CYBER SECURITY COALITION.be

whitepaper Enterprise Security Architecture

2024

TABLE OF CONTENTS

INTRODUCTION

1

The digital transformation of our economy has a major impact on any type of organisation, whether public or private; small, medium or large in size; delivering products, technology or services; etc. And while this evolution offers many opportunities, on the downside, the (cyber) risks are on the rise as well. In order to be prepared, enterprises need to invest in risk mitigation and be continuously on guard. But this can be a major challenge, as a broad range of domains must be covered.

Enterprise Security Architecture (ESA) can be part of the solution. It is a practice that helps defining a comprehensive security strategy and guides its execution, adapted to the specific risks and challenges of an organisation. But security architecture is poorly understood by most people, and even those who do understand it often struggle to articulate the associated benefits. So how can an organisation determine whether security architecture would benefit them, and if so, how do they unlock and realise its potential value?

In this white paper we will introduce ESA, and give you an overview of the various related aspects. We will describe its business value, and illustrate which factors determine the success of the ESA function. We will explain how to position the ESA function, and how to get started. To conclude, we will provide a list of deliverables that can be expected from an Enterprise Security Architect. Although ESA means different things to different people, and it comes in many forms, no specific prerequisite knowledge is needed to benefit from the content of this paper. However, we assume that the reader is familiar with or has an interest in Information- and Operational Technology (IT/OT), cybersecurity and risk, and is familiar with the typical roles in the governance and organisation of businesses, such as the Chief Information Officer (CIO) and Chief Information Security Officer (CISO), just to name some typical stakeholders of the ESA-function.

This document can thus be of use for anyone interested in the ESA practice, whether in a small, medium or large organisation. The goal of the paper is not to provide a comprehensive bible on ESA. However, after reading this paper, you will better understand the necessity, role and key success factors of ESA. Moreover, you can use this information to initiate a discussion about the use of ESA and the necessity of an ESA function in your organisation and, once decided, this white paper can serve as a guideline to get started.

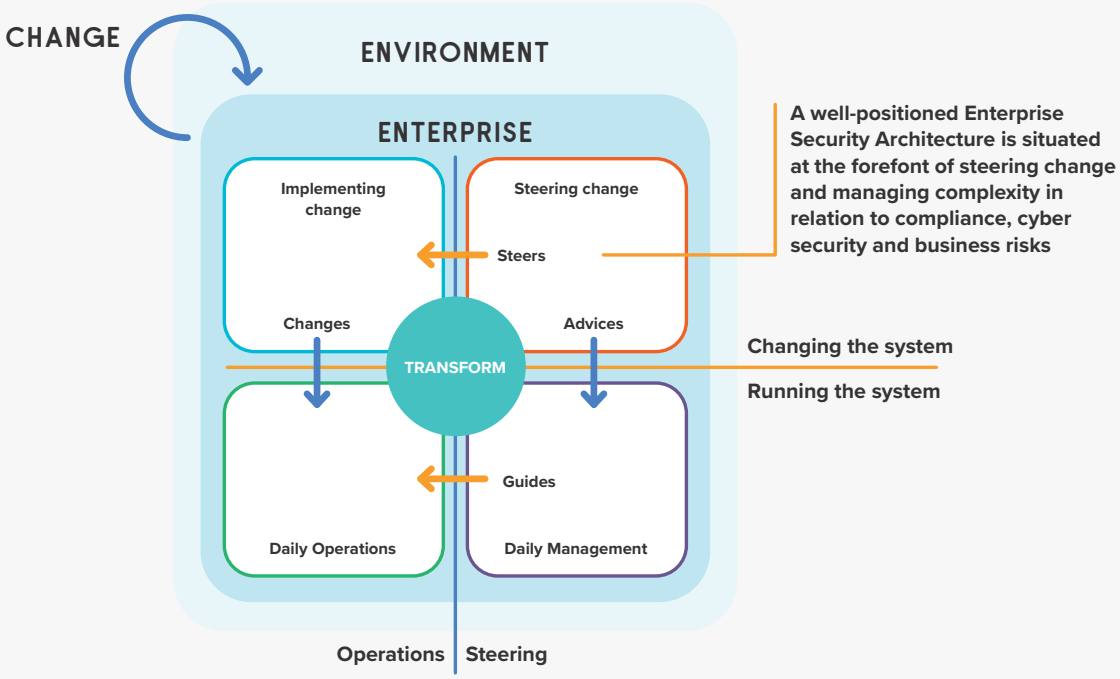
2 ENTERPRISE SECURITY ARCHITECTURE (ESA): AN ESSENTIAL PART OF THE DIGITAL ECONOMY

In this context, we consider an enterprise as being *a single or a collection of organisations that have a common set of goals and/or a single bottom line*. An enterprise can thus be a government agency, a whole corporation, a division of a corporation, a single department or a chain of geographically distant organisations linked together by common ownership. The term can also be understood as an "extended enterprise", which then includes partners, suppliers and customers. Large corporations and government agencies may comprise multiple enterprises.

Just as architecture provides a way for architects to convey complex information about the design and construction of buildings, Enterprise Security Architecture (ESA) can help in the selection and design of security capabilities and support the implementation of IT/OT and cybersecurity solutions. It includes elements of people, processes, information, and technologies, as well as, importantly, the culture of the enterprise in a complex and changing environment. We use the term "Enterprise Security Architecture", because we consider IT/OT and cybersecurity throughout the enterprise to be an important element that contributes to secure enterprise design in the understanding of business risks.

What is Enterprise Security Architecture about?

Enterprise Security Architecture (ESA) is about understanding the enterprise's strategic direction and business objectives, and taking actions to mitigate risks. ESA practices provide a comprehensive and rigorous method for describing, modelling and structuring the current and future state of an organisation's security ecosystem. Implemented through projects and programmes, the security strategy will deliver real results and achieve its goals in support of the business strategy, improving the chance of reaching those business goals in an effective and efficient manner by using a consistent, systematic and structured approach. It is an essential part of the relatively fast evolution of the digital economy, and is related to all aspects and layers of an enterprise: ranging from technological advancements, process innovations, awareness and training aimed at protecting enterprise assets against cyber attacks. ▶



An ESA can address a wide range of concerns expressed, for example, through architectural views, models, methodologies, reference frameworks, processes, technologies, organisation and communication. It is a discipline where “qualitative” concerns are addressed, such as agility, availability, flexibility, maintainability, fitness for purpose, reliability and resilience, just to name a few.

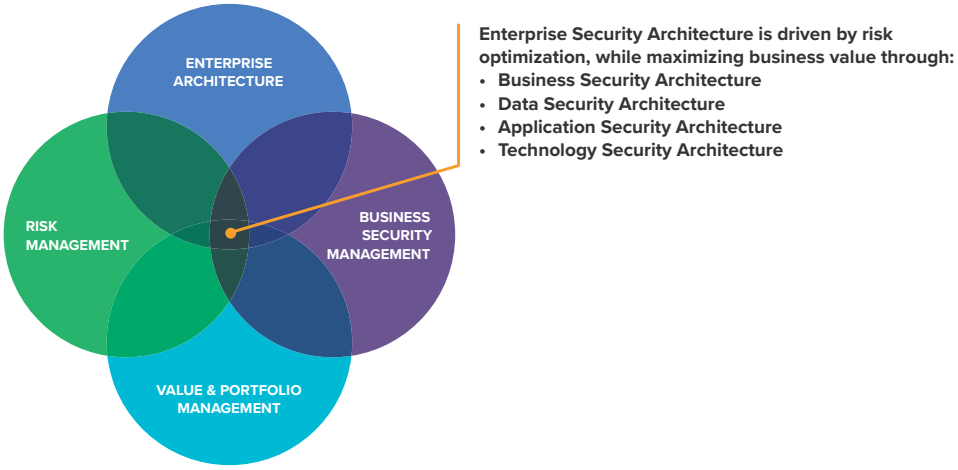
An ESA simplifies the process of selecting the right capabilities, meeting both compliance and auditability requirements.

An ESA approach enables the prioritisation of security projects. Once the framework and capabilities for the security architecture have been developed and the gaps identified, an implementation plan (programme) can be drawn up and executed, and priorities specified. This is usually a long-term effort, depending on the size, budget and maturity of the organisation. It also requires continuous evaluation and adjustment in view of the rapid developments in the digital economy.

In a context where it is a challenge to manage complexity, i.e. with regards to technology, and to steer change it is critical to enable and support transformation initiatives, the primary purpose of an ESA in this context is to:

- ensure that business strategy and IT/OT & cybersecurity are cohesively and continuously aligned in an agile way;
- enable informed, risk-based decision making;
- establish the context for the definition of security objectives and the selection of investment;
- offer a common language to the organisation, and act as the basis of the organisation’s cybersecurity measures, for a holistic end-to-end view that links the business (product, legal, etc.) and technology.

Last but not least, an ESA usually runs transversally across the four domains that together make up the Enterprise Architecture: the Business Architecture, the Information Architecture, the Application Architecture and the Technology Architecture.



Security is a property of each of those domains, each with its specific characteristics. Enterprise Security Architects (ESA´s) aim to bring coherence to the enterprise's information security attitude, while keeping the business benefits in mind. Business cases would not stand up if several projects all procured their own security solutions, for example.

Architectural views can link business needs to security processes, technologies and people, and can simplify decision-making. The views become less abstract and more detailed as they translate business requirements into security controls.

To succeed, it is a good practice to be surrounded by experts who can add simplicity instead of complexity. It is also better to have a limited number of elements to explain, rather than several elements that must be explained repeatedly.▶

What is ESA not about?

ESA is not an “all-or-nothing” proposition. Some organisations can benefit from picking and choosing certain elements of security architecture practices. ESA is typically not about running projects, implementing solutions, analysing security threats within a SOC (Security Operations Centre) or configuring systems. Certainly, ESA is involved in such activities, even if indirectly, but they are more the domain of IT/OT and cybersecurity engineering/operations staff. Smaller organisations with a limited number of security profiles might have individuals who aim to bring coherence to the enterprise’s security attitude and stay closely involved in the day-to-day operational tasks as well. This can be challenging for them, because driving a security direction or journey while being absorbed with keeping systems up and running is not easy. An ESA profile adopts Enterprise Architecture (EA) practices and extends them with IT/OT and cybersecurity specific methods and artefacts. ●

some STATEMENTS

1 The CIO needs to understand and approach security by design as an enterprise-wide management component, not just an IT component.

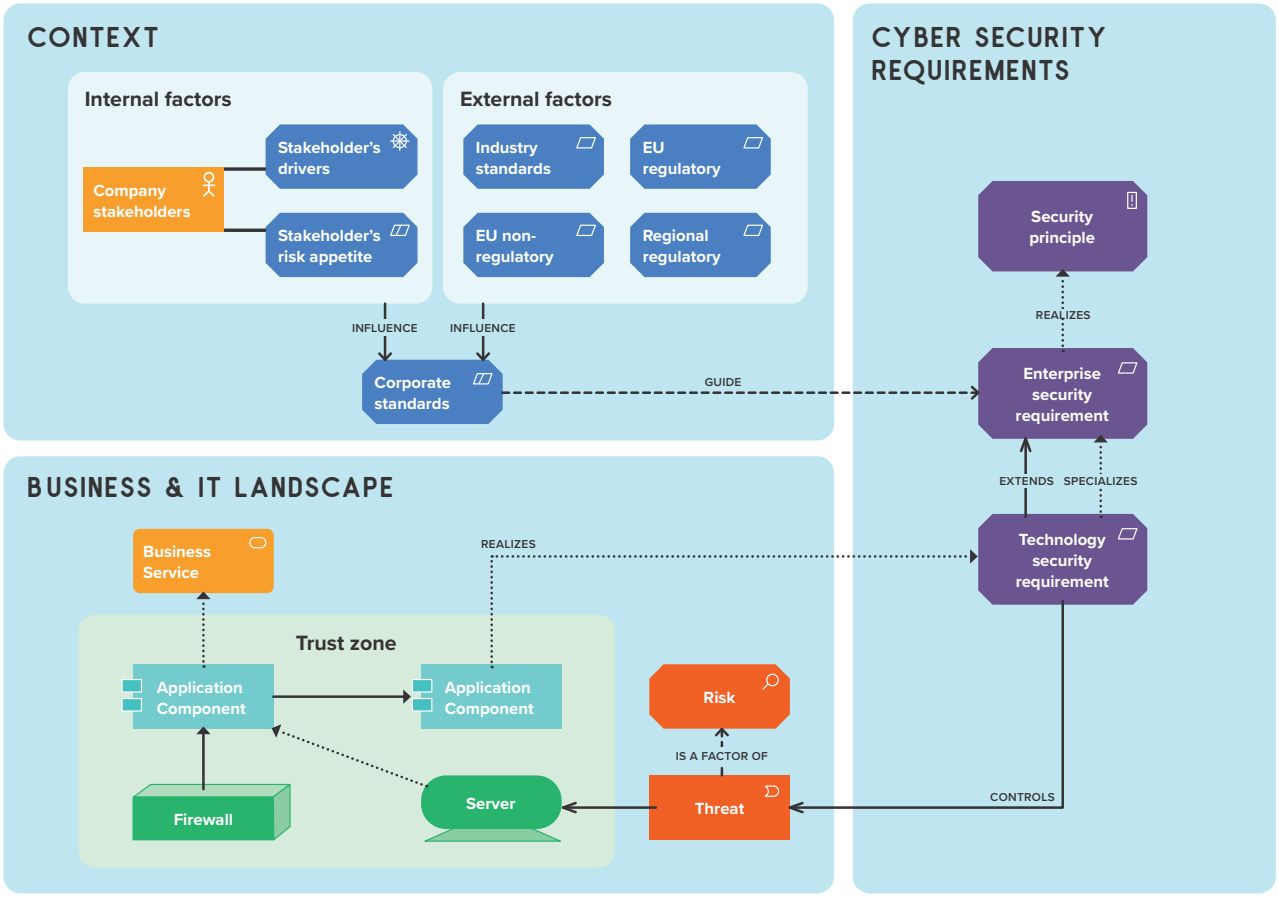
2 The CIO should set the expectation that management will establish an enterprise-wide security architecture framework with adequate staffing and budget.

3 Management discussions of security architecture should include identification of which design principles and requirements to select.

3 WHY DO YOU NEED ESA AND WHAT IS THE BUSINESS VALUE?

Business and IT programme objectives drive changes to security. Without security architecture, these changes can be chaotic and inefficient. Cyber attacks are getting more and more sophisticated, using different techniques ranging from social engineering to malicious software such as ransomware. Measures to mitigate those risks and safeguard assets should be integrally embedded in the organisation. Regardless of the methodology or framework used, an ESA must be defined based on the risks specific to the enterprise. Within the digital economy, technology is a key factor and influences all aspects of the enterprise. The ESA practice supports organisations to navigate complexity within their digital transformations. It plays a crucial role in successfully aligning a defined architecture with the business's security objectives, in understanding how to improve decision-making, efficiency and contain costs, in supporting agile and innovative business practices, and in making the best out of defined security solutions.

The ESA also has a strong relationship with other elements in the enterprise, such as Enterprise Risk Management (ERM) and Enterprise Architecture (EA). Although an ESA might be viewed as a single architecture, it should never be seen as an isolated architecture. It is about designing, modelling and structuring of organisational, conceptual, technical (logical and physical) components, people and processes that interact together to achieve and maintain a state of managed risk. It also provides



support for enabling secure, safe, resilient, reliable behaviour, while managing security and privacy throughout the enterprise.

Organisations that successfully implement an ESA identify and manage IT/OT and cyber risks proactively, prioritise the investments, create transparency, design mitigation measures at all levels, and embed security principles, requirements and counter-measures across all their processes and programmes. They involve ESA team members (including IT security operations staff as security domain experts), stakeholders within the business and IT, external parties and partners in order to increase overall awareness, to ensure that appropriate decisions can be made across all security aspects of the organisation, including reporting on fraudulent or suspicious behaviour.

The ESA contains elements of people, process, technologies and, importantly, the culture of the enterprise in a complex and changing environment. The practice supports changes in the enterprise by providing a balanced view of risks in such a way that negative consequences are kept to an acceptable level while positive opportunities are exploited to their maximum. The ESA supports a security programme management approach by linking security activities to enterprise missions and business goals through risk management methods. It addresses questions such as:

- What do our business and IT strategy tell us about the risks we should mitigate and the security capabilities we should maximise?
- What are the most important assets of the organisation?
- What will it mean for the enterprise if something goes wrong?
- What are the biggest gaps and priorities?
- What is the current state, what will be the future state, and which architectural elements do we need to close the gaps?
- Which preventive, corrective and curative controls do we need?
- What does this mean for the design and setup of the capabilities?
- What capabilities are necessary, in terms of people, information, processes and technology?

4 WHAT INFLUENCES THE ESA PRACTICE AND DETERMINES ITS SUCCESS?

While it is desirable to standardise and apply good practices from other organisations, each enterprise has its particularities, which are reflected in its ESA practice. For example, something important in a certain environment, may be less so in another. It is thus important to analyse the context in which the ESA function operates, to identify the environmental factors that must be accounted for, and to understand how they will shape the ESA function. This helps to determine the objectives for security architecture. The ESA does not always need to be installed by design, and can be developed progressively over time, enabling the organisation to make a sound choice for a security architecture that matches its needs.

Certain environmental factors inevitably shape the context in which the security architecture practice takes place. And while the size (small, medium or large) of an organisation may frequently reflect the size and maturity of its security architecture practice, other factors also play a major role.

Are you looking for a figure what small, medium or large mean? Note that the size of the organisation is not the only factor that influences the ESA practice.

We have identified the following environmental factors

- **size of the organisation**
- **organisation of the business**
- **sector and industry**
- **company culture**
- **risk appetite**
- **sourcing and vendor selection strategy**
- **innovation and self-disruption strategy**

Size of the organisation

The size of the organisation is a typical factor that influences the security architecture. Smaller organisations might have a single person taking on multiple architecture roles, combining security with other architectural domains such as information and infrastructure architecture, or even combining the security architect role with roles outside architecture, including risk management, risk governance and security engineering, thus creating a large span of control.

Medium-sized organisations may have more people per architectural domain, thereby creating clearer borders of responsibility between each role and allowing the security architect to focus more on his core duties. As one might expect from large-scale organisations, which have more means at their disposal but also more obligations, each role may be fulfilled by several people, organised in dedicated teams of expertise.

Sector and industry

The sector or the industry in which the enterprise operates can directly affect the security architect's role and contributions. Every business is subject to regulations, starting with the general laws at different political levels (local, regional, national and international) that apply to businesses, irrespective of their sizes. So, businesses need to take a systematic approach to compliance. When those rules relate to risk, compliance or security, the role of the security architect becomes more prevalent.

This is independent of the scale of the organisation, such as in the case in the healthcare sector, in which companies are required to adhere to the same health regulations. Another example is enterprises that make security and safety their core activity: they must comply with a vast number of regulations and industry standards that apply to the targeted customers (e.g., ISO 27000 series, NIS2, etc.).

Organisation of the business

While it is expected that large organisations may have multiple lines of business and even multiple entities, small and medium-sized businesses also grow organically through external acquisitions, and can thus comprise a collection of lines of businesses and entities. Enterprises may let those entities operate in different manners: "stand-alone" (largely independent), "federated" (with a degree of alignment and a degree of freedom), or "integrated" (making them appear as acting as one entity). These choices inevitably impact the enterprise architecture and thus also on the ESA, with different levels of IT and security standardisation, and higher or lower margins of freedom and span of control for the security architect, etc.

Company culture

The company culture should not be seen as the static result of a business, but as a continuum that influences the next business choices, which then feed the company culture. For example, enterprises setting high standards for themselves (whether for productivity, quality, innovation or ethics) must organise themselves to deliver on their promises. This leads to architecting the enterprise around those fundamental choices, thus also to shaping the role of the architect and of the security architect in particular, who might be highly present or totally absent, depending on the company's culture.

Risk appetite

The enterprise's risk appetite, whether it is "risk-averse" or "risk-tolerant", influences the agenda of the security architect. It is common to associate small enterprises with a high-risk appetite and large ones with a risk-averse profile. This is, however, not systematic and is also not necessarily a choice a business can make freely.
Small businesses may be taking risks that are proportionally large for their size, but that are relatively small when put in another context. For example, a company taking out a large loan from a bank might be taking a sizable risk for itself; for the bank, however, the amount of credit might well be "invisible" in the vast sea of credits it has with other customers.

A business's risk appetite is also shaped by the industry practices and the regulations inherent to the business, which may strictly constrain the freedom of the enterprise to take risks. The margins left by external business regulations can be such that the business is not allowed to take more risks than it might contemplate. This is especially true for businesses concerned with health and safety regulations, for the financial sector regulated by a "prudential supervision"[1], or for the business engaged in running "critical infrastructure"[2].

The importance of the security architect's roles can be correlated with the enterprise's risk appetite. Risk-tolerant enterprises need to organise themselves to take those risks and then quickly respond to changes, and thus must factor corresponding capabilities in their enterprise architecture, including their security architecture.

Sourcing and vendor selection strategy

The security architect's activities and duties are shaped by how the business chooses to select vendors and to source primary or secondary activities. In an enterprise that is heavily dependent on external providers and outsourced activities, the security architect's role will be oriented towards specifying the security objectives and requirements, challenging the business partner, and assessing the quality of the evidence of the security implementation, but leaving the implementation choice to the business partner. It thus involves creating a coherent enterprise architecture by assembling the right puzzle of solutions and vendors.

On the other hand, in an enterprise that is building its own solutions, the security architect will tend to constrain the implementation choices of the engineering and development teams through policies, guidelines, standard solutions, etc., and sometimes through security code reviews or by writing security code himself in enterprises where security knowledge is scarce.

Innovation and self-disruption strategy

The company's innovation and self-disruption strategy can be related to its risk appetite. It is nevertheless an independent facet of the enterprise. Innovating and disrupting oneself before being disrupted can be done with various levels of risk, or alternatively can be totally absent in conservative enterprises or enterprises choosing to keep the status quo. This will be reflected in the enterprise's architecture and security aspects, and thereby in the security architect role.

Conservative enterprises typically have a stable security architecture, which can be an asset but which can also turn into a difficult legacy. It is an asset when iterative improvements tilt the security architecture towards high levels of standardisation and integration, and make it possible to seize the resulting benefits and economies of scale. These organisations might also lean towards a web of legacy solutions that remain untouched due to the lack of a need to change, considering the risk of the heavy costs that can be incurred, in particular for sudden changes forced by external disruption.

In contrast, enterprises driven by innovation and self-disruption need an architecture with the flexibility to enable rapid and fundamental changes. This is partly done by projecting the security architecture into the future to identify early on where the enterprise might run into a steep change that requires an agile approach to set the change in motion over time, and to avoid building a big solution for a hypothetical future, which, as a moving target, will likely alter over time.

1 Prudential supervision: www.nbb.be/en/financial-oversight/prudential-supervision
2 Critical Infrastructure: en.wikipedia.org/wiki/Critical_infrastructure
3 Position paper: www.iia.org.uk/resources/delivering-internal-audit/position-paper-the-three-lines-of-defence

POSITIONING THE ESA FUNCTION IN AN ORGANISATION

5

Enterprises wonder where they should place the ESA function within the organisation, so that it is in the best position to accomplish its mission and have impact. There is no simple answer to this question. The ESA function can be positioned in different places within the organisation.

Some typical cases include:

When the ESA function ...

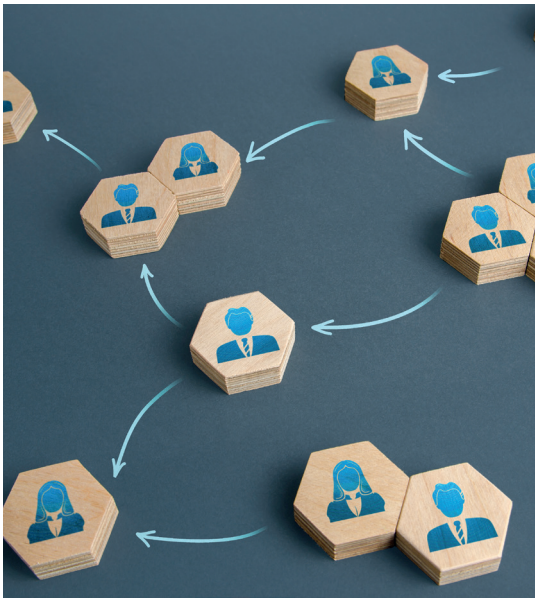
- is part of the Enterprise Architecture (EA) team, it can create security specifications that align better with business strategy. Often, this positioning creates a stronger working relationship between security architects and enterprise architects. There may be some decisions that the IT and security operations teams cannot take, however.
- is positioned within the Chief Information Officer (CIO) team, it may lean more towards operational technical challenges, and miss out on a holistic view over the business strategy or direct access to the skills and expertise of the enterprise architecture function
- reports to the Chief Information Security Officer (CISO), deliverables may better be aligned with the security strategy, allowing the CISO to make focused decisions about information security without competing with other business priorities. One disadvantage can be that the ESA function is not sufficiently aligned with the EA efforts, and can be inefficient in managing dependencies in the solution and infrastructure landscape.

In other words, the role of the ESA function can be challenging, balancing between the first line and the second line of defence[3], trying to find a consensus between different stakeholders, meeting the security and compliance requirements imposed by the CISO and/or regulatory security obligations, and all without slowing down the dynamic of the organisational digital transformation.

The ESA function actively associates with business, operational and compliance teams. The development of security capabilities should not be separated or isolated from other initiatives.

If someone is capable of integrating security capabilities in the EA and operational efforts, by design and with a balanced view of risk, there is a higher chance that negative consequences will be kept to an acceptable level through risk optimisation while maximising business value, allowing decision makers to take well-informed decisions moving forward.

Finally, an ESA function can be perceived as a barrier to agility, standing in the way of an iterative and incremental delivery. This does not have to be the case, though. It is all about a mindset, being transparent and pragmatic about how the requirements must or can be achieved, making well-informed decisions, and sharing responsibility. Avoid being the individual in the ivory tower who imposes security requirements and then leaves it up to others to figure out how to implement them. The role and mandate of an ESA function very much depends on the context, nature, culture, maturity level and scale of the organisation - but also on the ESA function's knowledge, attitude, behaviour and coaching capabilities. An ESA function should be multilingual, which means: speaking the language of business, IT and governance. In the end, it is a matter of working together.



6 HOW TO GET STARTED AND DEVELOP AN ESA PRACTICE?

A key question is how to implement and maintain an ESA practice. The objective of this white paper is not to create a detailed “how to” guide. However, we are happy to share some of our insights for developing and using an ESA practice.

Establish your objectives for the ESA

It is essential to ensure that the views and elements of the security architecture address specific business needs. Engaging with business leaders, project sponsors, new initiative leaders and IT representatives is key. When doing so, use the language of the business and avoid jargon, to demonstrate that you understand their role and concerns. Focus on cost efficiencies and other advantages such as standardised compliance processes, reduced frequency and duplications, trust relationships, business continuity and resilience, the impact of security incidents, etc.

Next, identify how security architecture is currently used. Build on what already exists. Do not make the mistake of developing the "ultimate holistic framework"; instead, engage in a tactical architecture project and learn from it. Analyse the architectural context to determine what practices are in use, which frameworks are being used and how, which team structures and relationships are in place, etc. Define how security architecture will help the organisation to reach its objectives. Guide small incremental changes on the as-is security architecture by means of actionable remediation plans to improve the current security posture. Establish targets and ways to measure progress against those targets over time. And last but not least, start small and deliver value quickly.

Determine the best way to achieve the objectives

With this in-depth insight on the objectives, determine what architectural views and elements can help advance security and business objectives. Specify the best way to achieve the established objectives. The reliance on existing frameworks (i.e., SABSA, TOGAF, COBIT etc.) can help you to structure the approach and to guarantee that the security architecture defined aligns with business goals and objectives.

Describe the current and the future state of the security architecture. Use visual representations that compare the current state with the future state, (re)use existing views, ask relevant questions. Determine what to create or update, and gradually build on knowledge. Establish how to update architectural content by defining resource requirements, create plans, and obtain the necessary approvals to create and update views and elements. Develop content by working with project teams and domain experts to create and update the views and elements. Apply version control over the changes ▶

to the views and elements, to ensure updates with pre-existing systems, processes and technologies.

Nevertheless, most companies do not start from a blank sheet (green field), which means that the existing systems probably should be reused and/or remodelled. Sometimes it is not wise to put too much emphasis on the existing environment when designing the conceptual components. The details of the existing environment will be taken into account more at the level of the logical and physical design.

Define design principles and requirements

Any organisation that applies security architecture will need to use a number of security-by-design principles and requirements as a minimum key reference. Security principles are the building blocks for determining why information assets need protection within an organisation. Principles should be followed when developing

architecture, reviewing and approving projects, and implementing security controls. There are many design security principles that can be defined, including:

- secure by design
- defence in depth
- secure by default
- default denial
- separation of duties
- fail secure
- weakest link
- least privilege
- access on need-to-know basis
- secure in deployment
- usability and manageability

Security requirements describe more functional and non-functional requirements of system users or a quality the system must possess to increase user trust.

A first set, and a key source of requirements, is the business areas. The business has internal requirements, such as service level requirements for customers, anticipating new business opportunities, and ensuring business resilience and continuity. External requirements are more driven by legal and regulatory compliance requirements or security threats in relation to the internet.

A security requirement is a statement of a needed security functionality that ensures one of many different security properties of software is being met. Security requirements are usually derived from industry standards, applicable laws, threat models and a history of past vulnerabilities.

Three types of security requirement obligations can be considered in the organisation:

- Regulatory security obligations: these are legal, compliance or contractual obligations that the security team must fulfil. For example, all organisations handling personal data must comply with the GDPR (General Data Protection Regulation).
- Business security obligations: these are the security commitments of the organisation. For example, ensuring that corporate assets and information – customer data, employee files etc. – is kept secure yet accessible when needed.
- Customer security obligations: these are the security commitments that the customer expects from the organisation. For example, customers of a manufacturing company that provides custom-made parts may require all proprietary blueprint files to be properly encrypted. ▶

Develop expertise and skills

Obtain the right balance of skills. Security engineers might select solutions that cover a specific problem, but that cannot be reused in other transformation efforts. On the other hand, security architects might design security architectures that are interesting in theory, but expose their limitations when implemented.

ESA functions have a broad role and often have a technical background; however, they need to communicate with the business, IT and overall governance of an enterprise. An ESA function sometimes use terminologies that are unknown to the other stakeholders.

Risk & control modelling

The risk model in the architecture repository should identify the assets of interest and incorporate a detailed threat catalogue. This model is much more fine-grained than those used in the Enterprise Risk Department, as it will support threat-modelling, which is one of the processes that drives control selection. Only the threats relevant in your environment and your risk appetite should determine which controls are eventually selected for your security strategy.

Some authoritative methods describe assets as “business quality attributes”, not physical resources. This means that not only the confidentiality, integrity and availability attributes of information, but also the cost-effectiveness attribute of a business process (relying on information), etc., are measurably protected.

Use a qualitative risk management method before a quantitative one, as the latter requires a higher level of maturity.

Learn and improve continuously

Learn continuously how to create an efficient ESA that can be maintained and support the business over time. Use a flexible approach for developing and using security architecture that can be tailored to suit the diverse needs and changes in your organisation.

Even when for example information security and an agile mindset do not always go hand in hand it’s crucial to find a balance and ensure that security is not compromised while maintaining the agility of the development process.

Mature the practice

More mature organisations have an Architecture Development Method (ADM) adopted for security, while tailoring their needs to their enterprise. Such a method consists of a process and a content framework:

- The **process** prescribes the sequence of activities (phases) and the possible iteration cycles. Just as in software development, the modern architecture process involves an iterative approach. Iterations can occur in different areas in the process, simultaneously triggering activities at different levels of the architecture eco-system (enterprise architecture, domain architecture, solution architecture).
- The **method** content framework prescribes the detailed roles, tasks, work products and techniques to produce architectural deliverables in each of the phases of the process. A typical framework will be derived from the Zachman ontology for enterprise architecture, distinguishing the Why-How-What-Who-Where-When aspects in several layers of abstraction, starting from a contextual and a conceptual model. A holistic method framework for ESA will be composed of architecture domain-specific frameworks, such as a risk framework, a control framework, etc.

Tailoring the method means a selection is made in the framework of items that will support the architecture engagement at hand. For guidance on the tailoring, see also step 4.

Choose an Architecture Description Language (ADL). This is a graphical formalism (language) used to present stakeholder views across the architecture model, as well as to facilitate the management of the building blocks and their relations as part of the models. In software development, UML is very popular.

Acquire an architecture management system (tool). In a method implementation, the framework data is persisted in a system of records, aka the Architecture Repository, which supports:

- The development of domain models and views
- Architectural decision making (rationale and registration)
- Collaboration between different architecture roles with a single source of truth
- Lifecycle management of building blocks
- Architectural traceability

For enterprise (security) architecture development, several tools can be used, such as Sparxsystems, Archi or LEANIX, among others.

With the help of the repository, the ESA function maintains oversight of the different domains: business/IT/OT (i.e., the risk environment ▶

itself), risk (i.e., risk factors, threats, vulnerabilities, etc.), control (i.e., control objectives, security tactics & patterns, control design effectiveness, control operating effectiveness, etc.), security services (i.e., security mechanisms, components, etc.) and security management (i.e., secure operating procedures, or at least their identification). In its most basic form, the management system is a spreadsheet workbook, where the architectural building blocks are managed in tables. Depending on the tailoring, a more robust solution could be envisaged, but a tool without a plan will not cut the deal. Architectural standards will facilitate the reuse of architectural work products, including their extension and specialisation through stepwise refinement.

Train the people to apply the method. Make sure to select a method implementation, with actionable procedures and data, and not just concepts. A lot of energy and money can be burnt in academic lectures or "a mile wide and an inch deep" training programmes provided by elitist institutions. In the end, the framework will be populated by you, selecting what works for you and ending up with a best-of-breed composition of a variety of industry standards.

For guidance on the development of these architecture management capabilities, a Capability Maturity Model for security architecture can be very helpful. However, one pitfall to avoid is executing the method exhaustively. To avoid analysis paralysis, the method should be "tailored" in method adoption workshops, selecting the appropriate method components for the mission and maturity level of the architecture organisation.

Design authority

Make sure to **install a governing body for security architecture** with an adequate representation of stakeholders from the business and IT/OT. Security should have a seat in the company's overall Architecture Review Board to ensure optimal alignment between business, IT/OT and security.

Maintain a log of architectural decisions in the Architecture Repository. Document the options, assumptions, associated project risks, justification of the final choice, consequences and dependencies. The Architectural Decision Record will enable the auditability of the architecture practice. Churn on decisions taken previously can be avoided.

Also **maintain a record of granted exceptions** and exemptions to security architecture compliance. Note that one can be compliant with security policy but not with security architecture, and the other way around.

The ESA practice can be distributed across the three lines of defence[1] (3LoD), because all LoD need the building block abstraction to manage complexity. Moreover, if the different LoD align on the same framework, their collaboration will be improved.

Finally, the above-mentioned steps enable systematic mitigation of architectural weaknesses in the security domain, the development of security services, support for day-to-day security operations, and reasonable assurance that, when designing a target architecture, negative consequences will be kept to an acceptable level by risk optimisation while maximising business value. In other words, reaching a target secured architecture. ●

1 LoD, cf. The Institute of Internal Auditors

7 DELIVERABLES FROM THE ENTERPRISE SECURITY ARCHITECT

What can be expected of the ES Architect? Deliverables can vary from large enterprises to smaller enterprises. However, generally speaking, the following deliverables can be considered as being part of an ES Architect role:

1

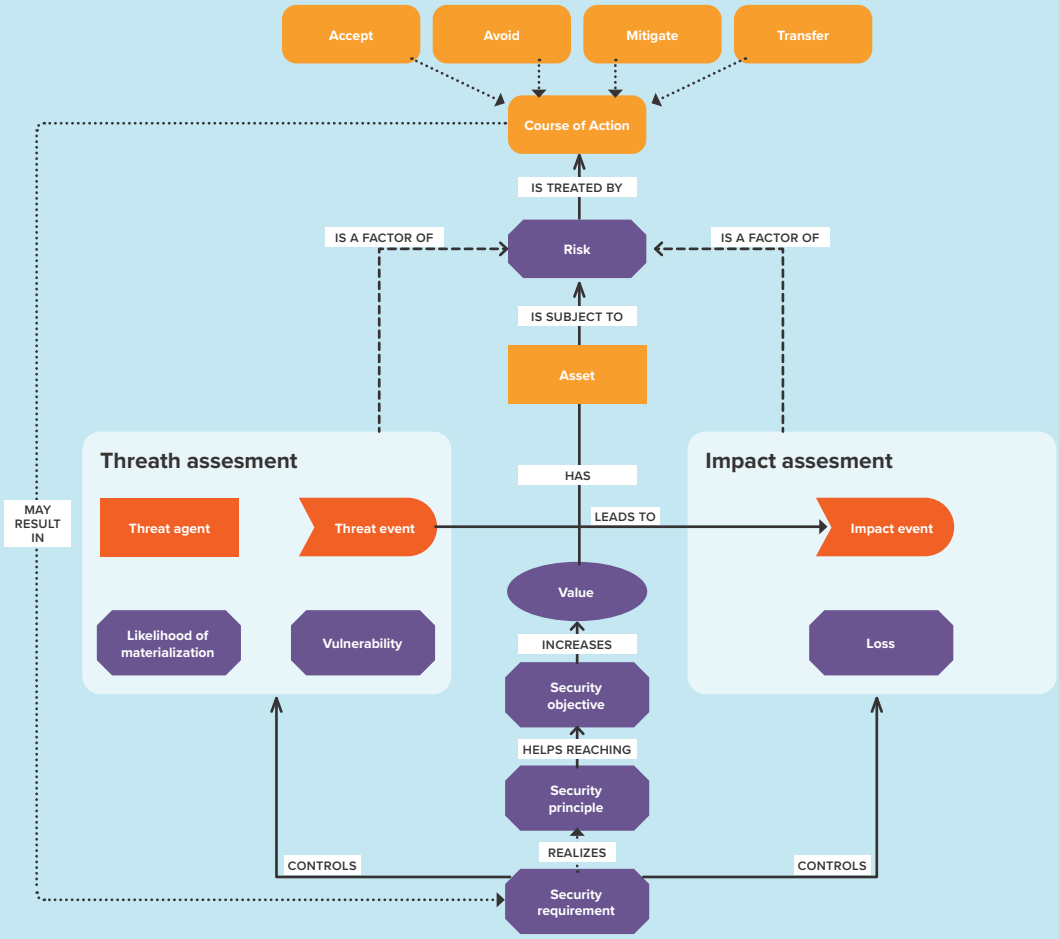
The security architecture process that enables the enterprise to develop and implement security solutions and capabilities that are clearly aligned with business, technology and threat drivers.

2

Models and views to support

a the assessment of the current state of compliance with strategy and policy.

b the future state with regards to security capabilities in-line with business goals.



3

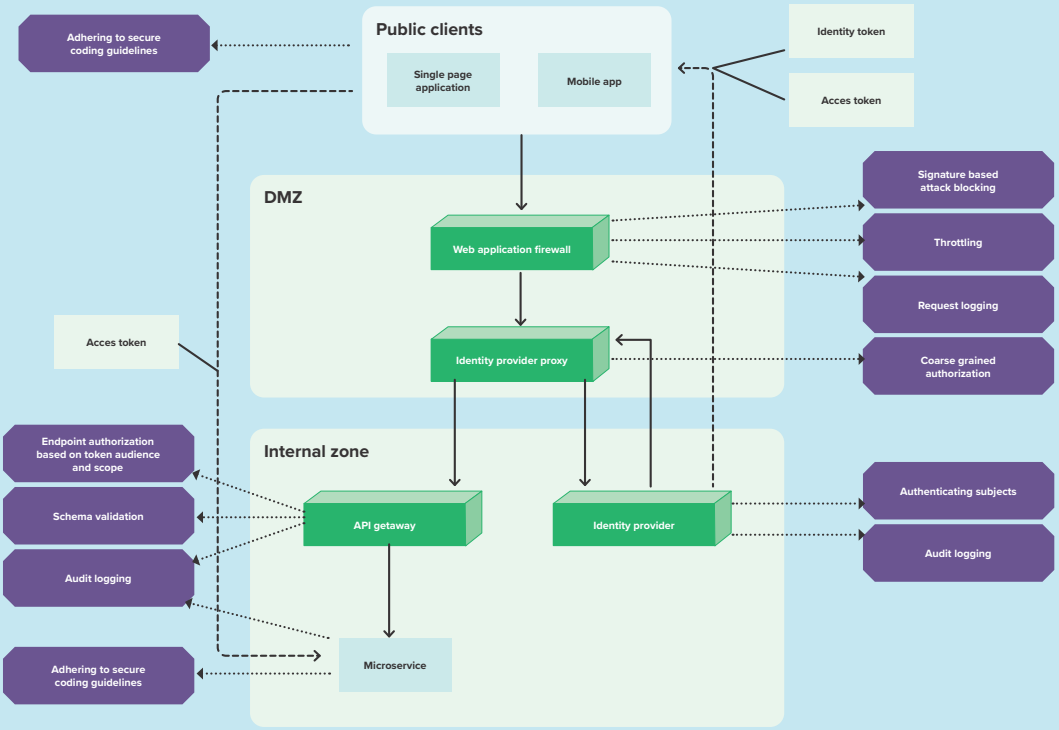
Security requirements that meet the enterprise business strategy.

4

Security principles, control objectives & measures, baseline configuration standards for all components such as operating systems, network, database, application and security solutions.

5

Security architecture artifacts (models, rules, documentation, templates etc) describe a system, a solution, or state of security of the enterprise and are used to express an architecture and document the architecture views and models that can be used to leverage security capabilities in projects and processes.



6

An analysis of the possible security threats and vulnerabilities and an evaluation of the corresponding risks (impact).

7

A review of the security technologies, tools and services, **and recommendations** to the broader security team for their use, based on strategic, financial and operational metrics.

8

Security standards and practices, such as data encryption and tokenisation based on the organisation's data classification criteria, identity and access management, trust management, application security, etc.

9

Secure reference architectures, security best practices and recommendations for changes to enhance security and reduce risk where applicable.

10

Assessments and recommendations for third-party solutions, services and security maturity.

11

A security framework for all development teams (including DevSecOps) to advocate secure coding practices.

12

Security planning advice
for application and infrastructure projects.

13

Threat models
that systematically identify the security weaknesses in the overall application and infrastructure architecture, to avoid misuse of the systems.

14

Evaluation of the enterprise security architecture maturity
(self-assessment, continuous evaluation).

15

An ESA dashboard with key risk indicators, legal and regulatory compliance reporting, level of training finished by relevant stakeholders, etc.

8 ABOUT THE TEAM

This paper is the effort of a team with diverse expertise, and has been produced to the best of their abilities:

- Benoît Moreau, Enterprise Architect IT Risk & Security, ING
- Frank Souffriau, Enterprise Security Architect, INNOCOM
- Peter Spiegeleer, Enterprise Security Architect, Proximus
- Pascal Mathieu, Head of CoE, Application Security, Security Architecture & Cyber Defence, BNP Paribas Fortis

With the support of a team of reviewers:

- Alain De Maght, CISO, Hôpitaux Iris Sud
- Benjamin Geens, Agile Coach, INNOCOM
- Benoit Delfosse, Enterprise Security Architect, INNOCOM
- Marc Vael, CISO, Esko and President, SAI.BE
- Michael Boeynaems, Enterprise Security Architect, Splynter
- Alexandre Pluvinage, ING
- Christian Mathijs and Cathy Suykens, Cyber Security Coalition
- Björn Crul and Anse Keisse, The Content Company

9 APPENDIX

Relevant books and guides

This list is a selection of relevant security architecture books that can provide more in-depth information (ordered from newest to oldest publication date).

1. "One approach to enterprise security architecture", *SANS 2021*
2. "Enterprise Architecture Reference Guide", *Cloud Security Alliance, 2021*
3. "The Azure Cloud Native Architecture Mapbook", *Stéphane Eyskens and Ed Price, 2021*
4. "SP800-207 Zero trust architecture", *NIST, 2020*
5. "Secrets of a Cyber Security Architect", *Schoenfield, 2020*
6. "Agile Secure Software Lifecycle Management- Secure by Agile Design", *ISACA Nederland, 2019*
7. "Security by Design", *Masys, 2018*
8. "Advanced Persistent Security", *Ira Winkler & AT Gomes, 2017*
9. "The Need for new IT Sec Architecture-Global Study on the risk of outdated technologies", *Ponemon, 2017*
10. "Enterprise Security Architecture-A Top Down Approach", *ISACA, 2017*
11. "Exploring Security in software architecture and design", *Felderer & Scandariato, 2015*
12. "Securing systems : applied security architecture and threat models", *Ransome, James F.; Schoenfield, Brook S. E.; Stewart, John N, 2015*
13. "Designing Secure Enterprise Architecture", *Deloitte, 2014*
14. "Designing an adaptive security architecture", *SUN, 2008*
15. "Enterprise security architecture: a business-driven approach", *John Sherwood & Andrew Clark & David Lynas, 2005*
16. Chess and the Art of Enterprise Architecture, *R&A Enterprise Architecture (rna.nl)*

Relevant websites

We have assembled a selection of the most relevant and neutral security architecture websites offering (free) available information that can serve as additional inspiration for developing the ESA in your organisation.

- en.wikipedia.org/wiki/Enterprise_information_security_architecture
- sabsa.org
- www.opensecurityarchitecture.org/cms/index.php
- cloudsecurityalliance.org/artifacts/enterprise-architecture-reference-guide-v2

For guidance on methods, follow these links:

- The TOGAF® Standard, Version 9.2 (opengroup.org)
- The SABSA Institute - Enterprise Security Architecture
- Open Security Architecture
- IB Patronen PvIB 1.0_11 jan 2013 definitief (noraonline.nl)
- ArchiMate 3.1 Specification (opengroup.org)
- Archi – Open Source ArchiMate Modelling (archimatetool.com)
- Architecture Maturity Models (opengroup.org)
- Building Security In Maturity Model | BSIMM

For risk guidance, follow these links:

- Information Risk Assessment Methodology 2 (IRAM2) - Information Security Forum
- Quantitative Information Risk Management | The FAIR Institute
- Threat Taxonomy — ENISA (europa.eu)
- CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC™) (mitre.org)
- Threat Modeling: Designing for Security (threatmodelingbook.com)
- Microsoft Word - Threat-Driven Approach whitepaper v3.03a.docx (lockheedmartin.com)

For control guidance, follow these links:

- Standard of Good Practice for Information Security 2020 - Information Security Forum
- Cybersecurity Framework | NIST
- SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
- CIS Controls (cisecurity.org)
- CSA (cloudsecurityalliance.org)
- Defendable Architectures (lockheedmartin.com)

This whitepaper is a creation of the content company, commissioned by the Cyber Security Coalition.
Editor-in-Chief: Cathy Suykens | Photography: iStock, Adobe Stock | Design: Anaïs Hoornaert

Cyber Security Coalition
Stuiversstraat 8, 1000 Brussels

info@cybersecuritycoalition.be
www.cybersecuritycoalition.be