Adaptation of Information Security in the Agile World

One of the core values of Agile is to maintain built-in quality, which implies that security controls should be embedded in the Agile mindset. However, it may be argued that information security and an Agile mindset do not always go hand in hand with implementation of an Agile framework within an enterprise. Teams often state that functionality and business value are more critical than security compliance.

Teams often state that functionality and business value are more critical than security compliance. IT auditors and Agile advocates sometimes disagree. While Agile teams argue that there is no one "right" way to run a sprint and no standardized approach to application development, IT auditors and IT compliance professionals prefer a consistent approach. They generally want there to be an established, comprehensive and documented process that is closely followed.

It is clear that the maturity of information security and compliance in the Agile framework is not well developed. There are many questions about how information security and compliance can be governed within the Agile framework. One answer is to use the Scaled Agile Framework's 10 SAFe Lean-Agile Principles to adapt and transform IT security approaches (figure 1).

Apply System Thinking

Systems thinking takes a holistic approach to solution development, incorporating all aspects of a system and its environment into the design, development, deployment, and maintenance of the system itself.

<table>
<thead>
<tr>
<th>SAFe Lean-Agile Principle</th>
<th>Security Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply system thinking</td>
<td>Security within the system</td>
</tr>
<tr>
<td>Assume variability; preserve options</td>
<td>Security principles as a beacon to variability</td>
</tr>
<tr>
<td>Take an economic view</td>
<td>Security controls with an economic view</td>
</tr>
<tr>
<td>Organize around value</td>
<td>Security managed around value</td>
</tr>
<tr>
<td>Build incrementally with fast, integrated learning cycles</td>
<td>Security tool integration and automation to support fast, incremental iteration</td>
</tr>
<tr>
<td>Visualize and limit work in progress (WIP), reduce batch sizes and manage queue lengths</td>
<td>Limited WIP and reduced batch sizes for security controls and implementations</td>
</tr>
<tr>
<td>Apply cadence; synchronize with cross-domain planning</td>
<td>Application of security cadence; synchronization with cross-domain planning</td>
</tr>
<tr>
<td>Base milestones on objective evaluation of work systems</td>
<td>Clearance of security requirements and objectives for each milestone</td>
</tr>
<tr>
<td>Unlock the intrinsic motivation of knowledge workers</td>
<td>Unlocking the intrinsic motivation for security</td>
</tr>
<tr>
<td>Decentralize decision-making</td>
<td>Empowering the team with knowledge and decision-making authority on security</td>
</tr>
</tbody>
</table>

Figure 1—SAFe Lean-Agile Principles and Associated Security Approaches

Gerald Pang, CISA, CISM, CIPM, CISSP, Certified SAFe Agilist
Has 17 years of experience in information security management across various industries, specializing in IT security, governance, risk management and compliance (GRC), and data privacy.
System thinking does not apply only to solution development. System thinking applies to the enterprise at large, which includes its people, management and processes. The system within both an Agile team and an enterprise must be optimized so that different parts of the system and the enterprise are working collectively and optimizing value streams.

Security Within the System
IT security and the risk team should be part of the overall system, along with design and development and operations (figure 2). Applications are often developed without the involvement of IT security and the risk team and, in some organizational cultures, they are involved only during the initial or final stage of development and not throughout the life cycle of the implementation. With such limited involvement, it is inevitable that any decision by IT security and the risk team will be made at the last stage of development, giving the impression that IT security and the risk team are the cause of delay and an impediment to implementation.

To remove this impression, IT security and the risk team must be part of the development and decision-making system within the enterprise. They must be part of the Agile release train (ART) and, if necessary, the Agile team. This will provide the necessary security support and guidance to the team, while reducing any friction between the security and engineering teams. IT security should provide guidance related to security controls, and the risk team should guide and advise on how to manage risk if a control cannot be added within an iteration. IT security and the risk team should be seen not as impediments but as resources to help prioritize security controls and manage risk.

Assume Variability and Preserve Options
Solution development is an inherently uncertain process. Technical variability and market variability are present throughout the development process. Innovative new systems have, by definition, never been developed before, so there is no guaranteed path to success.

Rather than reducing variability (options) from the beginning, the approach should embrace variability and remain flexible to support changing requirements.

When there are various options to navigate during the development process, planning and decision making are dynamic. When there is uncertainty and change happens throughout the development process, the team needs to be directed by a beacon, regardless of variability, and this beacon should be the enterprise’s security policy (figure 3).

Security Principles as a Beacon to Variability
Corporate security policy should be the beacon that guides the enterprise’s security principles and risk
appetite. This policy needs to be articulated and enforced at all levels of the enterprise. A defined security policy provides direction for the team, and a clear security policy directive provides a path for the team to navigate as it embraces variability and flexibility in product development. If the security policy is too specific, that path will be too narrow, limiting the team’s ability to embrace variability and flexibility. In contrast, if the security policy is too general, it will create ambiguity and confusion. Therefore, it is important that the policy provide clear direction on what the enterprise wants to achieve while allowing flexibility in the application of security controls.

**Take an Economic View**

> Taking an economic view requires one to achieve the shortest sustainable lead time with the best quality and value—requires understanding the economics of a mission. Without that, even a technically competent system may cost too much to develop, take too long to deliver, or incur exorbitant manufacturing or operating costs.4

**Security Controls With an Economic View**

It is tempting for information risk managers to cite the entire list of organizational security policies and controls when asked what controls need to be considered for a product. It is practically impossible to implement the whole list of security controls and standards (e.g., US National Institute of Standards and Technology [NIST], International Organization for Standardization [ISO]) while shortening the sustainable lead time and ensuring the best quality and value. This frustrates the team and usually causes it to overlook security measures because there is just too much to consider. Instead, risk managers may be required to determine the necessary security controls based on an economic view of the project and products. This decision by risk managers is crucial, as they need to balance the development cost with the right security controls for the output.

Risk managers are required to perform risk assessment and analysis based on the potential threats related to the product’s impact and value. Based on the risk assessment and risk exposure, they must determine at which stage the controls should be added incrementally, as the product gains functionality and market exposure. It is very tempting for IT security managers to add all controls within the first release; however, these controls may not directly support the economic benefits of the product.

**Organize Around Value**

Business agility demands that enterprises organize around value to deliver more quickly. When business demands change, enterprises must adapt...
quickly and reorganize based on value flow. Enterprises that organize around value are typically fast-moving and adaptive networks of individuals focused on the needs of their customers. They aim to deliver continuous value to customers while reducing the lead time required to deliver high-quality products.

Security Managed Around Value
When taking an economic view of security, risk managers must organize security controls and requirements around the value demanded by customers and society (figure 4). A paradigm shift in the traditional way of handling security and governance is required. An example of a security control with value to the customer is a feature that protects and encrypts customers’ sensitive data; customers and society expect enterprises to implement reliable and secure systems to manage sensitive data. An example of a security control with less value to the customer is a comprehensive 50-page security document.

Risk managers may be required to perform threat and risk assessments and make deliberate plans to determine which controls should be added to an iteration to support the value and risk exposure of products.

Build Incrementally With Fast, Integrated Learning Cycles
Building a solution is done incrementally, adding value and features to the solution over time. After each addition, results can be evaluated, allowing incremental capabilities to be presented to and assessed by customers for constructive feedback. Feedback from customers allows the team to build on previous increments, evolving the solution until the product is released.

Security Tool Integration and Automation to Support Fast, Incremental Iteration
To support the fast, incremental approach to software development, the security approach must
be adaptive and rapid and should not impede the development process. Security testing and assurance must be able to adapt to ever-changing and incremental iterations. To achieve speed in security testing and assurance, it is important that security tools used for dynamic application security testing (DAST) and static application security testing (SAST) are integrated and automated in the development process (figure 5). This ensures that testing is done effectively, without compromising the accuracy of the test. With integrated tools, vulnerabilities and security issues can be identified early in the development process, allowing the team to plan for and work on remediation. Security penetration testing and security bounty programs can be organized to detect security flaws and issues not identified during the fast-paced development of products.

Integrated and automated tools should continue to be deployed during the development process and throughout the product’s life cycle. Security tools must be able to monitor, detect and defend against threats to the application in the production environment.

Visualize and Limit WIP; Reduce Batch Sizes and Queue Lengths

“To achieve the shortest sustainable lead time, Lean enterprises strive for a state of continuous flow, which allows them to move new system features quickly from ‘concept to cash.’” To achieve continuous flow, work in progress (WIP) must be reduced to a level at which the work can reasonably be accomplished within an optimal time to build team motivation and productivity. To reduce WIP and improve flows, batch size should be kept small, and the queue length to process the job should be kept short. Smaller batches on shorter queues go through the system faster and with less variability.
Limited WIP and Reduced Batch Sizes for Security Controls and Implementations

The principles of limiting WIP, reducing batch sizes and managing queue lengths can also be applicable to security implementations and controls. Security controls and requirements need to be broken down into batches of work items for teams to develop and implement. With a smaller batch of security requirements, the enterprise can perform a value assessment and risk assessment on each specific requirement. Security requirements can be scaled accordingly and prioritized for each iteration. This reduces WIP for various security implementations in the development flow. Reducing the batch size for security implementations keeps the team motivated and reduces the impression that security is a hindrance to product development.

TO UNLOCK THEIR INTRINSIC MOTIVATION, WORKERS SHOULD BE ENCOURAGED TO EXPLORE AND MAKE DECISIONS BASED ON ENTERPRISE PRINCIPLES AND VALUES.

Apply Cadence; Synchronize With Cross-Domain Planning

Uncertainty is inherent in solution development. Agile development addresses this uncertainty in a defined boundary for the enterprise through cadence and synchronization. Cadence provides a rhythmic pattern of consistent events and routine, helping developers focus on solution development. Synchronization with cross-domain planning enable solutions to be explored, planned and integrated across multiple technology and business functions within the enterprise.

Application of Security Cadence; Synchronization With Cross-Domain Planning

Regular cadence and synchronization should be applied to security implementations and controls. Security requirements should be planned for deployment at regularly established intervals. Priority of security implementations should be determined from a risk perspective in accordance with product value and risk exposure. With regular cadence, key primary security controls can be deployed quickly, while secondary security controls can be added in subsequent iterations.

As security policy and controls cut across technology and business functions, synchronization events enable cross-domain teams to be aligned on security requirements and implementations at various levels of the solution. Server, database and application teams will be aligned on how data can be protected across different technology domains.

Base Milestones on Objective Evaluation of Work Systems

Throughout the development of a product, the system is built in increments, with milestones at each iteration to demonstrate feasibility and success of the solution in process. This is done routinely and periodically so that relevant stakeholders can evaluate the product. With periodic milestones, changes can be made early in the development process, allowing products to evolve based on what the customer wants.

Clearance of Security Requirements and Objectives for Each Milestone

Information security requirements must be detailed for each iteration, so that information security implementations can be evaluated during each milestone evaluation. To ensure an objective evaluation of the product’s information security, it is crucial that clear information security requirements and objectives be set up during every iteration. Therefore, iterations for security controls to be incorporated into the product must be represented in functional user stories for security requirements.

In the Agile world, it is important that security requirements are translated into clear user stories so that teams know how to interpret and implement the requirements and objectives of security controls for the product. Clear security requirements and objectives provide a clear basis on which to evaluate the security features at each milestone.
Unlock the Intrinsic Motivation of Knowledge Workers

The traditional workforce mentality is that employees do what the boss says. This traditional system does not utilize the capability and knowledge of workers. To unlock their intrinsic motivation, workers should be encouraged to explore and make decisions based on enterprise principles and values. Workers are motivated when they see that product success is the result of their contributions and decisions. Workers must be given autonomy within the stated purpose and mission.

Unlocking the Intrinsic Motivation for Security

The principle of motivation can be applied to the security mindset and culture. Agile teams must be motivated through cultural change within the enterprise. The enterprise must embrace security requirements and recognize that they are as important as any other features added to a product. Including security features in a product reassures customers and gives them confidence. Consumers tend to trust products with security features, leading to wider dissemination and quicker product acceptance within the market. Teams should ensure that security features and controls are added accordingly. Teams must be motivated to do so, and they must strive to ensure that their products will not fall victim to mistakes or attackers. They must be motivated to search for innovative ways to secure and protect the interests of their customers over various product iterations. They will do this not because IT security demands it but because they understand the value of ensuring the security of their products.

Decentralize Decision-Making

To deliver value in the shortest time, the Agile team must be authorized to make certain decisions, rather than requiring a decision at a higher management level. Not all decisions should be decentralized; however, decisions that are recurrent and common should be made at the team level. Time-crucial decisions and those that require local consideration should also be decentralized.

"TO DELIVER VALUE IN THE SHORTEST TIME, THE AGILE TEAM MUST BE AUTHORIZED TO MAKE CERTAIN DECISIONS, RATHER THAN REQUIRING A DECISION AT A HIGHER MANAGEMENT LEVEL."

Empowering the Team With Knowledge and Decision-Making Authority on Security

It is important that developers be empowered to make security decisions and be responsible for such decisions. This reduces the turnaround time needed for decisions on security matters. While the security team is involved in deciding policy and control requirements, the development team determines how these requirements can be met and during which iteration they will be implemented. The development team must be given the necessary resources and tools to perform security scans and fix any issues they find, as it is preferable to discover and mitigate security issues in the early stages of product development. Developers must be trained to evaluate codes and applications from an attacker's perspective, so that they can make informed decisions about the security of the product.

Conclusion

The evolution of an Agile mindset in product development has been gaining popularity among IT professionals. Agile has helped enterprises assemble the best teams to collaborate and achieve rapid and continuous product delivery while maintaining customer satisfaction. As the transformation of software development has progressed, the integration of information security and risk in a fast-paced environment has not kept up; it has not yet been defined and adapted to support such an environment. This often leads to confusion and frustration between development teams and IT security.

Using Agile principles, there are opportunities for security culture to be embedded in the Agile framework. With the right mindset and a willingness
to change how IT security and risk are approached—that is, aligned with Agile methodology—it will be possible to manage IT security and risk in a fast-paced and dynamic software development environment. The adaptation of security practices within the Agile framework will enable the team to manage risk and balance security requirements in accordance with identified threats and the demands of society.

Endnotes

4 Op cit Leffingwell, D.; “Apply Systems Thinking”
6 DevSecOps, Manifesto, https://www.devse cops.org/