# Application Security Maturity Model (ASM)

A PRAGMATIC APPROACH TO SECURING YOUR SOFTWARE APPLICATIONS

SecurityInnovation
THE SOFTWARE SECURITY COMPANY

187 Ballardvale Street, Wilmington, MA 01887 +1.978.694.1008 **www.securityinnovation.com**

# Table of Contents

## Introduction

The Application Security Maturity (ASM) model helps organizations understand where they are in terms of their overall approach to software security. The model was developed by Security Innovation in 2007 from analyzing and plotting over ten year's worth of data about organizations and their security efforts, in particular their investment in tools, technology, people, and processes.

Based on this research, it's clear that organizations that develop and deploy the most secure software have a high maturity level; further, they only reach maturity through much trial and error, particularly when it comes to purchasing and integrating tools into their software development and information security organizations. By understanding and using the ASM model, organizations can uncover their current maturity level and then understand the most effective course of action to increase this level quickly and pragmatically while introducing as little disruption as possible to their current development process and in-production application management.

This goal of this article is to:

1. Understand how the ASM model was created.
2. Learn how the model works and what it can tell you about your organization.
3. Help fine-tune your security-related investments in order to positively impact your software security maturity more quickly

## Creating the ASM Model

The ASM model was developed after analyzing first-hand the software security activities and investments of hundreds of organizations. The initial data input for the model is based on:

- Extensive software security research at Florida Institute of Technology (FIT). Led by Dr. James Whittaker, FIT project teams examined the security issues of software development processes as well as the underlying testing procedures and processes that were failing to catch so many critical software bugs. This work began in 1999 and conclusions were drawn from direct exposure to the tools used, developer mindset and skillset, and development processes used.
- In-depth consulting engagements with Security Innovation clients. Security Innovation was founded by Dr. Whittaker in 2002, and since its inception, has expanded on the initial FIT research. The company's staff of security experts has helped understand, assess, and classify thousands of software bugs. Its employees have written books and created methodologies adopted by leading software developers. As with the initial FIT research, the knowledge and expertise from Security Innovation staff is from real-world experience.
- Detailed analysis of data collected via interviews and SDLC (software development lifecycle) assessments. This data was collected at over 200 organizations, many of whom are Fortune or Global 500 companies. Interview data was validated and expanded upon by direct inspection and inquisition of tools, systems, and staff. In each case, baseline metrics were defined and tracked over time – in some companies for as little as 12 months, in most over a span of 3-5 years.
- The combined ten-year experience of the Security Innovation team and its academic predecessor means that we have access to – and continually generate – a wealth of information about how organizations approach the software security challenge. By analyzing all of our primary data, it became evident that there are two critical categories of investments that can impact how well any company meets the challenge.

## Technology and Tools (T&T)

These investments include the various software tools and applications an organization licenses or acquires to secure software during all stages of the software development life cycle (SDLC), from creating application or system requirements through final deployment. This is typically the area where most organizations, when faced with the threat of a security breach or looming regulatory pressures, first invest their dollars.

Specific investment in this area includes tools for:

- Version control
- Source code scanning
- Defect Management
- Test Automation
- Web Security vulnerability scanning
- Application-layer security mitigation (e.g., a Web application firewall)

In each area above, organizations were analyzed for both depth and breadth of application. For example, in source code scanning, organizations were examined on several factors, including:

- Does the organization utilize source code scanning tools?
- If so, are there *security* source code scanning tools in place?
- How and where are the source code tools used, e.g., on developers' desktops, at check-in or build time, continuous integration, at a single clearinghouse/ "gatekeeper" station prior to deployment?

Who uses the source code scanning tools, e.g., security architects, developers, testers/QA, information security officer/analyst, etc.

## People and Processes (P&P)

Investments in this area include the hiring of security staff, ongoing training programs, and improvements to the SDLC specifically for enhancing code or application security. While the typical reaction to real, perceived, or potential security threats is a tool-buying spree, over time companies learn to invest in improving security deeper in the organization by making investments in P&P, which almost always pay higher dividends than an investment in tools.

Specific examples of investment in this area include:

- Secure SDLC activities for development teams at each phase, e.g., design, code, test, et al.
- Training (both technical and awareness)
- Internal "Red Teams" (playing the role of attacker)
- Third-party security reviews (at code and as-built layers)
- Application security auditing
- Integration of Application Security with Risk Management practices

Just as we did with T&T, each P&P area is analyzed and explored in depth and breadth. The resulting database had over 10,000 data points that were sorted, normalized, and compared to extract trend lines and conduct point-in-time analyses.

Note that having invested in all of the specifics outlined above – essentially a laundry list of security best practices – in both the T&T and P&P categories would indicate a very high security maturity level for an organization, and high maturity is the goal if and only if the investment is coupled with the culture change necessary to integrate the investments as part of operational business. Therefore, it is not a simple matter of picking and choosing a handful of investments to make in each category. Rather, it is a journey that leads organizations to eventually understand the benefit of funding and implementing the T&T and P&P investments mentioned above.

Once you have built your policies, constructed your corporate secure coding standards and provided procedures for implementation, you need to give your people the training they need to implement correctly. Training should not be limited to technical training for your development team – managers, business analysts, and internal auditors or security assessors also need to be trained. A good curriculum will include 100-level "awareness" training as well as 200- and 300-level courses for each role, such as Manager, Business Analyst, Architect or Developer.

## Plotting the Data

Understanding these two critical elements led us to plot organizations according to these two criteria. Using a standard 4x4 grid, with the left corner (the origin) representing "low," and the top left and bottom right corners representing "high," we plotted an organization's investment in Technology & Tools on the vertical Y axis and its investment in People & Processes on the horizontal, X axis.

The grid was populated from information we knew directly about organizations and their security investments. For example, to be plotted, we had to be able to determine an organization's investment for both T&T and P&P based on our scale. From this information, we were able to:

- **Plot organizations over time (multiple data points).** By working with an organization for an extended period of time, we were able to plot its evolution in terms of the two primary axes of the ASM model. This organization-normalized curve mirrored the generalized (all organizations) curve mentioned below.
- **Plot individual companies (single data points).** We could plot each company we worked with according to the two major axes of the model. While a single point does not enable us to create a company-specific progression, it does help us validate an overall curve.
- **Determine the ASM curve (all data points).** Using the information we had from companies both over time and at a point in time, a predictable ASM curve developed. This curve reliably predicts where organizations are along the curve and their likely future course of action.

While the ASM model and the typical maturity curve provide great insight for organizations to understand and alter their security investments, there are some caveats of the model that should be taken into consideration:

- The model is based upon organizations that have asked us for help, so by definition (going to a third-party source for help), they are already more aware and mature than an organization just starting its ASM journey.
- Companies may not follow the path directly, though evidence suggests that most companies will adhere to the basic curve unless they have actively decided to influence it in a severe fashion by specific investments (or panic.)

## Understanding the ASM Model

The ASM Model has three distinct phases based on a company's investment in Tools & Technology and People & Processes. The phases are: The Panic Scramble, The Pit of Despair, and Security as a Core Business Process.

### THE PANIC SCRAMBLE

Most immature organizations are in this stage. They start their security journey by responding to some event, perhaps a loss of confidential data, a Web site breach, or the discovery of a network intruder. They may also enter this stage as a response to external events, such as a very public security breach at a competitor or media reports of massive data losses. Another potential catalyst is a new government or industry regulation.

Organizations that have found themselves in the Panic Scramble respond to the immediate security issues by spending money on software security tools and technologies that hold the promise of immediate impact to mitigate the perceived or real threat. However, such an investment without the requisite investment in P&P usually provides little overall return and limited security improvements; in fact, many times, tools become "shelfware" sitting unused because the developer or information security professional doesn't know how to use them or what to do with the results the tool generates, leading to the second stage.

### THE PIT OF DESPAIR

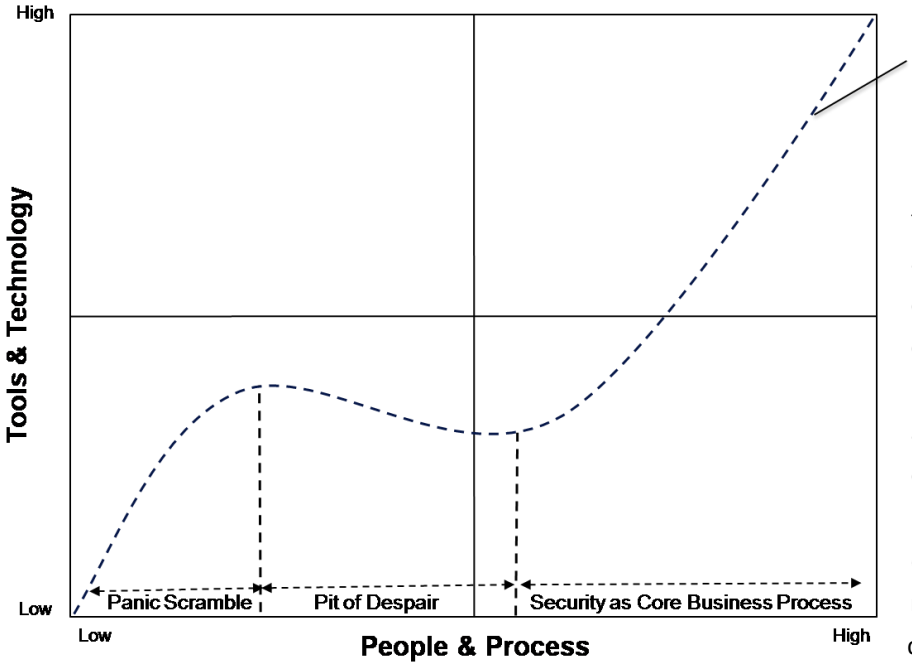
After a relatively brief period of panic, companies revisit their security investments and find the money they have spent has had only a minor impact on their security. A few areas of the company may have benefited from the efforts, but overall, security is not pervasive in either the IT or business aspects of the organization. The organization becomes security depressed as it bemoans T&T investment and languishes while pondering what to do next.

During this stage, organizations often see a *reduction* in tools usage as they try to figure out how to best leverage the investment made or rethink it altogether. Typically at this stage they do begin to invest in staff training, improved processes, and utilization of security experts to help with planning and assessments. However, they also tend to lower their budget on the tools and technology side. Without major returns, and faced with continual threats, companies will remain in this stage until a major security mind shift occurs. As procedures are detailed and driven by new security awareness and requirements, senior business and IT staff finally begin to understand the critical need to invest in long-term and company-wide security hygiene. Often after enlisting the help of third-party firms, such as consultants or security auditors, or being burned by a data breach – they move to the final stage.

### SECURITY AS A CORE BUSINESS PROCESS

Having made the important shift to understanding security as core to a successful business, organizations will begin to devote more budget (but more importantly time and focus) to the software tools required to ensure secure code in all phases of the software development life cycle, the training needed to educate developers and other non-IT employees, and the enhanced processes that bake security into all business and IT activities.

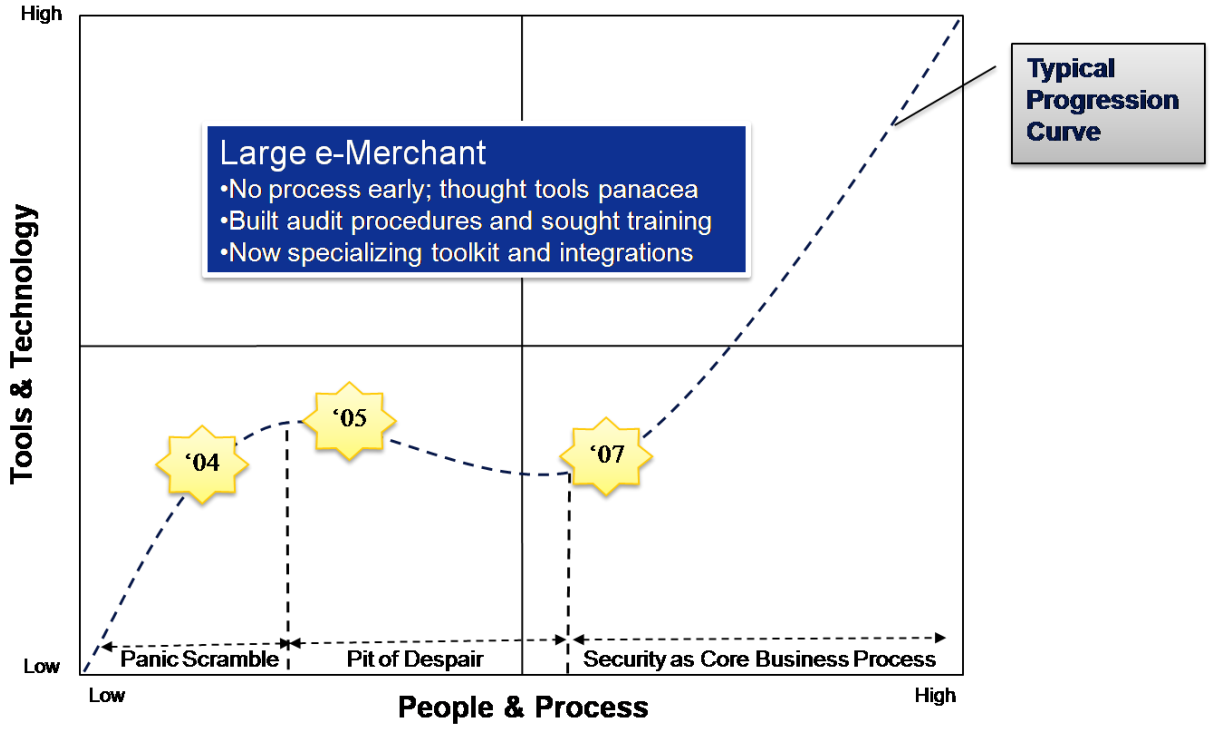
## APPLICATION SECURITY MATURITY MODEL (ASM)




This ASM Model graphic depicts a typical path an organization may take. Time is overlaid left-to-right and the speed at which an organization passes along this curve varies with their awareness, investments, and success of adopting new processes. Also, an organization's Pit of Despair may be deeper or elongated if they have difficulty adopting and integrating new tools and process. The duration of each stage and the slope of the curve can vary depending on many factors, including:

- **The influence of security-minded executives.** In many cases, business or IT executives can drive the move to the third stage quicker than it would happen normally. For example, an incoming executive that has already seen the value of being in Stage 3 in a previous company can often reduce the duration of the earlier stages and help the organization avoid common pitfalls.
- **The use of third-party consultants and service providers.** The primary research for the ASM model was based on direct interaction with organizations that have made the decision to employ external security experts. These experts can demonstrate the value of more quickly embracing security as a core business process.
- **Seeing security as a competitive advantage.** Some firms have chosen to embrace a pervasive security approach with its required increased investment in order to differentiate themselves from competitors with a more lackadaisical approach to security.

### SAMPLE ASM MODEL PLOTS (FOR LARGE ECOMMERCE ORGANIZATION)




## Using the ASM Model

Organizations can leverage the ASM Model to:

- **Determine their current location along the ASM curve.** Just knowing where an organization falls on the curve is a critical first step to understanding and improving overall security. With knowledge of where the company falls, the company can understand.
  - How it compares to others – either competitors or best-of-breed companies
  - It's likely ASM path
  - The time frame expected for the stage it is in
  - Their investment ratio

- **Circumvent the traditional curve to accelerate activities.** By understanding their current location, companies can then decide how to influence their own curve. For example, a CIO may aggressively avoid the Pit of Despair stage by embracing the proper mix of investments in tools, technology, people, and processes. That CIO may use the graph – and the organization's current plot – to help influence security investments, demonstrating the potential changes to curves as a result of too little or too late investment in all aspects of security.
- **Chart the ASM path along the curve over time.** A critical aspect of any security program is auditing systems, and charting the progress of the organization's dedication to security should also be undertaken. By periodically plotting the company's location on the ASM Model, a company can track its improvements as well as its efforts in relation to the average curve.

The easiest way to begin is with a self-assessment. Ask yourself where your organization is with respect to the T&T and P&P analysis areas:

1. Version control
2. Source code scanning
3. Defect Management
4. Test Automation
5. Web Security vulnerability scanning
6. Application-layer security mitigation (e.g., a Web application firewall)
7. Secure SDLC activities for development teams at each phase, e.g., design, code, test, et al.
8. Training (both technical and awareness)
9. Internal "Red Teams" (playing the role of attacker)
10. Third-party security reviews (at code and as-built layers)
11. Application security auditing
12. Integration of Application Security with Risk Management practices

For each area, ask both the "IS" and the "HOW" questions. For example, is your organization using test automation tools and, if so, how are they being used. And then dive one layer deeper and ask how it applies directly to your organizations' security and data protection objectives. Even this simple exercise will likely uncover some stagnant investments and need for awareness improvement.

## Conclusion

Understanding your Application Security Maturity level is critical to understanding your overall IT security posture and accurately assessing your data protection initiatives. Many people don't realize that applications and servers are responsible for over 90% of all security vulnerabilities; yet, more than 80% of IT security spend continues to be at the network or perimeter layer. There is no shortage of data points and industry studies that document this dangerous phenomenon; however, there are very few resources that give you practical advice on what to do about it. The ASM Model can be your first steps down that road.