Checkmarx

APMA

Checkmarx AppSec Program Methodology and Assessment Framework – Position Paper

> *Successful Application Security requires a well-designed and well-tuned AppSec program in addition to market leading security testing products*
>
> – Carsten Huth, Ph.D., CISSP, CSSLP, CISM, Global Head of AppSec Advisory at Checkmarx

As a leader in Application Security Testing (AST), we strive to offer market leading products. However, it is of the utmost importance to us that our customers get the best value and the fastest Return on Investment (ROI) from our products. A well-designed AppSec program is critical to achieve this objective. Based on our experience, a structured approach is highly advantageous when implementing AST products and building an AppSec program. The best approach should not only be based on proven long-running industry best practices, but also needs to be adaptable enough to incorporate recent technology trends and developments.

For this purpose, we have developed the Checkmarx APMA methodology to support our customers on their journey towards achieving their AppSec goals and sustained success. Our methodology consists of three parts: a framework, a maturity model, and implementation methods. These will be described in more detail below.

Key Features of the APMA Methodology

- Pragmatic and lightweight framework
- Maturity model with a rapid assessment options and low entry barriers
- Innovative methods to develop AppSec programs
  - Agile implementation
  - Balance between DevOps-driven and Management-driven
  - Practical best practices with clear initial guidance

Key Benefits for your organization

- Enables you to rapidly assess and understand the current state of your AppSec activities
- Understand gaps and measure progress through repeating assessments in the future
- Plan a desired end-state and carry out specific steps towards achieving that goal
- Receive practical best-practice guides for specific components of the program for various internal stakeholders

Methodology Details

1) **Framework:** The structure of components required for an efficient and effective AppSec program (see Figure 1). In APMA we distinguish 5 key dimensions, namely:

   i) The dimension ***Strategy and Governance*** focuses on high-level Goals & Objectives, Policies and KPIs, and is usually the CISO's responsibility.

   ii) The dimension ***Security Testing – Tactical*** focuses on Processes of an AppSec Program and is primarily the responsibility of the head of AppSec.

   iii) The dimension ***Security Testing – Operational*** focuses on technology, i.e., the tools and how to use them (procedures and guidelines), and is mainly the responsibility of the head of application development in conjunction with AppSec management.

   iv) The dimension ***Security Testing – Architecture and Scale*** focuses on the infrastructure required to perform security testing and is mainly the responsibility of the IT/infrastructure manager.

   v) The dimension ***Planning*** focuses on breaking down the work into work packages, a timeline, and to provision and/or train resources. This dimension is mainly the responsibility of project manager, program manager, and delivery manager.

For all the major components, we provide best practices advice. In general, best practices advice often falls short of providing clear guidance because it often only discusses potential best practices, but leaves the reader to choose the right practice. We are taking a different approach here, where each of our best-practice documents is aimed at providing clear initial guidance so that you know how to get started.

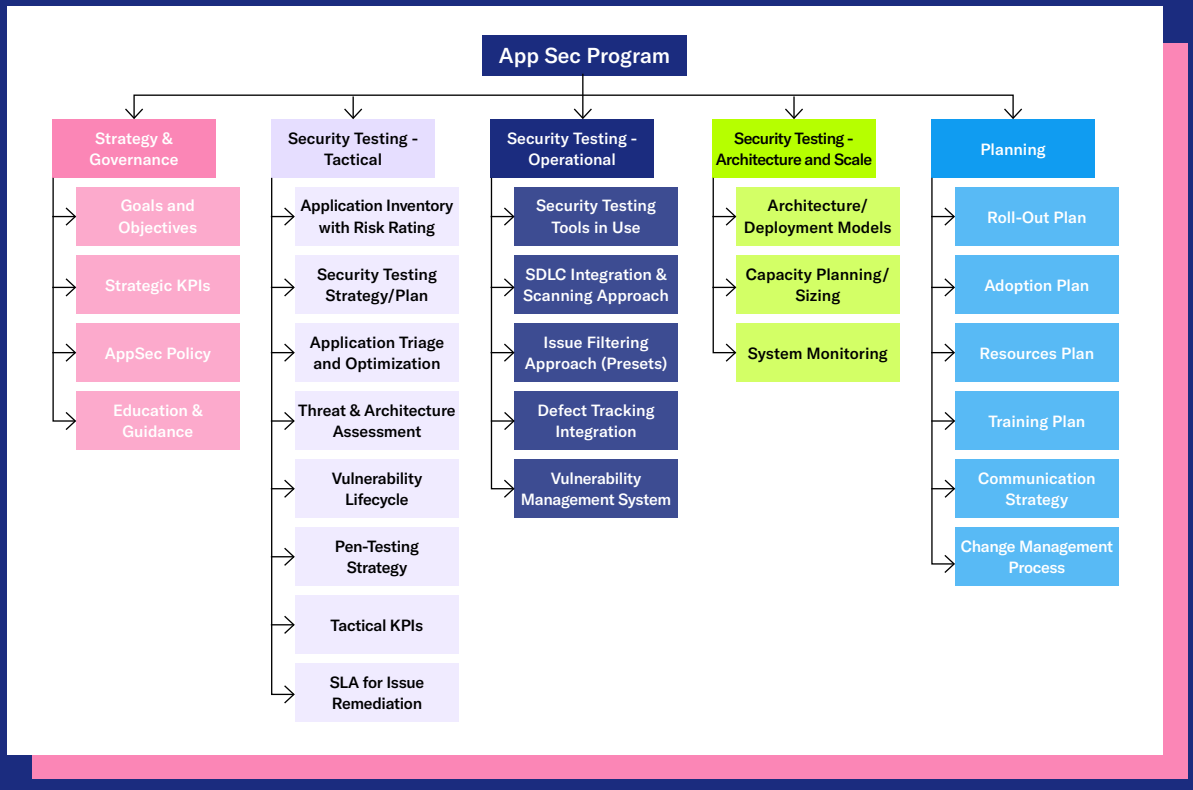


Figure 1: APMA Framework

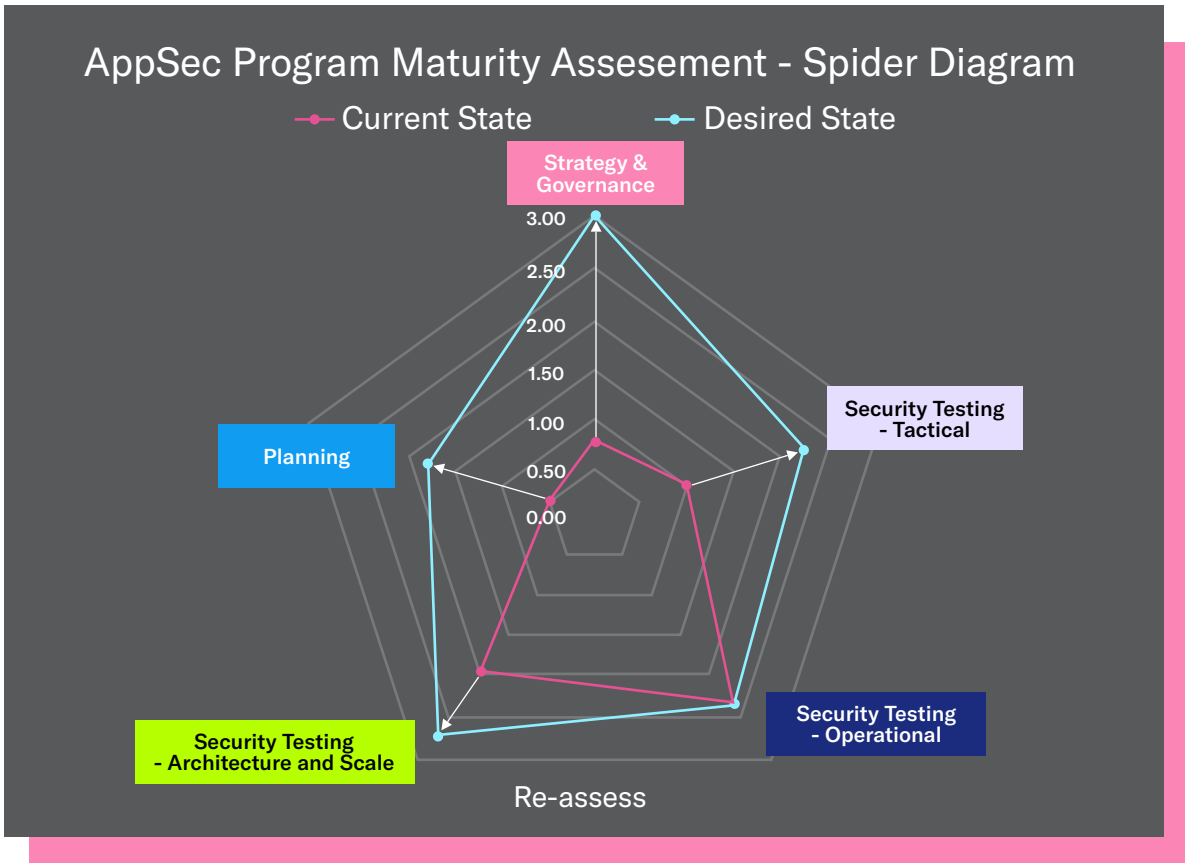


Figure 2: APMA Maturity Model

2) **Maturity Model:** We believe that it is important to measure the state of AppSec activities before starting an implementation. Using the APMA maturity model, we capture the initial state (as-is) and use it as a baseline for improvements. Furthermore, we determine a **desired (to-be)** state of AppSec program maturity in line with your goals for your AST solutions within the context of your program. We measure the maturity of each of dimensions mentioned above. Our maturity model centers around fast assessments that should take between **30 minutes** up to a maximum of one hour. Most organizations these days are skeptical about investing too much time with assessments upfront, but rather immediately desire to start taking the first steps. However, we think it is important to capture a snapshot of the ***before*** situation so that we can use this to measure progress against this baseline (see Figure 2). Additionally, we are convinced that defining a **desired end-state** of the AppSec program for the foreseeable future is needed. This prevents developing an AppSec program from becoming a **moving target**. By defining a definition of done, and carrying out additional assessments after making improvements, we can therefore measure if we have reached the planned end state **(desired state)** by comparing it with the **new current state.**

3) **Implementation Methods:** We developed implementation methods based on our many years of experience and tuned it to current industry requirements. We use agile methods and support different drivers to develop AppSec programs (see Figure 3). For example, key drivers for AppSec programs can be the information security management (CISO office) or the DevOps organization. Our implementation methods support both key driving forces (see Figure 4).

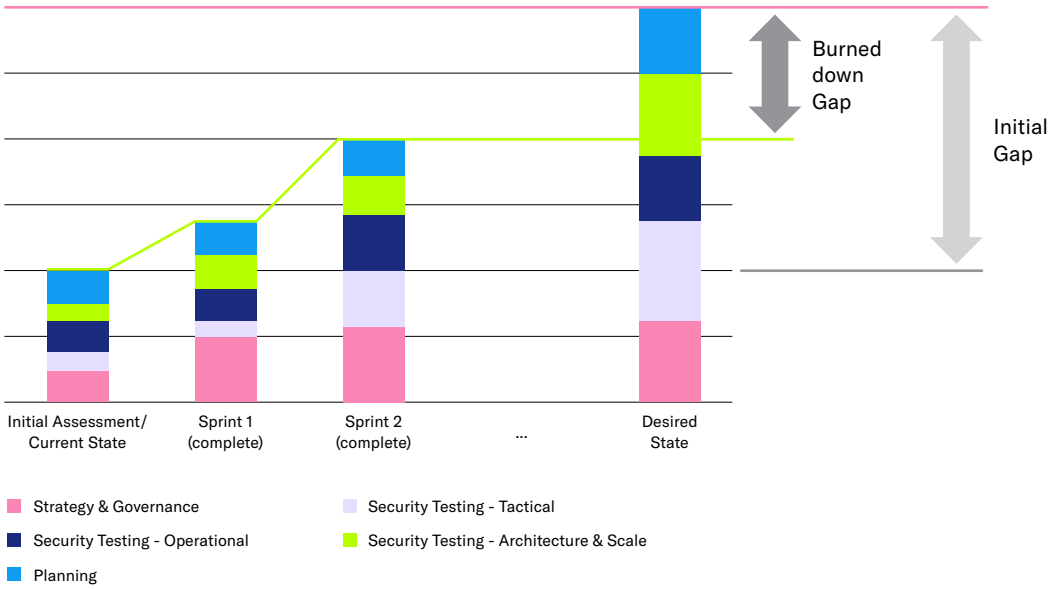


Figure 3: Gap burn down after two sprints

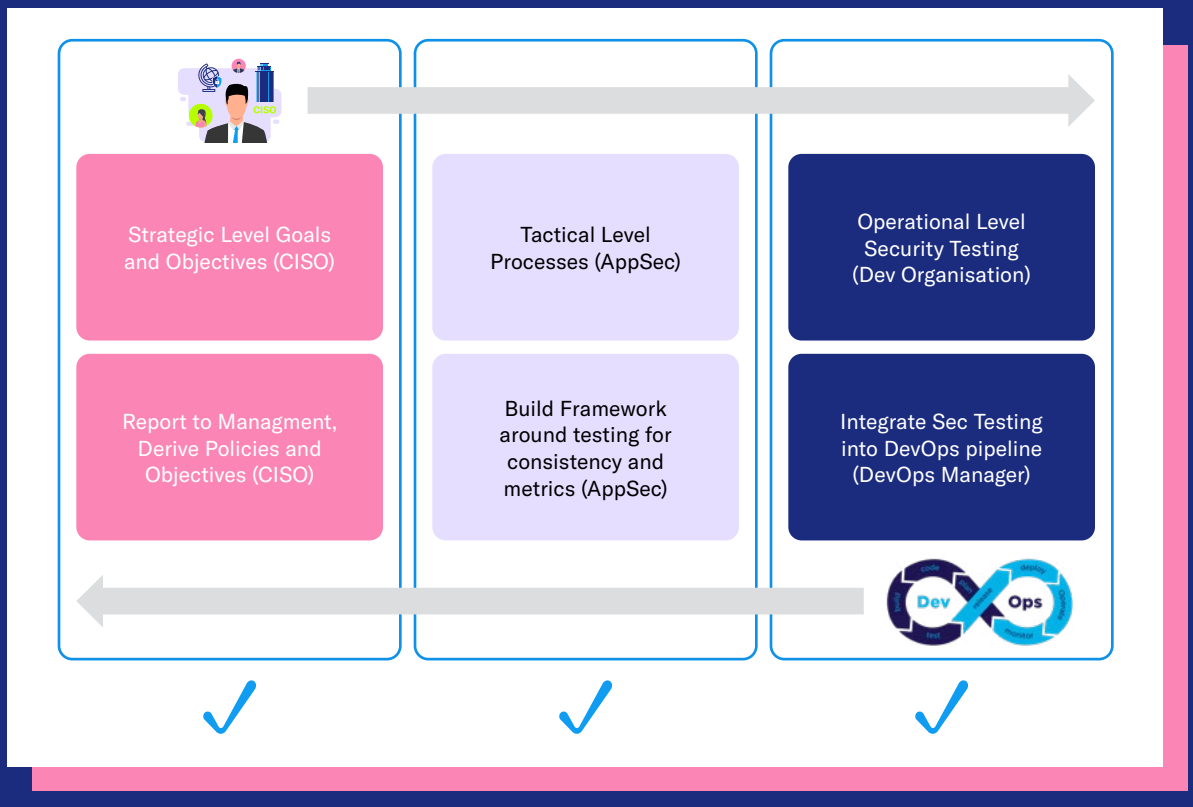
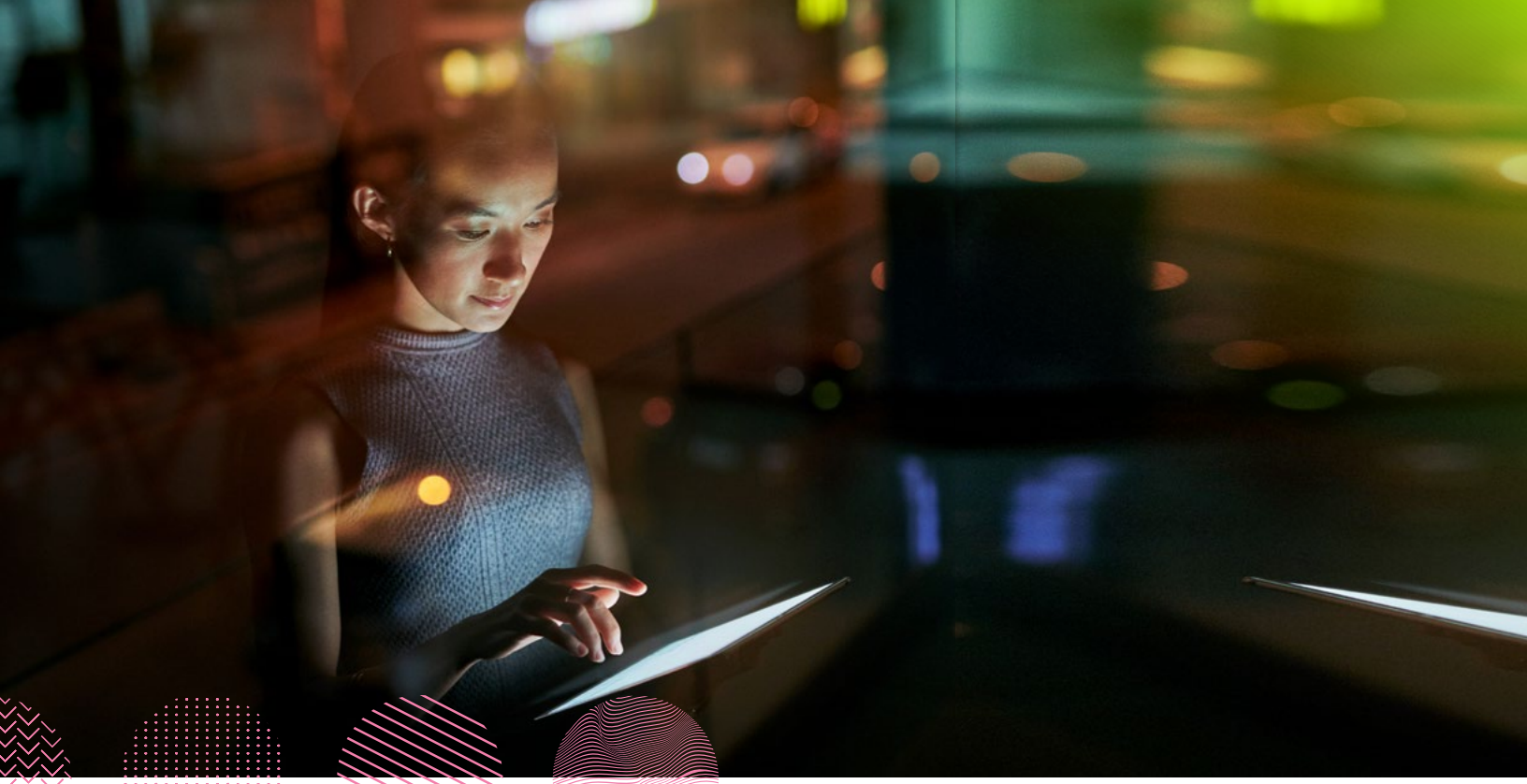


Figure 4: Support different drivers



Other Approaches – Why Create Something New?

There are other existing methodologies in the AppSec industry. However, the scope of these methodologies is often too broad for most of our customer cases. Therefore, these models have overall **low acceptance in practical implementations**. The APMA approach is designed to reduce the scope by introducing a more **lightweight model**, and to perform assessments much more rapidly as compared to other maturity models such as OWASP SAMM or BSIMM.

Furthermore, implementation cycles nowadays are expected to be weeks rather than months or years. Therefore, Checkmarx APMA approach builds on existing methodologies, but reduces the scope to what is **pragmatically achievable**, and introduces new implementation methods with execution-oriented best practices—with clear guidance. Additionally, we can adapt the model itself to quickly adjust to new developments.

Summary

To achieve success in the application security realm, organizations require a well-designed and well-tuned AppSec program, in addition to market leading AST products.

Our APMA methodology will assist you in defining an AppSec program that is directly in line with your desired end-state, and will also help you fast track your return on investment (ROI) in your overall AST investment.

Checkmarx