly what is required to understand risks in your projects:

Understand Risks in Your Projects:

"Risk in itself is not bad; risk is essential to progress, and failure is often a key part of learning. But we must learn to balance the possible negative consequences of risk against the potential benefits of its associated opportunity." (Van Scoy, 1992)

Risk is uncertainty that has an impact on project objectives in either a positive or a negative manner. The fact that not all uncertainty is either relevant or negative, is summed up in the analogy, that whilst a horse race may well be uncertain, it only becomes a risk once a bet is placed, the outcome of which may result in losses (threat) or winnings (opportunity). In order to manage risk, it is therefore necessary to not only understand the project objectives, but also the project context and risk environment. The project context determines how risk is to be interpreted and the primary drivers of risk (e.g., regulatory, technology, business), whereas the risk environment reflects what constitutes acceptable levels of risk (e.g., dispensations for research and development activities). Together these help assess the risk profile of a project in terms of the wider attitude towards, and tolerance of, risk within the organisation. This enables management to compare projects on a risk basis and to balance risk and reward. Whilst the understanding of risk as process variability might well be unique to Scrum, much of its literature implicitly frames risk negatively and limits its scope to requirements change and matters of technical implementation. Moreover, in keeping with most agile methodologies, there are no explicit measures to manage risk, relying instead on the implicit belief that “being agile” suffices.

Failure to adequately address risks within a project can lead to:

- Inability to make informed risk and reward decisions.
- Failure to identify appropriate risk response strategies based on risk exposure.
- Lack of oversight in risk monitoring leading to ineffective or inefficient treatment of risks.
- Poor understanding of when to engage in risk activities.

REDUCE PROJECT RISK IN THE REQUIREMENTS PROCESS

Gathering and managing requirements are important challenges in project management. Projects succeed or fail due to poor requirements at any time throughout the project lifecycle. The continuously evolving baseline of requirements needs to be managed effectively. The project manager needs to assess and understand the uniqueness of the requirements gathering process for his/her individual project

Risk Management

Risk management involves understanding, analysing and addressing risk to make sure organisations achieve their objectives. So it must be proportionate to the complexity and type of organisation involved. Enterprise risk management (ERM) is an integrated and joined up approach to managing risk across an organisation and its extended networks.

Risk management is the process of identifying, assessing and controlling threats to an organization's capital and earnings. These threats, or risks, could stem from a wide variety of sources, including financial uncertainty, legal liabilities, strategic management errors,

accidents and natural disasters. IT security threats and data-related risks, and the risk management strategies to alleviate them, have become a top priority for digitized companies. As a result, a risk management plan increasingly includes companies' processes for identifying and controlling threats to its digital assets, including proprietary corporate data, a customer's personally identifiable information and intellectual property.

.

Risk management standards

Since the early 2000s, several industry and government bodies have expanded regulatory compliance rules that scrutinize companies' risk management plans, policies and procedures. In an increasing number of industries, boards of directors are required to review and report on the adequacy of enterprise risk management processes. As a result, risk analysis, internal audits and other means of risk assessment have become major components of business strategy.

Risk management standards have been developed by several organizations, including the National Institute of Standards and Technology and the ISO. These standards are designed to help organizations identify specific threats, assess unique vulnerabilities to determine their risk, identify ways to reduce these risks and then implement risk reduction efforts according to organizational strategy.

The ISO 31000 principles, for example, provide frameworks for risk management process improvements that can be used by companies, regardless of the organization's size or target sector. The ISO 31000 is designed to "increase the likelihood of achieving objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk treatment," according to the ISO website. Although ISO 31000 cannot be used for certification purposes, it can help provide guidance for internal or external risk audit, and it allows organizations to compare their risk management practices with the internationally recognized benchmarks.

The ISO recommended the following target areas, or principles, should be part of the overall risk management process:

The process should create value for the organization.

- It should be an integral part of the overall organizational process.
- It should factor into the company's overall decision-making process.
- It must explicitly address any uncertainty.
- It should be systematic and structured.
- It should be based on the best available information.
- It should be tailored to the project.
- It must take into account human factors, including potential errors.
- It should be transparent and all-inclusive.
- It should be adaptable to change.
- It should be continuously monitored and improved upon.

The ISO standards and others like it have been developed worldwide to help organizations systematically implement risk management best practices. The ultimate goal for these standards is to establish common frameworks and

processes to effectively implement risk management strategies.

These standards are often recognized by international regulatory bodies, or by target industry groups. They are also regularly supplemented and updated to reflect rapidly changing sources of business risk. Although following these standards is usually voluntary, adherence may be required by industry regulators or through business contracts.

Risk management strategies and processes

All risk management plans follow the same steps that combine to make up the overall risk management process:

Risk identification: The company identifies and defines potential risks that may negatively influence a specific company process or project.

Risk analysis: Once specific types of risk are identified, the company then determines the odds of it occurring, as well as its consequences. The goal of the analysis is to further understand each specific instance of risk, and how it could influence the company's projects and objectives.

Risk assessment and evaluation: The risk is then further evaluated after determining the risk's overall likelihood of occurrence combined with its overall consequence. The company can then make decisions on whether the risk is acceptable and whether the company is willing to take it on based on its risk appetite.

Risk mitigation: During this step, companies assess their highest-ranked risks and develop a plan to alleviate them using specific risk controls. These plans include risk mitigation processes, risk prevention tactics and contingency plans in the event the risk comes to fruition.

Risk monitoring: Part of the mitigation plan includes following up on both the risks and the overall plan to continuously monitor and track new and existing risks. The overall risk management process should also be reviewed and updated accordingly.

Risk management approaches

After the company's specific risks are identified and the risk management process has been implemented, there are several different strategies companies can take in regard to different types of risk:

Risk avoidance: While the complete elimination of all risk is rarely possible, a risk avoidance strategy is designed to deflect as many threats as possible in order to avoid the costly and disruptive consequences of a damaging event.

Risk reduction: Companies are sometimes able to reduce the amount of effect certain risks can have on company processes. This is achieved by adjusting certain aspects of an overall project plan or company process, or by reducing its scope.

Risk sharing: Sometimes, the consequences of a risk are shared, or distributed among several of the project's participants or business departments. The risk could also be shared with a third party, such as a vendor or business partner.

Risk retaining: Sometimes, companies decide a risk is worth it from a business standpoint, and decide to retain the risk and deal with any potential fallout. Companies will often retain a certain level of risk a project's anticipated profit is greater than the costs of its potential risk.

Risk Management in Agile Way

Agile risk management is concerned with the identification, assessment, prioritization, treatment and monitoring of project risks in a manner consistent with agile principles and practices. It considers not only threats (negative risks) but also opportunities (positive risks) in the

context of the enterprise attitude towards risk and employs its own techniques and practices to inform decision making to balance risk and reward. Extending the agile mantra of "embrace change", agile risk management encourages practitioners to "embrace risk". Agile risk management is founded on the following principles:

Transparency: Make visible and accessible all risk artefacts used to understand, communicate and manage risks within the project.

Balance: Establish clarity about the nature and distribution of risk and reward throughout the project.

Flow: Ensure that risks do not inhibit the project and that the agile process itself is capable of withstanding perturbations arising from risk. Application of the agile risk management process involves establishing an understanding of the nature of risk facing a project and adapting the existing agile process to better cater for risk management. The agile risk management process comprises of the following stages:

Understand project objectives, context and risk environment. This stage is about achieving an understanding of the environment in which the project operates. This is a necessary prerequisite to frame risk management practices and assist in clarifying the relevance of risk within the project and in relation to the organization (e.g., the need for risk dispensations).

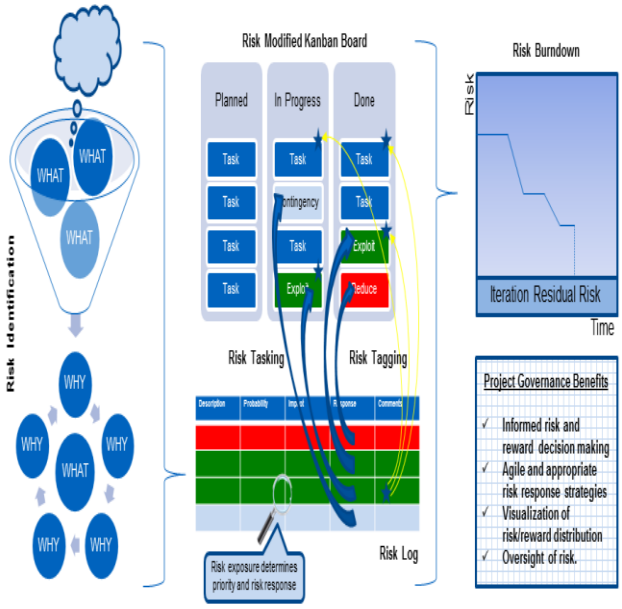
Risk Scoping: Identify Risk Drivers and Appetite. By scoping the project risk drivers, the primary sources of risk and the institutional attitude towards and tolerance thereof can be established and communicated in a clear manner. This ensures the foundations for alignment of personal and institutional attitudes towards risk-reward behaviour.

Risk Tailoring: Embed Risk Management in Agile Process. The dynamic view of agile process being employed is charted in order to determine the most appropriate positioning of risk management activities (e.g., risk identification workshops at the start of an iteration and risk retrospectives at the end). In light of the risks facing a project, additional measures may also be proposed (e.g., application of specific agile techniques to tackle risk).

Risk Management: Identify Analyse, Manage and Monitor. This encompasses the operational aspects of risk management within the project albeit imbued with an agile character (e.g., use of risk modified Kanban boards to visualize the distribution of risk and reward, tagging of activities to indicate the application of an agile technique in order to treat risk and communal ownership of risk artefacts).

Managing Risks in Scrum

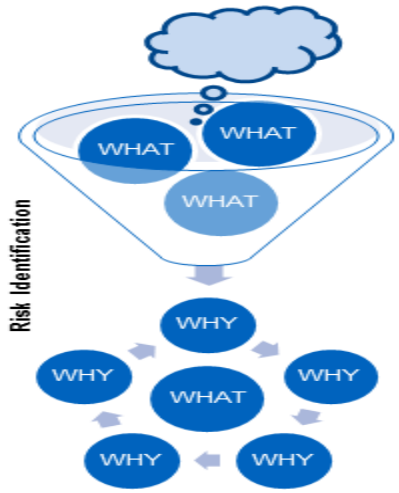
The following picture describes an approach to agile risk management that suits Scrum teams using a Kanban board approach (also known as a Scrum-ban) in their work. Omitted are the details of risk scoping and tailoring which usually take place before start of the project.



Risk Identification

Identification of risks is harder than one might imagine as the biggest problem is conflating

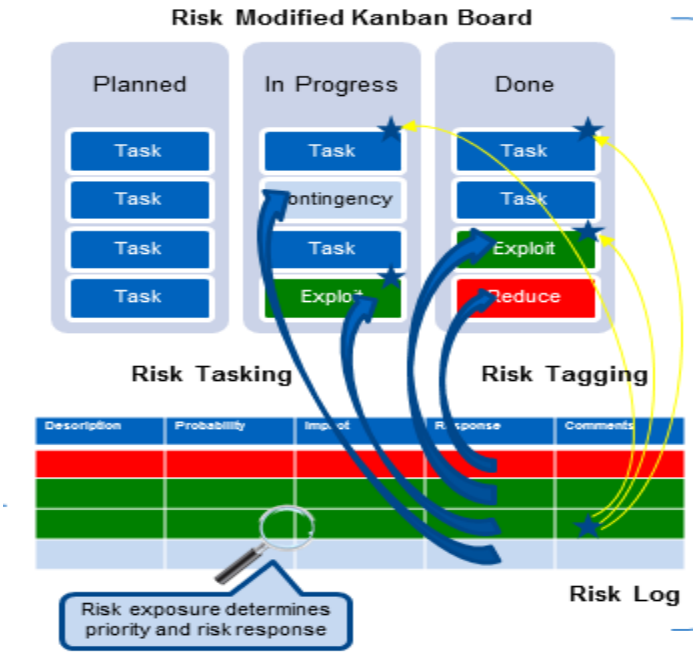
uncertainties and effects. For example, the risk in a website migration lies not in the lack of availability of the site afterwards (which is the effect of an unsuccessful migration) but rather the uncertainty surrounding the circumstances that led to its unavailability (e.g., how to configure DNS). A simple but effective technique for risk identification is to brainstorm what might occur (effects) and then in each case, ask why it might occur (risks)



Once identified risks should be recorded in a risk log (e.g., description, inherent risk exposure) to which will be added further information (e.g., risk response strategy and treatment, residual risk exposure) later.

Risk Analysis and Prioritization

Risk Analysis, Prioritization and Treatment The purpose of risk analysis is to determine a course of action and prioritize it accordingly. Risks should be assessed in terms of likelihood and impact (together these are known as risk exposure) for which T-shirt sizing (i.e., S, M, L) usually suffices. As a first step, the risk as originally encountered (inherent risk) should be estimated and later reassessed once a treatment has been determined (residual risk). Sometimes the treatment of risk introduces entirely new risks (secondary risks) and thus risks in practice are linked in a complex web of causality. Bear in mind, that range estimates of risk exposure components are perfectly acceptable if these serve as the basis for discussion within the team



It is important to understand the limitations of risk assessment techniques such as asking people (e.g., hidden agendas, confirmation bias), using past data (e.g., might not be indicative of future trends) or probability models (e.g., hidden assumptions) so whenever an assessment is made, it should be challenged. It is a common misconception that high risk must imply high reward. In fact, what should really be asked is whether or not the reward implied by a story or task warrants the level of risk it entails. Or in other words: is it possible to achieve the same level of reward for less risk? This helps better prioritize user stories on the backlog as risk becomes an influencing factor in prioritization though it is never the primary determinant of ordering on the backlog. The following six risk response strategies are commonly used in risk management to determine the nature of risk treatment

Accept Undertake no action to manage the risk, but instead have a contingency plan in place in the event that the risk is realized.

Exploit/Reduce Enact measures to increase/decrease either the likelihood or the impact of the risk.

Share/Transfer Endeavour to share/transfer the risk to other parties in exchange for a share in the rewards or a fee for assuming the risks.

Avoid Refrain from taking part in the task that gave rise to the risk.

Once a strategy has been determined the next step is to determine concrete measures to treat the risk. The following options are available:

Do nothing (but plan) Accept that the risk might occur and think about what would need to be done if it were realized. This becomes an optional task on the Kanban which might never be needed.

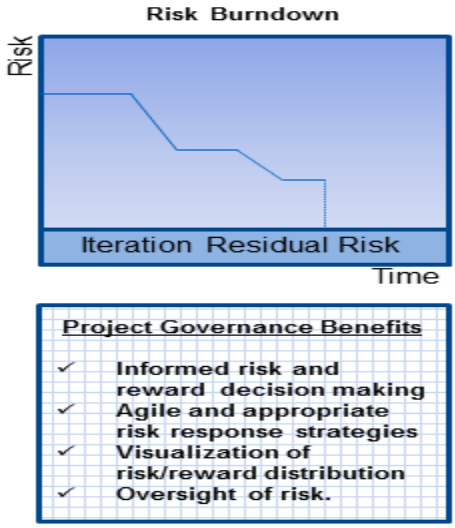
Risk Tasking Create a task that deals with the risk (e.g., exploit, reduce, share or transfer it). These tasks are just like any other task in Sprint planning. It is very helpful to colour code such tasks (e.g., red for reduction, green for exploitation) so that the distribution of risk and reward can be visualized on the Kanban board.

Risk Tagging This refers to the selection of an agile technique specifically chosen to cater for a risk (e.g., pair programming) and which is applied to a class of activities (e.g., all GUI related tasks). Tagging involves placing a mark next to each affected task to remind the team of the technique to be applied.

Task Dropping Remove the task from the Kanban that is giving rise to the risk.

Risk Monitoring

Risk monitoring provides a visual cue of what is being done to tackle risk whilst at the same time acknowledging the systemic nature of risk within the project.

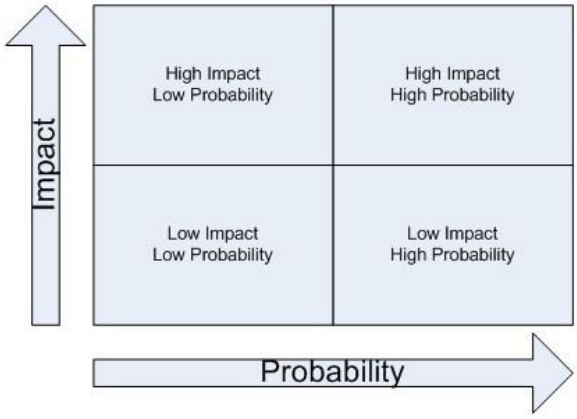


Risk monitoring requires the assigning of scores to risk exposure bands when assessing both inherent and residual risks. For example, the inner region of the risk response strategies chart might be assigned two points, the middle four and outer six. The amount of risk mitigated thus reflects the difference between inherent and residual risk scores and serves as the basis of a risk burndown for the Sprint.

Mitigating Risk in Agile

Risk mitigation is a major task for agile software development model. There are following tips available for mitigating your risks in agile way:

Balance risk with the needs of the business
The adoption rate of Agile is accelerating among large scale enterprises as IT responds to the "unceasing demand for speed and business alignment." "Agile also helps organizations address the complexity of software development today, given the impact of mobile devices, the proliferation of new languages and tools for Web apps, growth in cloud-based computing and the overall importance of digital processes to a company's success," adds Dunne.



Implement risk-based testing

"In order to take on more risk as part of Agile and DevOps thinking, there must be proper checks and balances integrated within the testing process. Instead of testing every feature and function, and shifting timelines, prioritize testing and quality management measures to fit business priorities. Risk-based testing commonly assigns a risk rating score for individual tests, which gives developers and QA an idea of the level of risk involved in delivering the code covered by that test if the test is skipped. As a result, the product team might spend more time testing versions of the application for devices which comprise the most important or largest sector of the customer base.

Benefits of Agile Risk Management

The benefits of agile risk management include the following:

- Improved capacity to manage project uncertainties that would otherwise threaten revenues or impede efforts to exploit opportunities that arise within projects.

- Enhanced communication of the nature and sources of risks facing projects within the organization, leading to an improved culture of awareness and understanding of the need to balance of risk and reward.

- Better alignment of project and enterprise risks that promote the transfer of lessons learned between projects of similar scope and complexity.

- Empowerment of project teams, enabling them to accept responsibility for the identification analysis, prioritization, treatment and monitoring of risks within their projects.

- Appreciation for the social and cultural influences on risk management, (e.g., risk compensation effects) particularly in environments where these can play a dominant role (e.g., geographically dispersed teams).

- Ability to extend and enhance existing investments in Scrum by tailoring and embedding risk management practices into daily activities.

A Risk Driven Approach to Security:

Most industries are under regulatory pressure, so they take a compliance-driven approach to security to meet minimum requirements. But compliance requirements are often static and prescriptive, according to security executives. Compliance gives organizations a false sense of security that can be misleading, and it provides only a one-time snapshot.

Managing risk can help to mitigate this cost. The shift to a risk management approach has been brewing for some time, according to the CISO Insights Study. Security leaders are realizing that simply checking the box to address compliance requirements is no longer a sufficient strategy. Those further up the maturity curve are transforming their programs to be truly risk-based by using a sophisticated approach to determine risks and prioritize security investments.

Below are some more key takeaways on risk programs:

Compliance Is Just One Factor

Compliance doesn't go away entirely, even in a risk-based program. The regulations are still there, but department heads and managers have

to start thinking in terms of acceptable risk levels versus compliance requirements. It's a change in language, and the moment when everyone understands the difference is transformational for the entire organization.

Risk Tolerance Evolves Over Time

An assessment plan and risk profile is expected to change over time. It is also difficult for organizations to properly assess risk before encountering a problem. However, frequent conversations about what department heads and senior management are comfortable with promotes risk awareness across all lines of business.

Making Risk Management Work

Risk management breaks down into three distinct areas: strategic, tactical and operational. As organizations move to a risk-based approach, they can explore assessment platforms, work to create risk profiles and partner with third-party providers to perform risk assessments.

Implementing Risk Driven Security Key Responsiblities:

Create human language goals and priorities: Before diving into any technology or creating any alert logic, it is helpful to write down, in human language sentences, what you would like to accomplish. This is similar to the programming practice of writing pseudo-code before writing any actual code. This accomplishes two important things. First, it helps the organization to organize its goals and priorities, which are derived from the risks the organization seeks to mitigate and can subsequently be used to frame and execute a work plan. Second, it serves to document those goals and priorities. Documentation (at all levels) is seldom fun, but it is an extremely important activity for a number of reasons.

Identify appropriate data sources: Once goals and priorities are identified, the appropriate data sources can be identified to meet those goals and priorities. The relevant data sources can include network traffic data, various types of logs (network, end-point, and malware), intelligence feeds, threat reports, and other sources. It is important to consider all data sources relevant to a particular goal or priority and to explicitly identify and document the relevant sources alongside it.

Identify appropriate technologies: Different technologies suit different needs. For example, for certain goals and priorities, a SIEM or data warehouse may be the appropriate tool. For others, a network or endpoint forensics platform might be the right fit. Or, for yet others, something different entirely may fit the bill.

Throw out the default rule set: This may sound radical, but for each technology, throw out the default or standard rule set. Why? Because it wasn't written specifically for your organization. Are there specific signature sets, rules, logic, alerts, etc. that meet the needs of your organization? Absolutely, and those should be retained selectively. It's important to remember, though, that many elements of the system's default set won't meet the needs of your organization. Keeping them in there will create noise and false-positives that won't help you accomplish your goals and priorities.

Write spear alerting: Alerts are a powerful force in security operations and should be leveraged accordingly. Write alerting designed to identify suspicious, malicious, or anomalous activity as defined by your goals and priorities. Don't bother writing any alerts that don't fit your goals and priorities. Why? Because that will just produce additional noise and false positives that you've already decided you aren't interested in.

Streamline the workflow: Regardless of how and where alerts are generated, they should all flow to one unified work queue. Priority should be used to assist the team in identifying what to work on first, second, etc. Highest priority goes to the highest fidelity, most reliable alerts covering the most critical assets. Lowest priority goes to the lowest fidelity, least reliable alerts

covering the least critical assets. The most important takeaway here is that one work queue allows your team to focus and provides them jumping off points into analysis, forensics, and investigation. More than one work queue leads to complication and confusion.

Practice Continuous Security Monitoring (CSM): Once you set up alerting and a work queue, use it. Every alert should be reviewed by the team and investigated appropriately to build context around it and understand what occurred. Some alerts will require more investigation, while others will require less investigation. There is really no point in setting up alerts that you never intend to look at. That's really the point of CSM -- reviewing each alert and performing analysis, forensics, and investigation as required.

Follow a mature process: Process is the glue that binds people and technology together. If you have great people and great technology, a great process is also required. Process helps the team focus on what tasks are value-added and converge to a conclusion. After all, analysis and forensics are not done for analysis' and forensics' sake, but rather, to reach a conclusion.

Leverage automation where appropriate: Once a mature process is in place, study the application of that process operationally. If time-consuming, manual labor exists for certain aspects of the process, consider automation. If time can be saved in one place, it means that more time can be spent elsewhere. This leads to greater overall visibility across the organization.

Maintain a communal presence: We can learn a lot from our peers. Maintaining a presence in the broader security operations community ensures that an organization is in the loop regarding current events, topics, discussions, and issues. All of these factors play a role in ensuring that the security operations program changes with the times, and that information is shared in a timely and relevant manner. Just remember -- this relationship involves both giving and receiving.

Continuously improve: Never believe that the work has been completed. Technologies, methodologies, and the threat landscape change continuously and quickly. It is important to continually seek feedback and improve. The steps described here are iterative and should continually be stepped through in a cyclical fashion.

References:

1. Project Management Institute, A Guide to the Project Management Body of Knowledge, (PMBOK Guide), Fourth Edition, ANSI/PMI 99-001-2008, pp. 273-312.

2. Cooper, D., Grey, S., Raymond, G., & Walker, P. (2005). Project risk management guidelines: Managing risk in large projects and complex procurements. Hoboken, NJ: Wiley.

3. Wideman, R. M. (1992). Project and program risk management: A guide to managing project risks and opportunities. Newtown Square, PA: Project Management Institute.

4. http://www.securityweek.com/risk-driven-security-approach-keep-pace-advanced-threats

5. http://institute.agileriskmanagement.org/wpcontent/themes/iarm/publications/AgileRiskManagementScrumWhitepaper.pdf

6. https://securityintelligence.com/a-risk-driven-approach-to-security-from-check-boxes-to-risk-management-frameworks/