

SSAP

SOFTWARE SECURITY ASSURANCE PROGRAMME

Confidence to thrive from the outset.

A Software Security Assurance Programme (SSAP) is a must-have robust security programme for technology companies or organisations wanting to build cyber resilience into their applications and organisation from the ground up.

Implementing an SSAP helps to mature customers and their software development teams, who are developing and deploying in-house applications, by including security activities from the outset. This helps to ensure they are free of security vulnerabilities and that the organisation has minimised the risks posed by vulnerabilities through early detection and remediation sooner in the software development lifecycle.



Is an SSAP right for my organisation?

Does your organisation's competitiveness hinge on the quality of your software delivery?

Security vulnerabilities and weaknesses can lead to potentially damaging outcomes for businesses, including the loss of productivity, revenue, customers, and brand reputation through occurrences such as cyber-attacks, or privacy and data breaches.

The fundamental objective behind an SSAP is to build security into the development lifecycle, regardless of the development methodology in use. This ensures that security issues and potential vulnerabilities are detected and addressed early on to prevent them from being exploited.

As every development environment is not the

same, neither does every organisation follow the same software development methodology. Ensuring a well-structured and well-implemented SSAP requires smart planning and execution. Therefore, SEQA treats each customer environment as unique and takes a bespoke and pragmatic approach towards defining a programme tailored to them which helps to ensure security is built into their software development by default.



Why is an SSAP important?

46%

>> of external attacks are carried out by exploiting software vulnerabilities

ESG Modern Application Security Report 2020

60%

>> of production applications contain OWASP Top 10 vulnerabilities

ESG Modern Application Security Report 2020

\$80

VS

\$7,600

>> average cost to fix security vulnerabilities in Development vs Production

IBM Security Systems



What does an SSAP entail?

Utilising industry best practices, SEQA will understand your business and help you build a customised SSAP roadmap. It involves a combination of security strategy, planning, assessments, consulting and training to ensure

a pragmatic approach to help achieve overall organisation software security goals.

The SSAP typically involves multiple phases, and each of these phases involves various tasks to achieve certain milestones. Taking such a phase-wise approach will not just ensure a pragmatic approach towards software security assurance but also helps to save a significant amount of cost and effort in achieving the overall organisation software security goals.

Elements of a typical SSAP

1 Software Security GAP Assessment

SEQA will take the time to understand how your business currently builds software and provide an assessment against industry best practices.

2 Building a Security Framework and Baking Security into the Development Lifecycle

SEQA then create a security testing framework which includes a roadmap tailored to fit with your development practices. This will provide practical steps on how to integrate security testing into the development lifecycle ensuring it is easily understood and repeatable while also factoring in any business constraints.

3 Deliver and Support

SEQA will be your software security partner, ensuring that our recommendations are practical and understood. We can then provide ongoing specialist security support, working with your technical team to help embedded security activities such as security assessments, and design and code reviews, into your software development lifecycle.



The benefits of an SSAP

- ✓ **Avoid expensive pitfalls and delays in the later stages of a project** - The 'shift-left' approach considers security and quality assurance earlier in the software development lifecycle and is a preventative measure
- ✓ **Minimise potential risks to an organisation, including cyber-attacks, or privacy and data breaches** - An SSAP is a proactive approach to the design and development of software and applications
- ✓ **Integrate best practices and enhance the security capability of your software development team and ensure software is built securely throughout all stages of the software development lifecycle**
- ✓ **Enhance your organisations maturity and improve on a pre-existing security assurance programmes efficiency and effectiveness** - An SSAP helps to achieve this by extending its scope, engaging earlier, making it scalable etc and actively looking for continuous improvement opportunities

To learn more about SEQA's SSAP service offering, please contact us.



seqa.co.nz



0800 SEQA IT



contact@seqa.co.nz