Security architecture development over 20 years.

Do we see progression and is it mature enough?

Author: Ing. Renato Kuiper CISSP CISA SCF SCPR

Introduction

The goal of this article is to give an overview of developments in the last 20 years of designing security architectures. We start by looking what security experts stated in 2005 and how this profession (Security architecture design) developed through time. It gives some examples of changes and a outlook for the future. Readers can use this article when they want to become familiar with security architectures.

The PvIB (Platform for Information Security[1]) wrote two expert letters in 2005 and 2006 on security principles [1] and security architecture [2]. At the time, it was assumed that security would become an integral subject of architecture and that the subject of security would become an integral part of the training program for architects. Now, almost 20 years later, we see that this is "unfortunately" not yet the case. I have seen a lot of architectures designed with functionality in mind and less with the non-functionals like security. One of the main reason is that critics often say: “Security architecture is too expensive and it hinders the agility activities of the organisation”[2]).

A limited number of security architecture frameworks existed in 2005 and 2006. The best known of these are: SABSA [3], OSA (Open Security Architecture) [4] and security as part of TOGAF (The Open Architecture Framework) [5].

When we look to a security architecture, the security architecture is built upon a framework with artifacts, it has users that needs the security functionality. The security architect is design by a security architect, and he/she uses, just like other architectures, artifacts like principles, patterns, and layers of content. New security strategies like Zero Trust and SASE are added into the security architecture.

Let's see how these topics have developed over the years:

- architectural frameworks;
- security principles;
- client role;
- security architecture framework and methods;
- security architect;
- patterns;
- content of the security architecture.
- Zero Trust Architecture

[1] PvIB: Platform voor Informatiebeveiliging, www.pvib.nl

[2] Quote from: Source: Gartner A Guidance Framework for Establishing Youre Approach to Security Architecture, January 7, 2021, ID G00385515.

- SASE (Secure Access Service Edge)3
- Outlook

Architecture frameworks

TOGAF and DYA are the most famous/ popular architecture frameworks used in the Netherlands. TOGAF defines security as a technical artifact in its framework. DYA calls it a quality aspect in architecture, but never addressed it. A positive development was evident in 2011. Integration of SABSA (Sherwood Applied Business Security Architecture) into TOGAF (about which more later) was taken up as a joint initiative by the Open Group and the SABSA Institute and is/was described in a white paper [5] of the Open Group. In this white paper, the SABSA artefacts were described and indicated where they could be in the ADM of TOGAF, as shown in Figure 1. At the time, the security architects believed that security - in the SABSA manner - would be fully integrated into the TOGAF (9.1 release in the TOGAF) framework (and method). Now, 8 years later, we know this is still not the case. In other words, security still does not have a place in architectural methods that we as a security community consider necessary. This is a development that I unfortunately expected more, so that is not yet a good development for our security field.

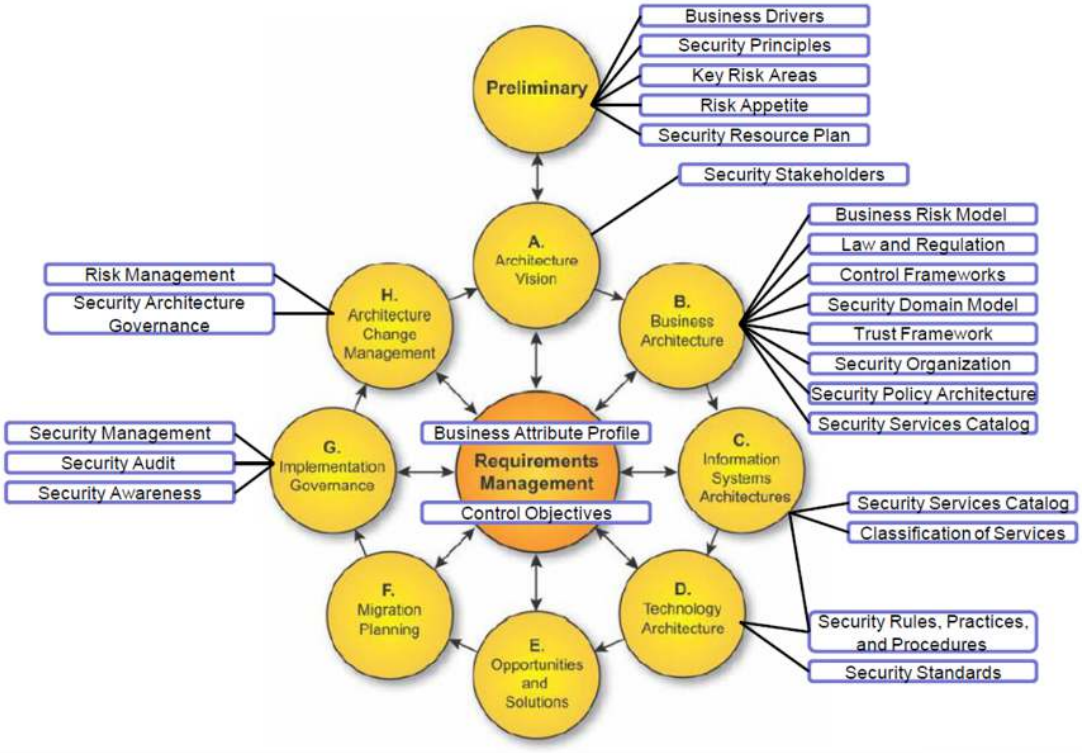


Figure 1: Integration TOGAF and SABSA.

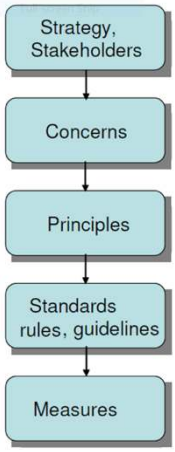
Source: TOGAF® and SABSA® Integration, How SABSA and TOGAF complement each other to create better architectures, October 2011, Open Group.

[3] https://en.wikipedia.org/wiki/Secure_access_service_edge

Security principles

Security principles have been around for a long time. In the period of the expert letters, the focus was on 'General accepted information security principles' (GAISP) [6]. These principles were recognizable to architects and applicable to architectures. What these principles lacked were well-founded rationales, based on concerns and of course the impact of the principle "what should be done for this?", as shown in Figure 2.

Figure 2: From concerns to measurements. Measurements or Measures?



Even now, we come across security principles in architectures without proper justification for why and what impact it has, to implement these principles. Security organizations such as ISF (Information Security Forum) [4], ISC2(International Information System Security Certification Consortium)[5] and ISACA (EDP Auditors Association)[6] have joined forces and have considered the subject of security principles. In 2010 they formulated a set of 12 security principles [7] that were recognizable and negotiable at a higher management level. Three important areas of attention have been formulated: "Protect the business", "Support the business" and "Create a security culture" (see Figure 3). These principles help to draw up the business-driven security principles, whereby the mandatory "it must be because of risks" actually looks at "how the business is supported to achieve its objectives." These principles also need to consider which problem they are now solving. The impact must still be determined by the organisation.

Benefit	Principles
Support the business	• Integrate information security into essential business activities. • Derive value from information security, helping to meet business requirements. • Meet statutory obligations, stakeholder expectations and avoid civil or criminal penalties. • Support business requirements and manage information risks. • Analyze and assess emerging information security threats. • Reduce costs, improve efficiency, and enhance effectiveness.
Defend the business	• Treat risks in a consistent and effective manner. • Prevent classified information (e.g., confidential, or sensitive) being disclosed to unauthorized individuals. • Prioritize scarce information security resources by protecting those business applications where a security incident would have the greatest business impact. • Build quality, cost-effective systems upon which businesspeople can rely (e.g., that are consistently robust, accurate and reliable).

[4] https://www.securityforum.org/
[5] https:///www.isc2.org
[6] https://www.isaca.org

Promote responsible security behaviour	• Perform information security-related activities in a reliable, responsible, and effective manner. • Provide a positive security influence on the behavior of end users, reduce the likelihood of security incidents occurring, and limit their potential business impact.

Table 1: Security principles of ISF, ISC2 and ISACA.

All in all, a positive development in the field of security principles.

Client role

The client also has an important role for security in defining what it wants and directing that development. In 1997, when developing my first security architecture for the Ministry of Finance, the following assignment was given once: develop a (security) architecture. The architects started working on this at the time and developed a security architecture based on a supplier's idea. By this I mean: the architects formulated the security architecture and security building blocks that they thought were good for the organization. Security building block re security artifacts like security processes like Vulnerability management, security technology like cryptographic PKI services and security organisation like the defined roles and responsibilities to maintain the security within the organisation. This ignored the business case for security, which simply did not exist. Security building blocks are made to solve a possible problem, without the client being asked what problem should be solved. Currently, the security architecture is being developed much more to give substance to the groups of the client(s). The client has taken up his role and the organizations are actually being challenged because of the security risks that are present. This is therefore a good positive development from a security perspective.

Security architecture Frameworks

Security architecture framework Architecture frameworks for security have also existed for over 20 years. The most important of these are SABSA and OSA at the international level and PvIB patterns at the local level (the Netherlands). These PvIB security patterns have become part of the NORA (Nederlandse Overheid Referentie Architectuur- Dutch Governmental reference Architecture). At SABSA it is indicated from a risk-driven approach (from the business) what is important. This is then translated into governance aspects, security processes and security services that must be realized. SABSA is a "heavy" method for the development of a security architecture. It is seen as complex in the market. Perhaps the most important reason is that the architect is struggling to determine which parts are now important and that a full SABSA life cycle is too complex, and an iteration is too much, meaning that the creation of the first iteration of a SABSA methodology requires a long timeframe and much effort. This is comparable to ITIL. The first ITIL implementations immediately picked up all IT management processes, while the intention was to tailor it to the organization. I think it would be desirable for SABSA to develop a light version that is more accessible and faster to use. OSA is not a security architecture, but a collection of patterns.

Patterns

A pattern is a generic solution that has been proven to be implemented, based on a known security problem. As a (security) architect you therefore have guidance on how to build solutions, which still applies: what problem do you solve? OSA is shown in Figure 4.

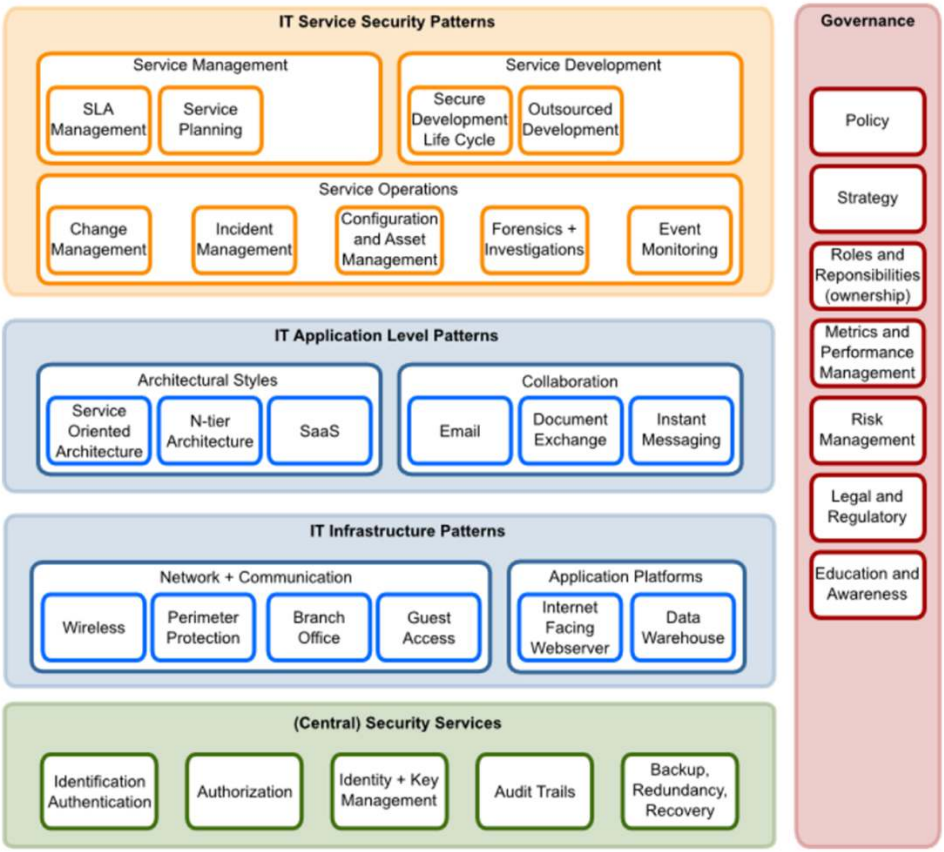


Figure 4: OSA Pattern landscape. Source: http://www.opensecurityarchitecture.org/cms/foundations/osa-landscape

The PvIB security patterns [8] were developed in the period 2011-2013 by a group of security architects. A set of patterns has also been drawn up based on experience and proven field of application. These patterns have even been given a place in the 'Operational guide' of the BIR: Baseline Information Security Rijksdienst[9]. These patterns still have a right to exist but do require adjustments to better support the latest technical developments. I myself have worked on the PvIB patterns for two years and it is time for a new generation to update the PvIB work. Because frameworks such as SABSA are very heavy, you increasingly see the development of security architectures based on your own 'experience methods'. Cherry picking is done from methods such as SABSA, OSA and PvIB patterns. All in all, this part has not yet been sufficiently elaborated in the field in easily applicable models, so work to be done.

Security architect

When the expert letter "Security principles" was drawn up in 2005, the discussion arose: is a security architect a necessary function? At the time, the expert group said: the security architect as a function still exists for 5 years, during which period the architects in training will integrate the subject of security integrally, from a business point of view (risk management and compliance

requirements). Now, almost 15 years later, this is still not the case. Architecture courses do name security, but they do not work it out enough. The architecture field has now also recognized that the security architect is a special function with a right to exist. Education is gradually coming up on the agenda, both at HBO and WO level [10] [11]. I have fulfilled the role of security architect for 20 years and I have also taught in this for over 7 years. The biggest risk now is that security is still seen as a separate part of the architecture and not yet an integral part. The vacancies for security architect in the Netherlands cannot be filled with the existing architects. It is a good career path to become a security architect, it has enough challenges for the coming years.

Security architecture content

The content of the security architecture has changed significantly. In the period 2000-2010, the security architecture, especially security functions, mainly contained technical oriented elements (with the supporting processes as shown in Figure 5).

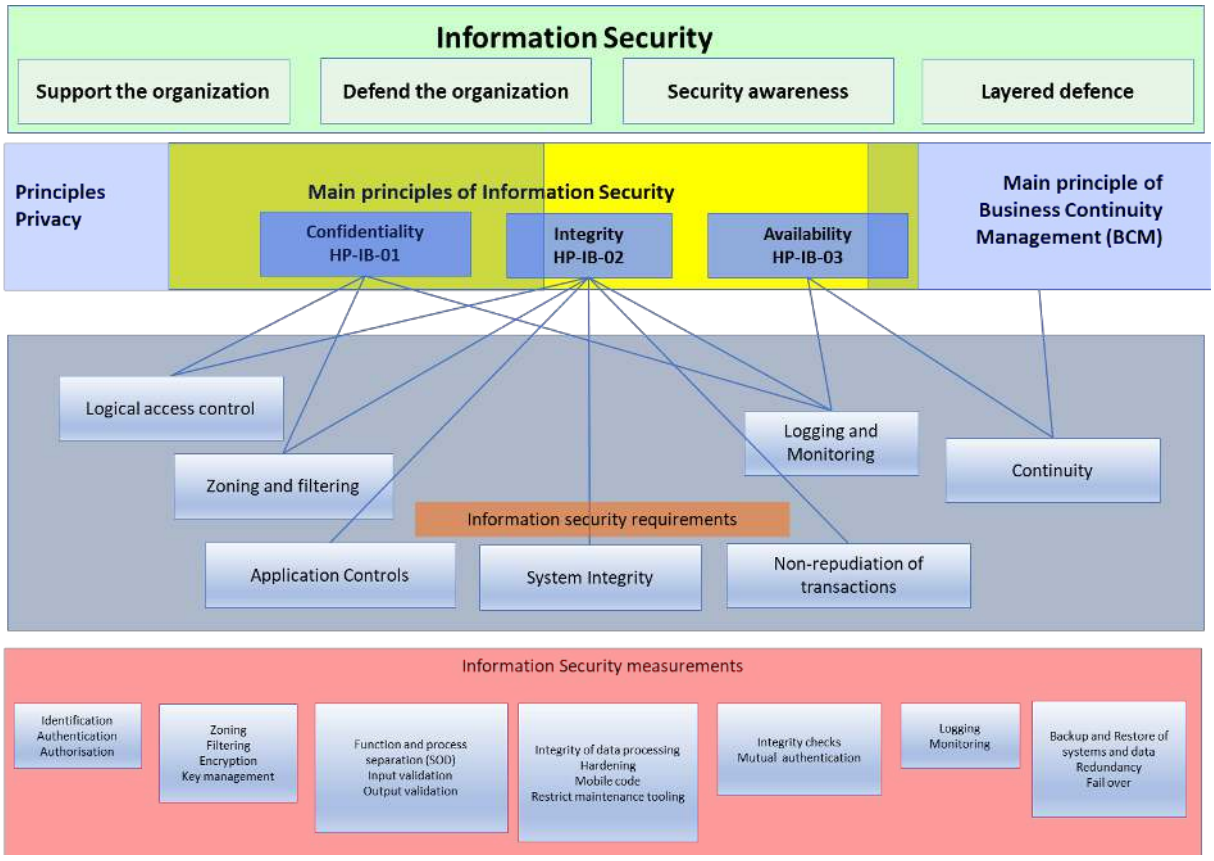


Figure 5: Security functions on basis of CIA-classification.

The picture shows that information security has four main areas of interest:

- Support the organisation: security should be an enabler to achieve the business goals.
- Defend the organisation: manage the security risk within the risk appetite of the organisation.
- Security awareness: create a culture that security is helping the business and make people aware of their roles and responsibilities.

- Layered Defence: apply security in different layers (technology, physical, organisational, processes), so the security cannot be broken by circumvention just one security measure.

Security will focus on confidentiality, integrity, and availability (CIA) of data and information systems. Confidentiality and integrity of data is also a privacy topic. Availability is also a business continuity topic. That's why a security architecture will cover security, parts of privacy and business continuity.

These quality aspects of information expressed with the CIA trade can be protected using security functions or capabilities and are expressed in Information Security Requirements. Examples of well-known security functions are: Logical Access Control, Security Monitoring and Zoning and filtering. An example of a security function for Logical Access Control can be: information classified as "Internal" shall use an RBAC (Role Base Access Control) mechanism based on group membership. Information classified as "Concern Confidential" shall use an RBAC and a ABAC (Attribute Based Access Control) mechanism based on a combination of: Location (within Europe), Time, (between working hours) and Device (company managed device).

These security functions are a functional description of the requirements, the security measures under it are the security measures to be implemented into the organisation environment. This can

Security functions and the resulting measures are taken, based on only the CIA classification. This does not explicitly look at the risks and the environment in which the data is located. In modern security architectures, you see parts in the contextual and conceptual layer describing the context of the organisation, applicable laws, the business goals that should be supported by security, the threat profile of the organisation. This information is not defined by the security architecture but come from the business, legal and risk department. Based on these topics, the security architect will in cooperation with the business define the conceptual layer containing the security vison, the principles, and the security strategies.

In modern security architectures, the various architectural layers are supported with risk management and security aspects. An example of this is shown in Figure 6.

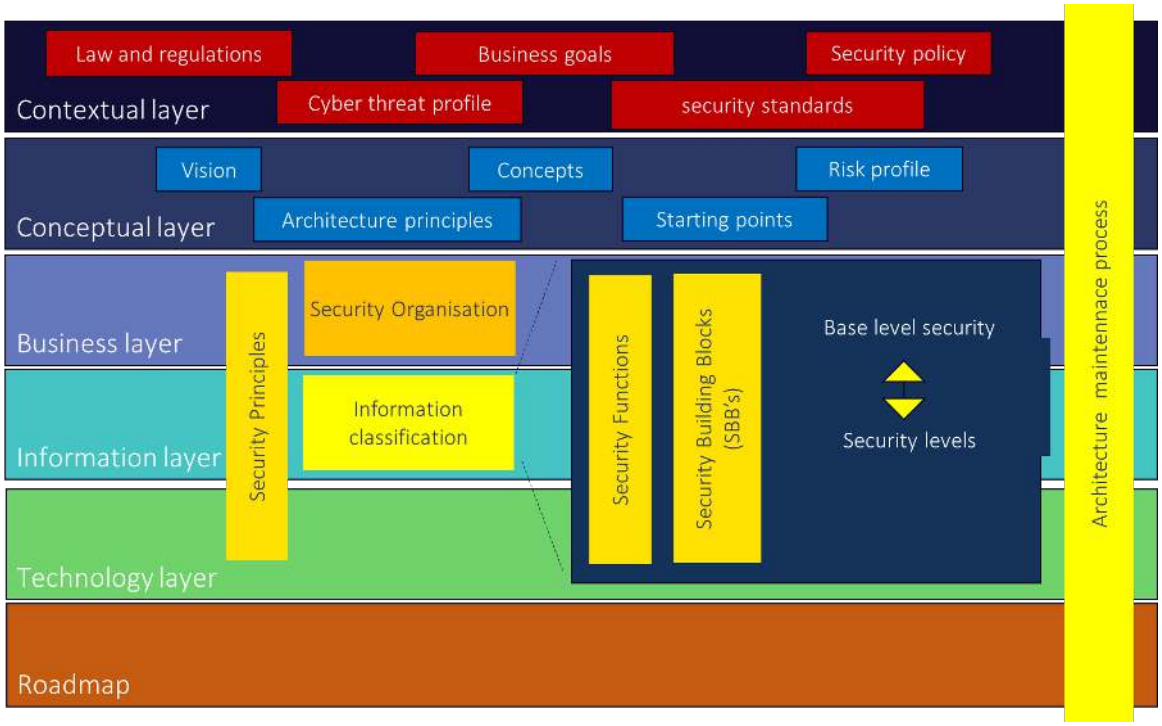


Figure 6: Content of a practical security architecture framework.

In these security architectures, you see parts in the contextual and conceptual layer that are usually not part of the architecture. Laws and regulations are a given, input comes from legal (legal affairs) and compliance is for the architect. A cyber threat assessment is input from the business with the CISO (Corporate/ Chief Information Security Officer), the information security policy is input from the CISO. The business objectives are input from the business, which must be embedded in the "Enterprise Architecture" (and thus become input from the security architecture). We now see the security functions shown in Figure 6 reflected in modern architecture, positioned vertically over the BIT layers. In the period 2000-2010, security functions with a preventive character were designed.

We now know better, we cannot protect everything and that is why we see more and more security functions besides preventive measures, including detecting, responding, and recovering measures.

These functions and processes are elaborated in the NIST CSF[7]: Cyber Security framework [12], of which Figure 6 gives an interpretation of the various security functions. Security is given a clear place in this framework.

[7] NIST CSF: National Institute of Standards and Technology, Cyber Security Framework, https://www.nist.gov/cyberframework

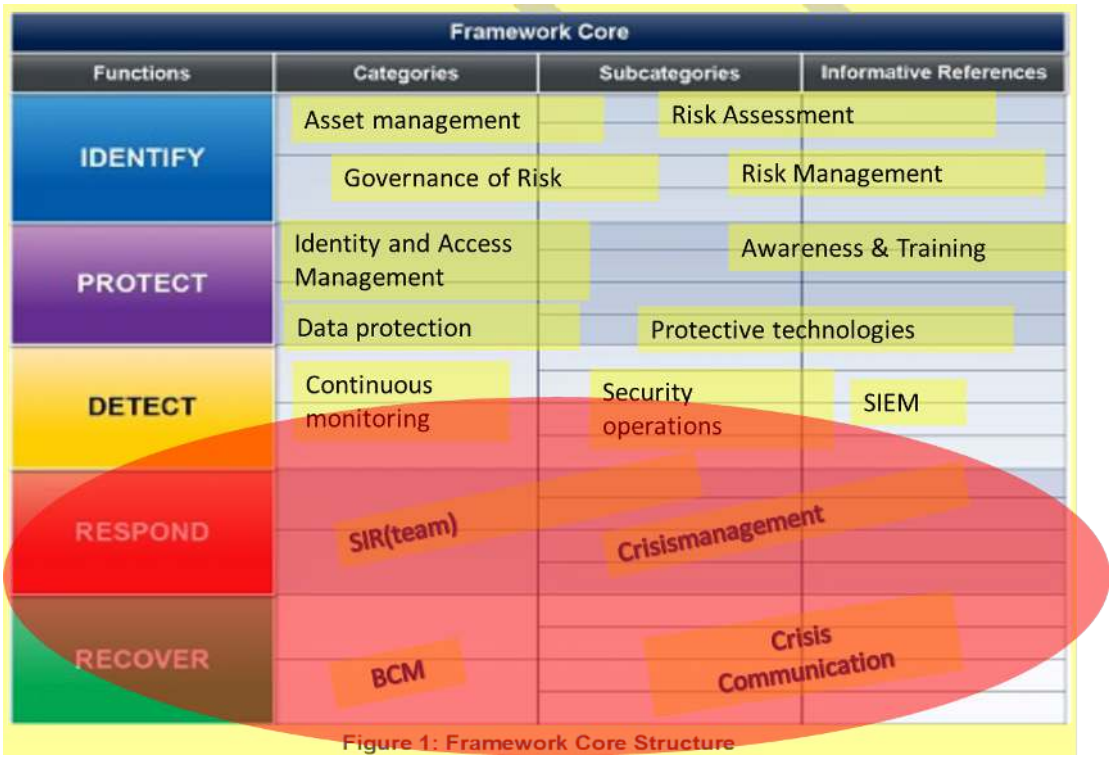


Figure 7: NIST CSF- Cyber Security Framework.

The NIST CSF is a collection of security requirement based on international standards and best-practices in the market. It contains 5 functions: Identity, Protect, Detect, Respond and Recover. Each function is supported by categories and subcategories contains security requirements. For example: in the Identify function, security measures are described for conducting a Risk assessment as part of the risk management process. In the Protect function, security measures are taken for access control (IAM) and firewalls and cryptography (protective technology). In the Detect function, security capabilities for detecting attacks and unusual behaviour of information systems are described using intrusion detection and Security monitoring capabilities. The Respond function contains security requirements for when things get out of hand (Crisis management, security incident response team). When information systemin are broken or damaged, the Recover function described capabilities for business continuity management (BCM) and the way is can be communicated to stakeholders (Crisis Communication).

Architects usually use a tool that can be used to model a security architecture, using Archimate (reference), for example. Archimate can be used to model security and risks, the subject of security is also secured across all architectural layers. An example of a modelling is shown in Figure 8.

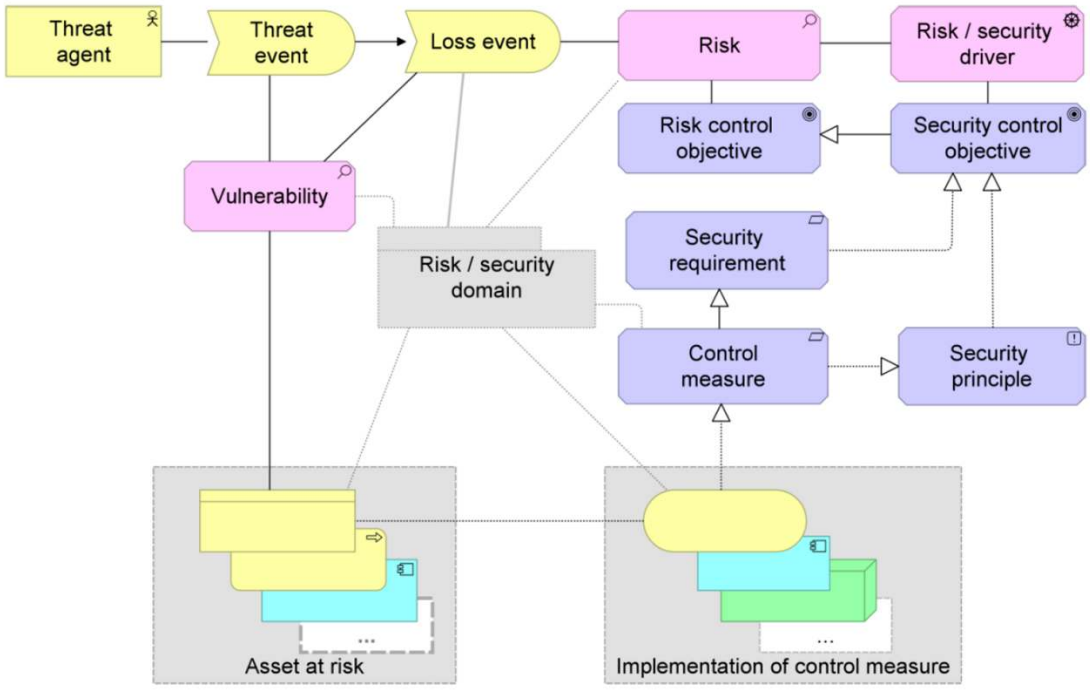


Figure 8: Security- and risk modelled in Archimate, source: HOW TO MODEL ENTERPRISE RISK MANAGEMENT AND SECURITY WITH THE ARCHIMATE® LANGUAGE, document number W172.

Zero Trust Architecture

The previous mentioned security architecture models look mainly to security processes and technology which have been used for a long period. With the rise of cloud adoption and grow of BYOD (Bring Your Own Device) devices information can be everywhere, and devices are not controlled anymore by the organization. This led to a new way approach by Forrester (reference), the ZTA (Zero Trust Architecture). In that model the main starting point was: “Trust nothing, Verify everything”. This means, in short version, verify the user, verify the device, and verify the application. Authenticate users, devices, and applications. Access to objects is based on a security policy, all communication is encrypted, and actions are logged.

This ZTA security model, still needs all the mentioned security functions which we used in the past, only these security functions, Identification, Authentication, Authorization will be used more frequently and more granular. Within the ZTA-model, there is a control plan where the business rules are defined and maintained, and a data plane where the important data resides. A plane is a collection of ICT components. Discussions already started about the missing of the monitoring plane, with artefacts like data classification, information flow mapping, Threat detection, SIEM (Security Incident and Event Monitoring) and SOC (Security Operations Centre) functionality. More can be found in the paper: “Zero Trust: What You Need to Know to Secure Your Data and Networks” [13].

SASE: secure access service edge

Organizations are thinking about implementing ZTA (Zero Trust Architecture). Before organization have done that, Gartner already defined a new model: SASE: Secure Access Service Edge. This model can be seen as a convergence of “Network as a Service” and “Network Security as a Service”.

- Network as a service, containing Software Defined WAN, CDN (Content Delivery Networks and network services to deliver high quality bandwidth).
- Network Security as a Service containing (Firewall as a Service, DNS(sec)[8], CASB[9] (Cloud Security Access Broker), Cloud SWG(Secure Web Gate Way), ZTA (Zero Trust Network Access) and Network security and WAAPaaS (Web Application and API Protection as a Service).

So, SASE will be a combination of delivering network quality of service with security functionality added to it like Zero Trust. This SASE concept looks promising, but I have not seen any customers using it at this time. More details of SASE can be found in the Gartner publication: The Future of Network Security is in the Cloud [14].

Outlook

The profession for security architectures and the security architect will evolve in time. During the 15-year period, quite a lot has already happened to give security a place in architecture. However, the integrated approach to security as part of the enterprise architecture is by no means commonplace. The role of the security architect is becoming increasingly important. Security has been introduced as a subject in architecture lectures. It would be nice if the Open Group again puts effort into the integration of security in TOGAF. Perhaps the integration whitepaper TOGAF and SABSA was too large and complex, the need still exists. All in all, about the various aspects discussed, I think we have made good steps, but we are certainly not there yet. Developments like Zero Trust Architecture will help us to grow in our profession.

References

[1] GvIB Expert letter - Security Principles: Information security on the management agenda, ISSN 1872-4884, Volume 1 – No. 3, September 2006.

[2] GvIB Expert letter: Security architecture: a new hype for specialists, or a useful means of communication? ISSN 1872-4876, Volume 2 – No. 1, June 2009.

[3] SABSA: https://sabsa.org/

[4] OSA: http://www.opensecurityarchitecture.org/cms/index.php

[8] DSN: Domain Name Service, the capability to find an IP address belonging to a URL.
[9] CASB is a cloud security capability to fulfill different security functions like Identity and Access management, encryption of data, logging and monitoring of traffic and content.

[5] TOGAF® and SABSA® Integration, How SABSA and TOGAF complement each other to create better architectures, october2011, Opengroup, https://sabsa.org/sabsa-togaf-integration-white-paperdownload-request/

[6] GAISP: http://www.gaisp.org/

[7] Principles for Information Security Practitioners Principles for Information Security Practitioners, http://www.isaca.org/KnowledgeCenter/BMIS/Pages/Security-Principles.aspx

[8] PvIB security patterns: https://www.pvib.nl/kenniscentrum/documenten/201301-ib-patronen

[9] BIR Operationele Handreiking: https://www.earonline.nl/images/earpub/5/5c/BIR_Operationele_Handreiking_v1_0.pdf

[10] Security architecture and SABSA, Den Hague University of Applied Sciences, http://www.hhs.nl.

[11] Security in architecture, Executive Master Cybersecurity, http://www.csacademy.nl

[12] NIST Cyber security framework, version 1.1, April 2018, https://www.nist.gov/cyberframework/framework

[13] Zero Trust: What You Need to Know to Secure Your Data and Networks, SANS publication, Dave Shackleford, March 2020, https://www.sans.org/webcasts/zero-trust-to-secure-data-networks-113050

[14] The Future of Network Security Is in the Cloud, Gartner, ID G00441737, Neil MacDonald, Lawrence Orans, Joe Skorupa, 30 August 2019.

About the author

Renato Kuiper is Principal consultant cyber security, working at Capgemini and has more than 20 years of experience in developing security architecture. He was a guest lecture at the Executive Master Cyber Security of the University of Leiden, The Netherlands.