dimension data

data sheet

Security Architecture Assessment

Traditional approaches to information security are no longer adequate to protect information networks from modern threats. Threats continue to evolve rapidly and you need to take a proactive approach to protecting your information assets.

A review of the current state of your security architecture should form part of your ongoing security improvement initiatives. A security architecture includes the unified and integrated design, implementation, and operation of security practices across your organisation. This will enable you to formulate a plan to manage risks, maintain compliance with external regulations and contractual mandates, or at least align to industry best practice.

Dimension Data's Security Architecture Assessment

Our Security Architecture Assessment is a flexible engagement through which we undertake a detailed assessment of your security architecture, from policies to technical controls. Delivered through a choice of three service models, the outcome is a specific set of recommendations that allow you to apply your resources and controls in the most effective way to protect key assets. Combined with a remediation roadmap, the results can be used to build a budget and resource plan, or simply align to an existing strategy for confirmation and reassurance.

The Assessment includes:

- an interactive workshop to assess your current and desired state
- the option to choose from a selection of security assessments that assess the security landscape
- recommendations for improvement
- the development of a security roadmap based on business and technology initiatives

Our approach

Our engagement starts with a workshop with a representative audience from your team, facilitated by one of our experienced consultants.

Following the workshop, our consultants will help you to select the optional security assessments to deliver the desired outcomes. These assessments may include:

- a review of documentation, policies, and technical controls
- a firewall assurance assessment
- a vulnerability assessment
- a tailored attack and penetration test of the representative Internet defenses to determine the adequacy of controls that support the security architecture

Options for these assessments will be discussed upfront and agreed prior to the commencement of the engagement.

Using the outcomes of the workshop and the selected assessments, we'll define your current state, review the internal and external security influences, determine the desired/required state, and make recommendations for improvement to achieve your goals in a mutually agreed timeframe.

We'll also create a dashboard that shows the current state as rated by our maturity scale, along with a future state, based on your objectives and aligned to a proposed remediation roadmap.

Our Security Architecture Assessment is a flexible engagement through which we **undertake a detailed assessment** of your security architecture, from policies to technical controls.

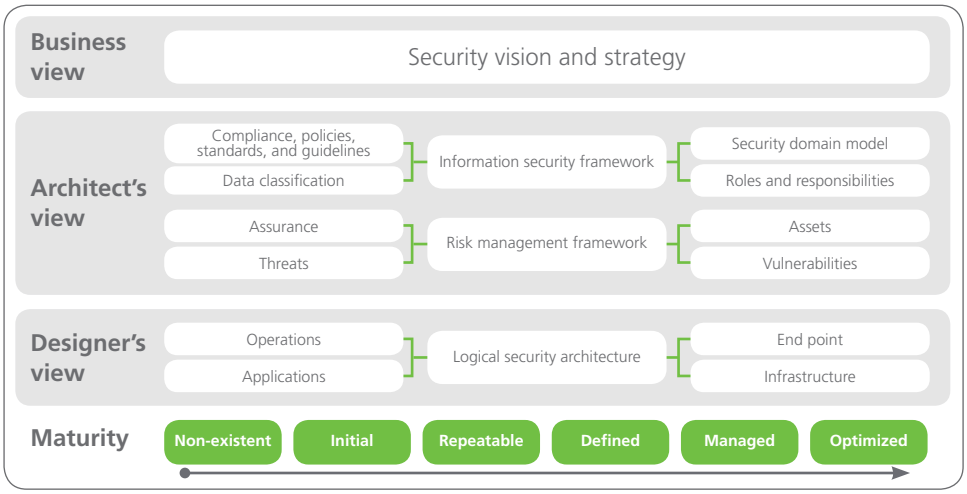

Figure 1: Dimension Data information security dashboard

Information security dashboard

As part of our assessment approach, we've developed an information security dashboard which summarizes the assessment outcomes, based on our security maturity level model.

Figure 1 represents a holistic information security framework which represents our architecture model. Concepts of the framework have been inspired by SABSA: Sherwood Applied Business Security Architecture to assist in delivering architectures based on business-driven objectives.

The dashboard can be used to illustrate maturity across an organisation, a business unit, system or simply a business application. At the end of the engagement, each of these boxes is coloured to match the security maturity level, as depicted in Figure 1.

Determining where you are, and where you want to be

As part of any organisation's ongoing security improvement initiatives, it's always recommended, and in most cases a requirement, to review the current (as-is) state security architecture and understand the need for improvement, based on the agreed future (to-be) state.

Not all organisations aspire to achieve the same level of maturity; it's driven by many factors which may include business goals, appetite for risk, security culture, budget, market vertical, regulatory compliance, and industry competition.

Our maturity model is based on the Carnegie-Mellon University Capability Maturity Model, using stages 0 to 5 to determine the level of maturity across people, process, and technology.

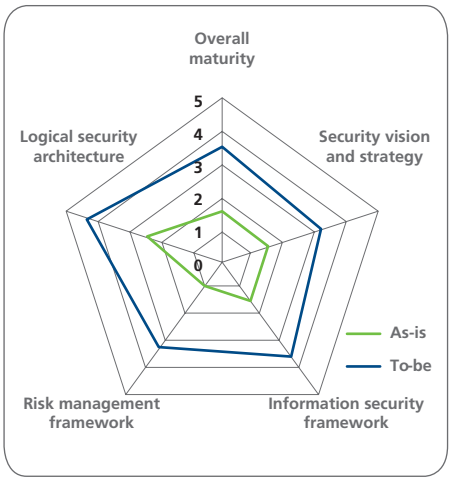

Figure 2: Illustrating current and future state

Benefits to you

Achieve tangible results

- You need to understand what security means to you and how that translates to appropriate and proportional security architecture. Our proven methodologies present solid security architectures to protect against the latest, most advanced threats, while providing flexible, agile environments that enable and support business initiatives.
- Our approach ensures repeatability and consistency. It applies a methodology that delivers adaptive and dynamic security to support and enable all business initiatives including cloud, mobility, and bring your own device.

Speak to one of our representatives today to ensure you're well-armed to protect your information assets.

Why Dimension Data?

- broad expertise across a variety of technology focus areas
- global footprint, local delivery: with over 25,000 employees and operations in 58 countries, across five continents
- proven track record: over 6,000 security clients across all industry sectors
- highly certified security consultants with expertise across various infrastructure, system, and application technologies

Service models

The Security Architecture Assessment offers multiple service models to suit your requirements:

Level	Scope
1	Workshop only
2	Workshop + architecture review
3	Workshop + architecture review + assessment(s)

Multiple service models