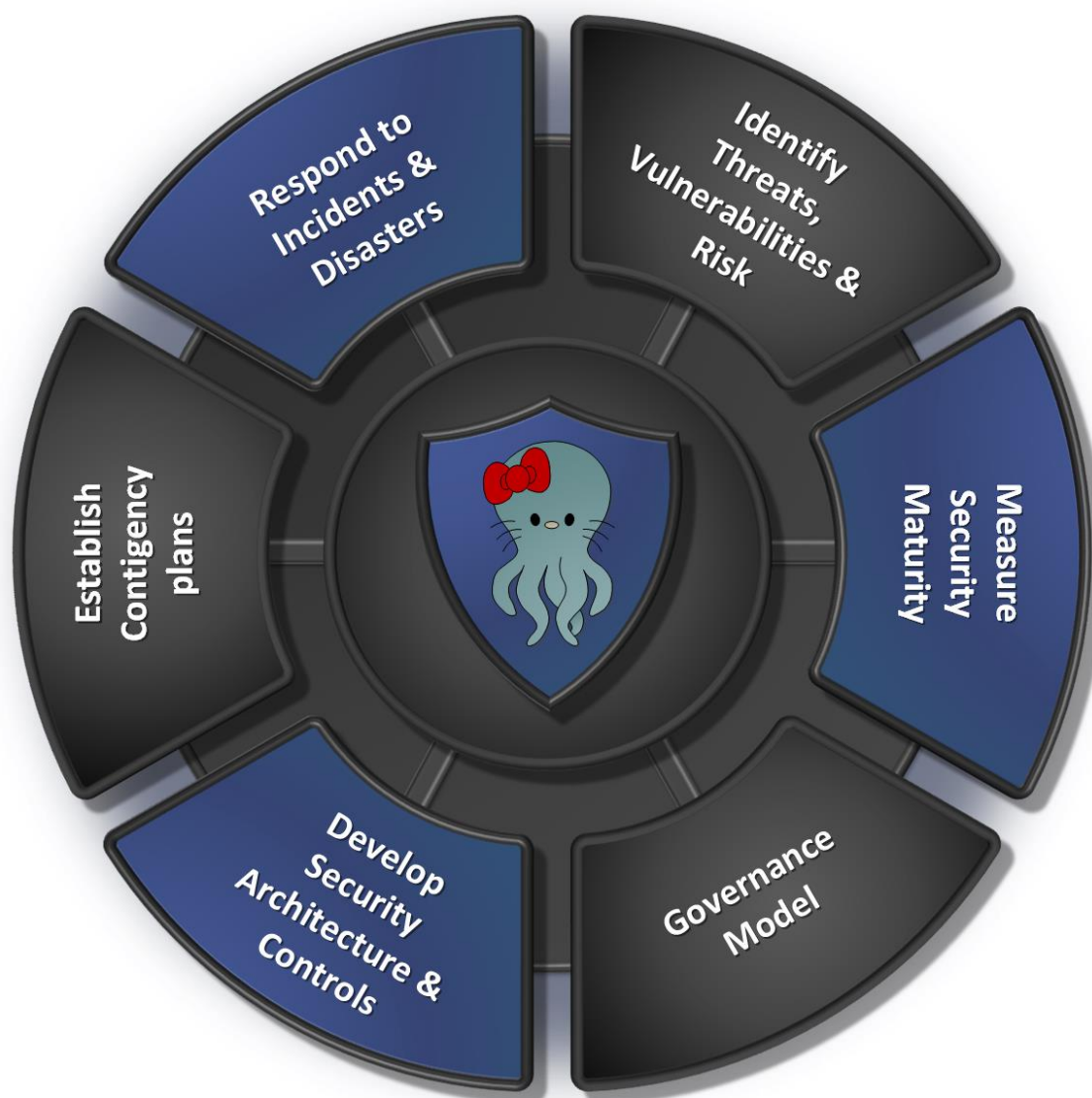


Defendable Architecture Guideline



Developing, implementing and measuring an effective security strategy & architecture

DAG-2020-001

Document Author: [Erik Kvarvåg](#)

About the Author



As an IT professional devoted to technology Erik provide more than 25 years of experience with the majority of time in key roles ranging from IT system administrator to network operations engineer and chief infrastructure & security architect.

Having spent most of his career within the telecom industry, Erik have seen technology evolve from dial-up modems into fiber access and 5G mobile networks. Always ready to dive into new technology or infrastructure areas to learn more about them but have in later years focused more on security related topics, both within the technology space as well as information security.

As Chief Cloud Infrastructure & Security Architect with Telenor Group, a mobile operator focusing on Scandinavia and Asia with approx. 180 million customers¹ Erik regularly interacts with most major established as well as upcoming vendors in the IT and Telecomm industry. The development on the virtualization of telecom operator networks makes IT infrastructure, virtualization and security skills extremely also relevant in the telco space and key development and focus in later years have been on NFV and cloud native technologies for 5G usage.

Among his many accomplishments you can find:

- Author of target architectures for cloud infrastructure and IT/NFVi infrastructure security
- Design and delivery of NFVi platforms in Thailand, Malaysia, Pakistan, Bangladesh and Myanmar
- Design and delivery of IT datacenter networks in Norway, Pakistan and Malaysia
- Countless solution designs for various infrastructure projects in Telenor's business units
- Several technical whitepapers on cloud, infrastructure, security architecture and networking

Originally from Oslo, Norway, Erik decided that after spending several years on assignments in different places in Asia that friendly warm Thailand was a better place to stay than a country where half of the landmass is above the arctic circle and large parts of the year the temperature is in the range between -20C and 5C. Currently a Bangkok citizen with no intention of leaving soon greatly enjoying Thai food and developing a growing Hello Kitty obsession.

When not being glued in front of his work computer, Erik is a big fan of books and computer games, and enjoys movies to the extent that he built a complete home cinema in the basement of his house back in Norway to properly enjoy his sci-fi movie collection. Occasionally seen jogging in Benjakiti Park near Asoke.

¹ <https://www.telenor.com/about-us/telenor-at-a-glance/>

Executive Summary

A security strategy is a unified set of processes that help identify potential security risks, address vulnerabilities, and lays out a plan of action should a risk turn into an actual security threat. To create an security strategy, it's essential to map out all informational assets within an organization. Creation of the strategy also involves selecting and managing which security controls will be put into place, as well as constantly assessing and retooling those controls as the need arises.

To be effective to the organization formalizing security strategy and planning is absolutely necessary. Security must be integrated into every aspect of organization's that wants to take security seriously. This ranges from HR implementing security awareness programs to legal ensuring regulatory compliance, the IT operations teams building a secure infrastructure and implementing security controls and the Security Operations monitoring for threats. All these together, in an effort to promote and become an enabler of secure, responsible business by putting security at the foundation of everything the organizations should do.

Of the many advantages of developing a well-defined and formalized security strategy the primary one is getting other parts of and departments of the organization to join the effort by inviting them and asking them to contribute to the strategy and be part of the governance of the strategy. This gives the other part of the organization the opportunity to influence security, have their concerns addressed, and pull in the same direction being part of the solution rather than continuously being on the receiving on of the many polices, controls and perceived limitations coming from the security governance function of the organization. By promoting inclusiveness and integrating multiple aspects of business, the security function of the organization build a strong starting point of integrating security into every corner of the business.

There are several key requirements in a solid security strategy:

- Communicated and understood security mission statement
- Inclusive governance function and management anchoring
- Properly defined security objectives ,priorities and policies
- Adopted risk management framework and practices
- Developed security architecture and control blueprints
- Established plans for incidents, disasters and business continuity
- Processes for continuous assessment, development and improvement of controls

A security strategy's success depends on its implementation. Proper communication, training, and interaction between the organization's security governance unit and other different functions, and third parties is key in building the understanding of the security strategy, the supporting architecture and relevant policies so that they implemented according to the defined standards.

The successful execution of the strategy involves identifying relevant exposure in the form of threats, vulnerabilities and overall risks assessing them and prioritizing them in order to determine the most efficient implementation of security controls to mitigate them. For this purpose, development processes of security strategy and the supporting security architecture should be integrated with the information security policies and risk management functions of the organization.

To be successful, the security strategy and supporting architecture development should be continuous have defined processes in place for measurement and tracking of the effectiveness of the implemented security controls and functions that the organization have implemented in their infrastructure. Only by a constantly repeated development cycle and improvement of existing controls and removal of inefficient ones can the security maturity of the organization be developed over time and ensure that the security posture is robust enough to withstand attacks from threat actors and not disrupt the overall business.

Defendable Architecture Guideline

Developing an effective security strategy and architecture

Table of contents

1	Introduction	6
1.1	Objectives	6
1.2	Scope	6
1.3	Target audience	6
1.4	Definitions	6
2	The basics, Information Security Governance	8
2.1.1	Information security management system	8
2.1.2	Information security management system scope and split of responsibilities	9
2.1.3	Risk management framework	10
3	Setting the stage	13
3.1	Defining success factors	14
3.1.1	Business driven security strategy	14
3.1.2	Threat driven defendable security architecture	15
3.1.3	Continuous development process and measurement	16
3.1.4	Anchoring & governance	16
4	Developing the security strategy & architecture	17
4.1	Statement of sensitivity	17
4.2	Exposure	18
4.2.1	Identifying threats	18
4.2.2	Identifying Vulnerabilities	19
4.2.3	Assess Risk Exposure	19
4.3	Develop strategy & assign control framework	20
4.3.1	Control Prioritization	21
4.4	Develop architecture & security controls	22
4.4.1	CIS control to architecture mapping	25
4.4.2	Plan and structure security architecture development	27
4.4.3	Technology & Vendor strategy for security control design	28
4.5	Establish contingency plans	29
4.5.1	High availability architecture	30
4.5.2	Supporting the security incident response process	31
4.6	Planning, prioritization & building	31
4.6.1	Short time planning	31
4.6.2	Long term planning	32
4.7	Security maturity & measurement	32
4.7.1	Developing different levels of maturity	33
5	Security Governance structure	35
5.1	Security governance decision forums	35
5.2	Security governance ecosystem	37
5.2.1	Executive management and board of directors	38
5.2.2	The Joint Security Management Board	39
5.2.3	Architecture review board	40
5.2.3.1	Architecture change management	40
5.2.4	Information Security	41
5.2.5	Architecture & Planning	42
5.2.6	Operations & Maintenance	43
5.2.7	Sourcing & Procurement	43
5.2.8	Security Operations	44

Defendable Architecture Guideline

Developing an effective security strategy and architecture

5.2.9	Other non-decision making Forums	45
5.2.9.1	Architecture Forums	45
5.2.9.2	Coordination Forums	45
5.2.9.3	Vendor Management forum	45
5.3	Documentation	46
5.3.1	Information Security team	46
5.3.2	Architecture team	46
5.3.3	Operations and Maintenance	47
5.3.4	Security Operations	47
5.3.5	Sourcing and procurement	47
5.3.6	Strategic governance bodies	47
6	Definitions, Abbreviations and Legend	49
6.1	Definitions	49
6.2	Abbreviations	49
6.3	Legend	51
7	List of references	52
8	List of directional statements	53
8.1	Summarized Security Principles	53
8.2	Summarized Observations	55
9	Document history	56

Table of figures

<i>Figure 1.</i>	<i>ISO27001 Scope and Controls</i>	<i>9</i>
<i>Figure 2.</i>	<i>Risk Management Process</i>	<i>11</i>
<i>Figure 3.</i>	<i>Strategy Development and incident response processes</i>	<i>13</i>
<i>Figure 4.</i>	<i>Risk Analysis Process</i>	<i>17</i>
<i>Figure 5.</i>	<i>Security Architecture domains and areas</i>	<i>23</i>
<i>Figure 6.</i>	<i>Security Architecture Development Structure</i>	<i>27</i>
<i>Figure 7.</i>	<i>Integrated Incident, Disaster & Business Continuity Response Planning</i>	<i>29</i>
<i>Figure 8.</i>	<i>Sample implementation plan of security controls</i>	<i>32</i>
<i>Figure 9.</i>	<i>Security Maturity levels</i>	<i>33</i>
<i>Figure 10.</i>	<i>Security governance tiers and decision bodies</i>	<i>35</i>
<i>Figure 11.</i>	<i>Security governance ecosystem</i>	<i>37</i>

1 Introduction

1.1 Objectives

The purpose of this document is to highlight the steps required to create a security strategy and to define the scope of a defendable security architecture and what problems it is meant to solve within the organization.

1.2 Scope

This document covers the foundational principles and main processes related to develop a security strategy and the supporting defendable architecture framework. This guiding is intended to be useful across any organization that wants to define and implement security controls, and to measure progress and effectiveness

The target scope for this document is to provide guidance on what strategic direction within an organization is required to properly apply defendable architecture

The sum of each of the defined strategic initiatives is what makes up an organizations security posture., develop effective security controls and to respond effectively to security incidents.

1.3 Target audience

This guiding is intended to be read, understood and used by:

- Security managers
- Security architects and other architects (enterprise, system, network)
- Lead architects

To get full benefit and understanding of this document the reader need to have a good technical knowledge and understand the basics of infrastructure and information security terminology

1.4 Definitions

Security Architecture describes a structured inter-relationship between different technical and procedural solutions to support the needs of the business from security perspective.

- Security architecture need to involve people, processes and vendors
- Security architecture not only about security related elements (e.g., services, functions), but also covers inter-relationship with other technical or procedural elements
- Security architecture must support business needs

Defendable Architecture: A conceptualized security architecture framework that is utilizing a risk and threat intelligence based design process to describe a set of defined security controls based on CIS20 controls.

Confidentiality: System and data confidentiality refers to the protection of information from unauthorized, unanticipated, or unintentional disclosure. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, legal action, or injury against the organization, its employees or customers

Integrity: System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or a system or service by either intentional or accidental acts. If the loss of system or data integrity is not corrected,

Defendable Architecture Guideline

Developing an effective security strategy and architecture

continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions.

Availability: If a key system or service is unavailable to its end users or customers, the organization's overall business objectives and mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time or reputation; impeding the end users' performance of their functions in supporting the organization's mission or the customers access to the organizations offered services.

Risk: the possibility, or the potential occurrence of events or incidents that might materially harm the organization's interests.

Asset: Any form of object, physical or logical that either stores, processes, transports or in the wider context, access information related to the organizations business operations

2 The basics, Information Security Governance

The development of a security strategy and risk based and business and threat intelligence driven security architecture begins with the overarching information security and risk management governance. All further distribution of responsibilities, scope, control design methodology and methodologies rest on this foundation.

To help and guide towards information security best practices as part of the implementation of a security strategy and to implement an traceable and auditable set of policies and procedures, organizations makes use of defined frameworks for systematically managing their security. There are options from [ISO](#), [NIST](#) or [CIS](#) available, each with their different strengths which makes them suitable for at different levels of security governance in the organization.

While the NIST cyber security framework provides the overall strategy framework for implementing security and CIS20 provides a concrete scope and priority to implement technical security controls, it is not enough to cover the full scope of an organization's security requirements. People and processes needs to be addressed as well, and this is where information security management² with supporting governance and risk management comes into the picture along with ISO27000 series of documentation.

Security Principle 001-1: *The information security management system shall act as a framework for the organization security strategy and its implementation*

2.1.1 Information security management system

Every business process within an organization that is technology driven is potentially exposed to threats, either security or privacy related. While advanced technology based controls are capable of preventing or detecting attacks from threat actors the organizations must ensure that business processes, policies, and personnel behavior also minimize or mitigate these risks. . An ISMS main objective is to minimize risk and ensure business continuity by limiting the likelihood of and the business impact of a risk being triggered.

Observation 001-1: *An Information Security Management System gives the organization the ability to recognize the full range of risks that the organization or its data may encounter in a short to medium time frame and is a pre-requisite for implementing the relevant mitigating measures in the form of security controls*

The framework for an ISMS is usually focused on risk assessment and risk management, which is a structured approach to the balance between the costs of implementing controls and mitigating risk vs the cost of the business impact of the risk being triggered. While being meant to address the complete picture of an organizations business risk, this methodology is also key to designing the security controls in a business and risk driven architecture which is also the core concept of the security architecture and corresponding technology based controls that is described in detail in DA-2020-002. The overall value of a successful ISMS is based on the thoroughness of the information security risk assessment, which is key to any implementation.

The applied scope of an ISMS is typically centered around employee behavior and processes as well as technology and related data. The ISMS can be targeted towards a particular type of data which may be considered of the highest priority, such as customer data, or other regulatory protected, or it can be implemented in a more comprehensive way that become an integral part of the organizations culture and way of work.

² https://en.wikipedia.org/wiki/Information_security_management

Defendable Architecture Guideline

Developing an effective security strategy and architecture

Is with other capabilities, there are multiple risk management frameworks that can be applied, ISO 27000, NIST Risk management framework (RME) ,or COBIT to name some. ISO/IEC 27001 is widely known and provide specific requirements for creating a properly scoped and measurable information security management system. It does not mandate specific actions, but includes suggestions for documentation, internal audits, continuous improvement, and corrective and preventive action.

Security Principle 001-2: The information security management system shall be scoped based on ISO27001

2.1.2 Information security management system scope and split of responsibilities

ISO 27001 specifies the standard of an ISMS implementation and how organizations can comply with it. The standard describes what are the mandatory requirements and what an organization is required to implement to comply with it. A certified ISMS, independently audited by an approved certification body, can serve as the necessary reassurance to customers and potential clients that the organization has taken the steps required to protect their information assets from a range of identified risks.



It should be noted that each document in the ISO 27000 series is designed with a certain focus, for building the foundations of information security in the organization with the purpose of defining its framework ISO 27001 should be used. If however the target is to implement security controls ISO 27002 provides a more detailed insight into the control implementation. For risk assessment and risk treatment, ISO 27005 may be used.

As specified in the ISO 27001 standard ISMS security controls is required to span multiple domains of information security and provide a clear and solid scope for the security strategy. The ISO27001 annex A along with the more control oriented and detailed IS27002 provides the baseline scope of what is required to be implemented.

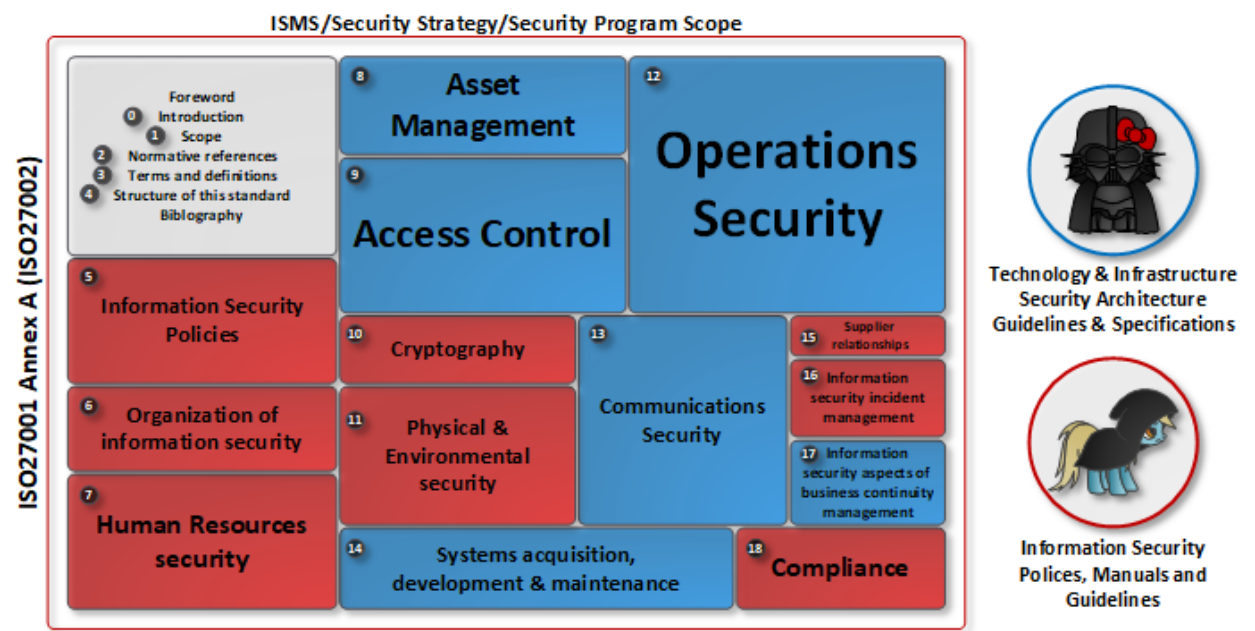


Figure 1. ISO27001 Scope and Controls

While the overall responsibility on security in the organization lies on the information security unit through the creation and governance of the ISMS, most of the design and architecture for projects, solution blueprinting etc in most major organization happens in the technology or IT division. The development of technology and infrastructure related controls can therefore be delivered through the architecture and planning unit through technology blueprints. For a separation of duties, and to address potential conflict of interest, blueprints produced by the architecture teams should be reviewed by the

Defendable Architecture Guideline

Developing an effective security strategy and architecture

information security team to verify that the design of any security controls are in correspondence with the defined policies, and manuals in the organization. This review should follow the ordinary architecture review and control processes of the architecture review board as explained in more detail under section 5 where the specialized governance functions and their relevance to the overall security governance.

While this “shift left” mindset opens up for a much needed increased bandwidth for an otherwise usually overworked security team, it requires a strong security mindset in the technology organization for this setup to work properly. If security also becomes embed in the technology organization, it can bring along a strong relation between the two units working in tandem embedding security naturally in all technology related architecture development, projects and line functions.

Observation 001-2: *Making the technology units accountable and responsible for security in all the development, project deliveries and line functions within their scope of responsibility while measuring progress, effectiveness and security maturity is an excellent catalyst and a major step in making security embedded into all aspects of the organization*

Looking at the overall scope of IS27002 and the defined controls there as shown in **Figure 1** when the scope is divided between the architecture & planning team and the information security team the need to develop manuals, policies guidelines showing how to implement in practice various controls.

The blue part of the scope is in the distributed model, the main responsibility of the technology unit, under the oversight of the information security team and is included in the “technical” security architecture. This more technology focused security architecture, often referred to as Defendable Architecture, is a framework again within the information security and ISO27001/2 scope that have been delegated to the technology organization to develop and maintain which provides a detailed description of the different types of security controls. All projects, blueprints, solutions etc should then align and integrate with the security architecture framework.

Security Principle 001-3: *Areas in the ISMS which are heavily dependent on technology related controls more than policies, should be considered to have the development of those areas delegated to the technology division under the oversight of information security governance functions*

2.1.3 Risk management framework

Risk is the possibility, the potential occurrence of events or incidents that might materially harm the organization’s interests. **Management** implies proactively, deliberately, explicitly and systematically identifying, assessing, evaluating and dealing with risks continuously.

The organization has to plan how to address the risks, threats, and opportunities. This is also greatly emphasized in ISO 27001 which focus on:

- How the risks integrate into the wider information security management system
- How actions are taken, and evaluating the effectiveness of the actions taken on the way

An audit expect to see a documented methodology that explains both these items well and to see how the ISMS operates in an integrated fashion. The organization’s assets should be linked to the risks which in turn are linked to the policies and controls being used to address them.

Defendable Architecture Guideline

Developing an effective security strategy and architecture

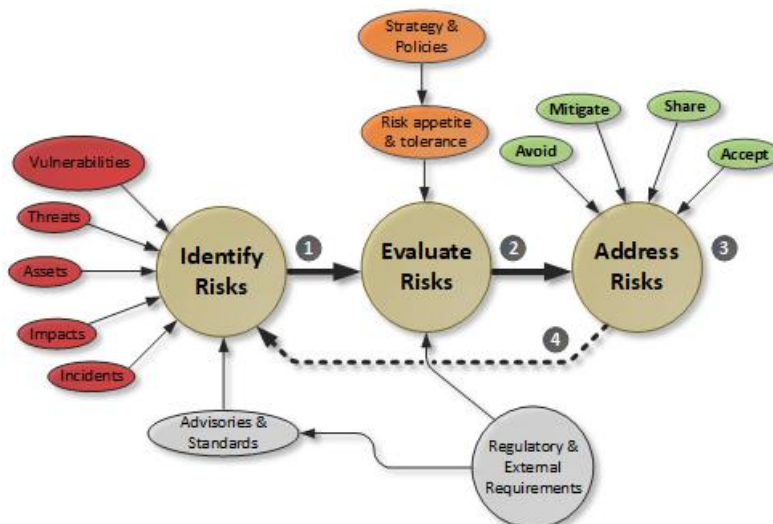


Figure 2. Defined Risk Management Process

The first step of the risk management process is to identify the relevant risks. Several input sources go into identifying the relevant risks such as:

- Vulnerabilities
 - The inherent weaknesses within technologies, , people and relationships
- Threats
 - Relevant hostile entities (insiders and outsiders) or natural events that might cause incidents
 - If triggered on vulnerabilities threats cause business impacts;
- Assets
 - Primarily information Assets that either, store, process or transport information under either regulatory scope or which is considered business sensitive. May also include HW/SW object, end user equipment or other
- Impacts
 - Negative effects or consequences as a result of incidents or disaster that affects assets and cause a degree of damaging to the organization and its business
- Incidents
 - Events that scale from minor (very low), or events of limited consequence (low to medium) up disasters (high) and catastrophes (very high)
- Advisories, standards
 - Refers to relevant documentation from either official standards organizations such as ISO/IEC, technology vendor recommendations, national cyber security defense warnings or CERT flash memo lists

The next step, which is to evaluate the risks involves processing and analyzing the information collected to determine the importance of the identified risks, the importance directly dictates the priorities for the next step in the chain. The organization's tolerance for risks needs to be clearly defined and applied at this stage. The risk tolerance levels needs to come all the way from the top and reflect the relevant business strategies

Treating risks means how to deal with them and there are several outcomes of how to address each individual risk. They can be avoided, mitigated, shared and/or accepted them. This step includes both the decision of what to do with the risks, and deciding on what to do with it, as in implementing whatever the decision which have been made.

Defendable Architecture Guideline

Developing an effective security strategy and architecture

The 4th step as illustrated in the figure above means to represent that the risk management process is continuous. As the threats, vulnerabilities and assets change, so does the risks associated with them which may change in either frequency or impact. It is thus required to continuously repeat the process.

Regulatory requirements are external to the organization, but is important input, since relevant authorities may demand that certain risks are kept at a certain tolerance level, thus impacting both prioritization and the resolution of the risk, as it may not be permissible to tolerate certain regulatory risks for instance.

The risk management process is highlighted further in DA-2020 as a key ingredient to design relevant security controls as part of the security architecture.

Defendable Architecture Guideline

Developing an effective security strategy and architecture

3 Setting the stage

A solid security strategy along with the supporting security architecture is fundamental in helping any organization to take a more holistic and not least proactive approach to security as opposed to a traditionally more reactive one which the organization only responds after an incident. After recovering from the incident (unless its an extinction type of event) security is then assessed individually based on that specific event and a limited set of gaps in the organization's security posture is addressed . From a resource perspective, a reactive approach is both time consuming as well as expensive, and potentially disastrous. Independently if the organization have an outdated strategy already enforced which needs a refresh or a new one is being developed, the security strategy work should follow a structure process.

The NIST Cyber Security Framework (CSF)³ is a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to attacks from threat actors. While the NIST CSF contains 5 main steps, Identify, Protect, Detect, Respond and Recover, which the security strategy and architecture development process also need to address and properly integrate with, to provide the organizations the capabilities and maturity required to meet those defined goals.

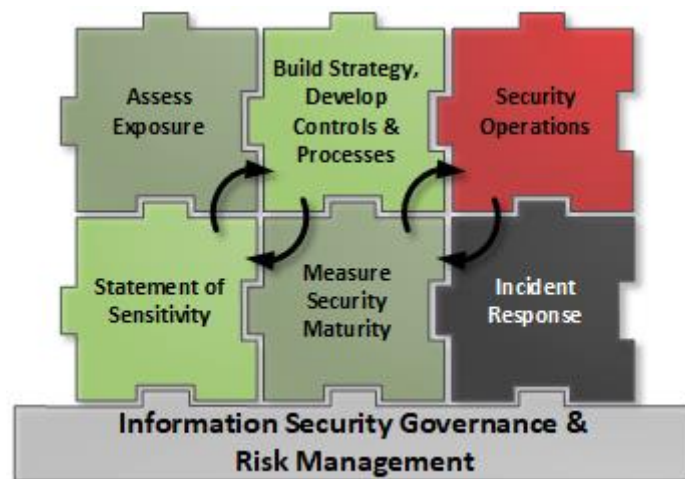


Figure 3. Strategy Development and incident response processes

On a high level there are two relevant main processes within the organization that is interlinked, the development process for the strategy and architecture and that of the security operations incident response.

The **identify**, **protect** and **detect** steps are the main focus of the development process which identifies the assets, risks and threat along with business, legal and regulatory requirements of what to address. Various protective and detection security controls and mechanisms are both defined and designed based on those requirements. This process takes place on governance and strategic level, with the input of subject matter experts across the organization and requires anchoring with senior management to be acknowledge throughout the organization. Setting target priorities, identifying gaps, creating roadmaps for implementation, budget planning etc are crucial elements of the development process.

The security operations teams then consume the relevant developed capabilities, tools and processes following the strategy direction and use them to conduct incident response in an efficient manner and

³ <https://www.nist.gov/cyberframework>

Defendable Architecture Guideline

Developing an effective security strategy and architecture

thus **respond** to any threats that are detected. The overall goal of the security strategy is to protect the organization's assets and support effective incident response.

Incident response, disaster and business continuity plans are also produced similarly with the objective to **recover** after an incident or disaster occurs.

The effectiveness of both the development and incident response processes can be measured through the **measurement** of the organization's security maturity, which across technologies, process and people areas gives a clear indication of the organizations ability to detect, respond to and recover from security incidents. Tracking the effectiveness of the implemented capabilities and processes, measuring them and seeing if they deliver on their intended targets goes into the continuous development process. Capabilities and processes that does not deliver the expected results will be revised, removed or fine-tuned to meet the targets

The fundament upon which both the strategy and security operations processes rest upon is the organization's governance and risk management functions. Both stakeholder management and understanding the appetite for risk, or the total tolerable levels risk the organization is willing to accept is key to understand before starting to develop the strategy and budgeting for the implementation of controls.

Security Principle 001-4: *The security strategy needs to be a continuous process that is able to identify all critical assets, prevent them from attack, detect threat actors attacking the assets, respond to incidents caused by threat actors or natural events and be able to recover from them*

3.1 Defining success factors

For a security strategy to be effective, it needs to deliver on some very clear objectives to be successful and prove that it supports the overall goals of the business. The strategy also needs to be realistic and not over ambitious and try to deliver beyond the capabilities and available resources of the organization.

3.1.1 Business driven security strategy



The security strategy must be business driven with the main goal of supporting the organization's business objectives and not the other way around. For this to properly work it is important to understanding threats ,risks and business impact to design the most efficient controls to mitigate the business risks. This is done by Identifying where the organization's main assets or so-called "crown jewels" and business opportunities are and then the defense strategy should be built tailored to those particular assets and business opportunities associated with them.

The gaps between as-is security posture and the defined target should be determined with a clear roadmap for closing the gaps.

The strategy should enable business opportunities by deploying vendor agnostic technologies and new partner models. This can as an example be achieved by using more cost effective equipment and suppliers of services while bringing down the associated risks to tolerable levels.

Some realism should be applied though, as implementing security controls will come with a cost in regards to resources and time for the organization, there is no silver bullet that can be applied with minimal cost while significantly keeping the organization secure, this needs to be understood and accepted across the different levels of the organization. The goal is to use the right level or resources to

Defendable Architecture Guideline

Developing an effective security strategy and architecture

reduce the accumulated business risk to the right and tolerable levels as defined by the senior management of the organization.

Security Principle 001-5: *Security strategy should be realistic and balanced between security, quality and price effectiveness and be based on a threat and risk based methodology addressing the requirements of the organization*

The defined objectives of the security strategy and supporting security architecture:



- 1) *The organization shall have a clearly defined security strategy with properly anchored and established organization wide inclusive governance*
- 2) *The Organization shall have developed, documented, implemented and maintaining a defined security architecture to protect the confidentiality, integrity and availability of its assets*
- 3) *The Organization shall continuously develop and maintain its security maturity by defining and implementing security controls and incident response capabilities as defined in the security architecture to detect and prevent unauthorized access and data theft in critical systems.*

3.1.2 Threat driven defendable security architecture

While the strategy outlines the direction and scope of security implementation, the architecture provides the framework of how to put it into practice as it supports translating business objectives into aligned (information/Infrastructure/physical) security implementation in such a fashion that it can be traced back to the original business goals. Within the architecture conceptual overview is created to support the implementation of a holistic and consistent security level, across projects and enterprise as well as from business objectives to implementation. A well-defined architecture framework reduce the possibilities for having unknown risks, weak links and design gaps while avoiding unnecessary costs related to spending more time and resources on some parts of the components without any noticeable effect or change to the cumulative level of security. Through the architecture a broader level of view and coordination on changes than a single project scope of delivery can be established, and interlinks to other security controls and functions can be established as required. When properly established a defined architecture supports cost efficient re-use and integration of security services across different solutions.

Security Architecture should address the following items to be useful and effective:

- The need to be cost effective
- Modularity
- Scalability
- Ease of component re-use
- Operability
- Usability
- Inter-operability both internally and externally
- Integration with the Enterprise Architecture and existing legacy solutions
- Defendable
- Automatable

Prioritization is a key, Investments should be focused on implementing security controls that provide the greatest reduction of risk and protection from the most likely and impacting threats and which can be implemented in a reasonable cost and time frame.

The security controls chosen to be implemented should be engineered towards supporting automation to provide greatly increased efficiency, reliably scale and continuously monitor for compliance to the defined policies that the controls are set to enforce. It should also be considered to extend the defined

Defendable Architecture Guideline

Developing an effective security strategy and architecture

controls to third-party vendors and managed services providers and their vendors by continuously monitoring third-party and fourth-party security postures to mitigate supply chain risk and exposure.

3.1.3 Continuous development process and measurement

Continuous diagnostics and mitigation: Continuously monitor the organization's security posture to test and validate the effectiveness of security controls and to help drive next steps in developing the overall security maturity of the organization.

The security strategy and security architecture needs to follow a continuous development process, collecting data on sensitivity of assets, threats, vulnerabilities and the effectiveness of implemented processes and controls. Collecting telemetry through the process is one of the most important priorities. This data and additional feedback gives the possibility to re-balance and if required, to adjust the strategy. The strategy and supporting architecture needs to be revised at regular intervals, gap analysis and action plans updated to reflect the current state.

Use the learnings from actual security incidents that have resulted in breach and compromised systems to provide the foundations to learn from and to build effective, practical security controls. Avoid the use of controls that have not been proven to stop real-world incidents.

Measurements and metrics through the use common metrics can provide a shared language between senior management, security subject matter experts, suppliers ,auditors and other employees to measure the effectiveness of security measures within your organization.

3.1.4 Anchoring & governance

Equally important to the security strategy plan is the governance surrounding it. For it to be effective, the key importance is inclusiveness of the major stakeholders in the organization. By integrating stakeholder interests through the multiple aspects of business a strong starting point can be built by integrating security into the foundations of the organization.

Setting the vision and the ideas by anchoring is the first thing that is required along with defining a "mission statement". This part of the security strategy needs to be externally focused and address all parts of the organization end to end to bring everyone on the same page from day 1. The main purpose of the security strategy is not to bring aboard the security unit itself, but to ensure that all stakeholders from the different parts of the organization is involved and motivated.

Mission statement: *Develop Organization Security Maturity, by defining and implementing security controls and incident response capabilities to detect and prevent unauthorized access and data theft in critical systems.*

The purpose of anchoring the security strategy at senior management level is to get the business side involved and should be two-way. It is not simply enough to inform about the strategy from the security teams point of view, but to get the input of the stakeholders for their concerns, points of view, and what they want to be addressed as part of the strategy going forward.

Without this inclusiveness the security strategy will mostly be ignored and be more of a special pet project for the security department and various subject matter experts without any real connection or impact to the business.

See further details in section 5 for details of relevant decision bodies, collaboration forum and roles and responsibilities of the different organizational functions involved in the different parts of security governance.

4 Developing the security strategy & architecture

In order for a security strategy to be effective, it must demonstrate value to the organization while avoiding the traditional pitfalls associated with security being perceived as only being an inconvenience and an obstacle to effective business operations and not a business enabler. Some security related risks represent business opportunities and should therefore be considered tolerable and thus be accepted.

A business-focused approach to developing and delivering enterprise security architecture that is focused on enabling business objectives while providing a sensible and balanced approach to risk management. A balanced approach when developing the security architecture can create the important connection between the goals and objectives of a business, and it provides appropriate measures to protect the most critical assets within an organization while accepting risk where appropriate.

4.1 Statement of sensitivity

The purpose of a sensitivity analysis builds on the defined information security risk analysis process and the main objective is to support the classification of organizations assets and what data it is storing, processing or transporting to be able to capture the **Confidentiality, Integrity, Availability** (CIA). The value properties of the information assets for systems and makes the organization aware of critical business functions, data, assets, and relevant compliance requirements. The sensitivity analysis in addition to outlining the strategy of what assets to protect acts a precursor to a system security threat and risk assessment later when developing the controls required.

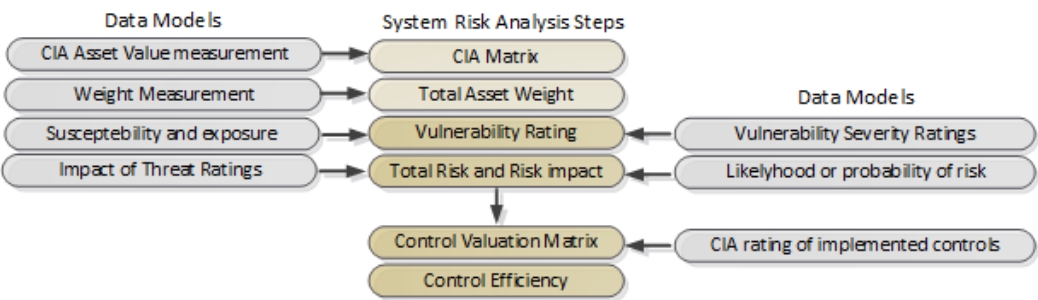


Figure 4. Sensitivity Analysis Process

The key point of the sensitivity analysis though, is to provide an overview of the organizations assets, and based on the importance of the assets, form the strategy accordingly by helping with the identification of the most critical ones and the required controls to meet CIA requirements for each of them.

A detailed methodology for classifying of assets following attributes for confidentiality, integrity and availability to provide risk based analysis can be found at the ISACA website [here](#)

Requirements also needs to be addressed from a business perspective and objectives and goals need to be tuned to be as effective as possible and can help to spot any over-classification as it is costly and it impact the potential user experience and efficiency of the information assets.

During the statement of sensitivity, the acceptable risk levels of the organization also needs to set and the overall **risk appetite** decided along with clearly define thresholds. Similar to the asset classification, this is important for the risk and threat based design of the controls as part of the architecture development work later.

Regulatory requirements also needs to be clarified, and how they impact the various assets, since requirements mandated by governmental agencies are not up for debate in regards of risk tolerance or risk appetite. Fines can be significant (GDPR up to 4% of all revenue) and relevant licenses to operate can be withdrawn if repeat breaches or lack of improvement is found over time. Naturally, any organization's

Defendable Architecture Guideline

Developing an effective security strategy and architecture

assets that falls under potential regulatory impact should get priority accordingly when implementing controls.

The statement of sensitivity can help establish the available options, and priorities for the recovery of assets and/or information stored within them. Recovery is essential for sensitive information, services and business functions, thus this needs to be taken into account in the defendable architecture later on addressing the requirement for **high availability** definitions.

4.2 Exposure

After identifying what assets and data that are the most important to protect, the next step to develop the strategy, architecture and controls is to assess the level of exposure. This is done by analyzing the environment in which the organization operates. What sector it operates in, what types of customers does it have, and what type of technology is used in either offering services directly, or supporting the main business. Looking at potential threats, measuring exposure & risk identifying attack vectors, vulnerabilities, threats are all key aspects to gain an insight in the overall threat level of the organization.

The process of doing a detailed threat based analysis and security control design is the core of DA-2020-002 in how to design a “threat driven defendable architecture”. The threat driven methodology uses elements from both Lockheed Martin’s Defendable Architecture as well as that of PASTA threat modelling framework.

4.2.1 Identifying threats



As part of determining the exposure of the organization it is important to understand both the external security threats to the organization as well as any internal security threats posed by inappropriate use and lack of awareness of its employees.

From perspective of analysis the definition of threat assumes the existence of a threat “source,” which is an actor posing the threat, referred to as threat actor or TA for short. Threat is defined as being composed of Capability, Intent and opportunity.

The figure to the left shows the commonly accepted components of threat which includes the concept of opportunity and hostile intent. It also shows the overlapping fields of the different threat elements can be used to display the different levels of threat states posed by threat actors:

- Impending threat is the combination of capability and hostile intent, however, without the opportunity to act, the threat remains in the impending stage and is considered to be dormant
- Potential threat is the combination of capability and opportunity. Without hostile intent, this threat remains in the potential stage. This is the main category of the insider threats. Insiders have both the opportunity and capability but in general does not display any hostile intent until something triggers a change in motivation.
- Insubstantial threat is the combination of hostile intent and opportunity. Without the capability, many attempts to act will fail or turn out to be insubstantial

For a more detailed insight into the different capabilities, threat actor tiers and their mode of operations, see section 3.5 of DA-2020-002.

Security Principle 001-6: *The external security threats to the organization must be acknowledged and understood*

Defendable Architecture Guideline

Developing an effective security strategy and architecture

Security Principle 001-7: *The internal security threats posed by inappropriate use and lack of awareness must be acknowledged and understood*

4.2.2 Identifying Vulnerabilities

Asset management of the organization's infrastructure and systems is a foundational requirement for information security in general. This is normally used to establish a baseline for what components are actually authorized to be running in the organization's infrastructure and what is not but is key in this process to separate what is important from that which is not.

Inventories of the different systems and their HW and SW components need to be developed showing direct and indirect communication links into an asset inventory database. Based on the inventory, known vulnerabilities can be identified along with the business impact and risk associated with a breach of the same systems. Combined with the insight into already implemented and possible limitations of existing preventive controls the full threat picture for each individual asset can be painted and then aggregated to provide a holistic view of the organization's threat picture.

Security Principle 001-8: *The consequences of a security threat to the organization's assets must be acknowledged and understood*

Security Principle 001-9: *The capabilities and limitations of existing protection measures must be acknowledged and understood*

4.2.3 Assess Risk Exposure

Depending on scope, risk and vulnerability assessments can encompass some or all of the organization's assets and services utilized and use them to gather necessary data about the security posture of the underlying infrastructure.

A risk and vulnerability assessment of the identified assets is a fundamental building block in the organization's integrated risk management processes. Without visibility into potential exposures, it is difficult to know where to focus security investments and resources where they are most efficient and most required. A vulnerability assessment identifies, quantifies, and prioritizes the relevant risks associated with the vulnerabilities that are discovered in a system. The risk assessment also takes into account the different recognized threats and threat actors that are identified and the likelihood of the combination of these factors will result in an incident with subsequent exposure or loss.

An assessment of the vulnerabilities & threats that exist in the organization's environment and the likelihood that they will be exploited and cause a business impact to the organization builds an understanding of the exposure and collective amount of risk.

Security Principle 001-10: *The likelihood of vulnerabilities being exploited by external threats must be determined*

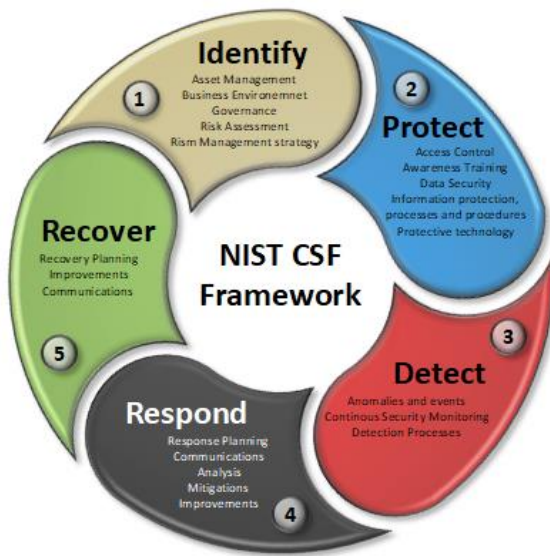
Security Principle 001-11: *The likelihood of vulnerabilities being exposed by inappropriate use must be determined*

Security Principle 001-12: *The security and business impact of any individual or combination of vulnerabilities being exploited must be determined*

Defendable Architecture Guideline

Developing an effective security strategy and architecture

4.3 Develop strategy & assign control framework



To properly develop the strategy and architectures it is important to pick a framework to use so progress can be effectively tracked while prioritizing the most important steps. Similar to help defining the scope of the ISMS as mentioned earlier, there are options from [ISO](#), [NIST](#) or [CIS](#) available⁴.

IS27000 series provide the foundation for various information security practices and is a standard that focuses on keeping the organization's information confidential while maintaining integrity by preventing unauthorized modification and being available to authorized people and systems. There are multiple documents within the ISO framework such as ISO27001 which defines information security management and governance, ISO27002 which defines controls etc. assessment.

The National Institute of Standards and Technology (NIST) has a cybersecurity framework for organizations that are responsible for or operating critical infrastructure. The goals are the same as ISO 27001, with an emphasis on identifying, evaluating and managing the acceptable risks to information systems.

The NIST Cyber security framework (CSF) provide five concurrent and continuous functions which are identify, protect, detect, respond and recover. These functions provide a high level strategic view of the lifecycle of an organizations management of cyber security risk.

CIS Critical Security Controls is a non-profit computer security organization that has been around for quite some time. CIS is well-known for publishing best-practice security recommendations and benchmarks for hardening of operating systems. For security architecture for organizations that either want a clearly defined scope or doesn't entirely know where to start, CIS20 is considered to be the most suitable framework to apply. While ISO27002 include a smaller set of more loosely defined controls, the CIS Controls provide a concrete set of detailed multi-domain controls along with a holistic approach to security across the technology aspect of the organization along with a set of tiers based on the importance of the controls. CIS controls map into the same continuous function as NIST CSF categories, except for the recover part which needs to be addressed separately

These controls are typically viewed as industry best-practice due to the reputation and credibility of CIS, and serve as a great baseline for any security strategy. Combined, the 20 high-level controls in CIS v7 are organized into basic, foundational, and organizes easy to provide recommendations based on the implementation groups based on size and maturity of the organization. CIS serves as a good first framework to use in building a security strategy.

The CIS Controls have been developed through the common understanding of what security controls that are the considered to be the most efficient overall to prevent security incidents, unauthorized access and data theft through breaches while mitigating the damage caused by threat actors attacking the organization's infrastructure. The CIS controls does not only address prevention but also the detection of indicators of compromise and indicators of attack to preventing additional incidents.

⁴ <https://www.infosecurity-magazine.com/news/nist-cis-security-frameworks-see>

Defendable Architecture Guideline

Developing an effective security strategy and architecture

The defense strategy identified in the CIS framework, which the security architecture is based upon addresses the limitation of the initial attack surface by hardening endpoints and applications, identifying servers that have been compromised through detection and forensics, disrupting threat actors C2 traffic by finding unauthorized installed malicious software and rootkits and establishing defensive controls that can be continually improved.

Additionally the CIS framework address also the respond and identify dimensions for various sub-controls under the main 20 security controls, and can cover 4 out of the 5 sectors as defined by NIST CSF. Only the recover section, involving recovery planning and business continuity would need to be addressed outside the defined CIS controls.

By combining ISO at the top level, supplementing with the more specific CIS20 for the design of controls, a hybrid approach is taken with balancing the good processes (guidance from ISOs, NIST) with a more concrete design scope from CIS and enriched with threat-intelligence approach using PASTA and Lockheed Martin's Defendable Architecture . The necessary guidance can then be applied from threat intelligence and taken into account based on the CIS control framework and the technology based controls can be more focused and implemented in the right place.

Security Principle 001-13: *Overall security strategy and information security management system shall follow the ISO27000 framework*

Security Principle 001-14: *Defendable Security architecture, scope, design and implementation of controls shall follow the CIS20 framework*

Security Principle 001-15: *Security controls relevant for the security architecture not addressed by CIS20 should follow NIST CSF*

4.3.1 Control Prioritization

CIS benchmarks and control sets acknowledge the reality on the ground for most organization, which is the fact that resources are limited and thus hard priorities must be set. CIS acknowledges this and separates the designated controls into three main categories, basic, foundational and organizational.

Of the basic level of controls the 4 below is strongly recommended to be implemented and be in place before moving on to the others:

- CIS17, Organizational, Implement a security awareness and training program
- CIS3 Basic, Continuous vulnerability management
- CIS4 Basic, Controlled use of administrative privileges
- CIS6 Basic, Maintenance, monitoring, and analysis of audit logs

The security awareness program might not be the obvious first choice for everyone to start at, but given that 90% of security incident and subsequent data breaches occur because of phishing and social engineering, it is now considered the main entry point for threat actors to gain access to the infrastructure. Loss of control of operators and administrators managed endpoints can be particularly devastating.

Vulnerability management is the next area that should receive proper attention and focus. Approximate a third of all the security incidents and corresponding security breaches occur due to software not being properly maintained and updated. Automated vulnerability management and patch management will do wonders to the overall security posture. The information gathered from the vulnerability management solution is also directly usable and is a key input to the security strategy when deciding the overall business risk and exposure of the organization.

To secure access to its assets and sensitive data, the number of privileged accounts should be both limited and controlled within the organization. A proper operator remote access platform using multi-factor authentication and privileged access management can bring down the main risk of insider threats

Defendable Architecture Guideline

Developing an effective security strategy and architecture

and credential abuse significantly. If the organization have a complex operating model and making extensive use of managed services providers for outsourcing, this becomes a must-have to reap the business benefits while maintaining tolerable risk levels and compliancy.

The collection and auditing of log data is the key for detecting ongoing or previous security incidents. All access and changes to the organization's assets and data must be logged, and the logs must be regularly analyzed for abnormal activity that may indicate a compromise or attack. Without the collection of log data from relevant assets, the organization is completely blind to what is actually happening.

After the absolute basic minimum level of control are implemented to a satisfactory level, the next set of controls to be implemented should be based on the results of the earlier statement of sensitivity analysis and exposure of key assets.

As an example, if the organization deals with the processing of heavily regulated data, whether it be personnel data of a government agency, healthcare data covered under HIPAA regulation, or a telecom operators customer data regulated by GDPR and the controls are data governance and access control are considered lacking, the following CIS controlled should be applied.

- CIS10 data recovery capabilities
- CIS13 Data protection
- CIS14 access based on need to know

If the already implemented controls in this area is considered to be adequate, and the risk associated with data governance is low, but the risk analysis shows that infrastructure configuration and change management is an issue the following set of controls should be applied before that of data management and access controls:

- CIS5 secure configuration of HW / SW of endpoints
- CIS11 Secure configuration management of network components such as switches and routers

If perimeter defense and detection controls are discovered through the risk assessment process to be insufficient, the following foundational controls should be applied as a priority item

- CIS8 Malware defenses
- CIS12 Boundary Defense, perimeter controls and functions

Either way, the CIS controls gives a good overall ability to track the implementation of various controls across multiple domains in the organization. The supporting security architecture needs to go in detail on how to create these controls and provide the necessary blueprints and requirements to both implement them. The architecture and blueprints provide the ability to audit that the controls actually fulfills their intention by being implemented in the correct way.

Security Principle 001-16: *CIS control implementation and priority shall be based on overall risk assessment process outputs*

Security Principle 001-17: *Security Architecture framework should document relevant basic and foundational CIS controls as defined by the security strategy*

4.4 Develop architecture & security controls

Security threats are constantly evolving and changing, and similarly is every organization that have learned to adapt to shifting conditions and market development. As the organization keep evolving, so should the security architecture and corresponding roadmap(s). Constantly managing and developing new strategies, controls, response plans and overall policies is therefore essential to remain in front of the challenges of the ever-evolving threat landscape.

Defendable Architecture Guideline

Developing an effective security strategy and architecture

With CIS as the framework choice for implementing security controls, designing the overall architecture and designing the required counter measures can begin. The objectives of the security architecture and control design can be summarized below:

- Strategy alignment objectives
 - Prioritize control design and implementation based on risk assessment and gap analysis
 - Develop protection, detection and access control measures to deliver on CIS control objectives
 - Apply a business driven and threat intelligence driven design process
 - Design a set of controls that are interlinked and overlapping but still modular
- Design process objectives
 - Reduce the likelihood of vulnerabilities being exploited through preventive controls
 - Reduce the impact of a vulnerability being impacted
 - Detect threats that manage to breach the preventive controls
 - Secure access to assets and/or sensitive data and audit all user activity
- Implementation Objectives
 - Develop methodology to measure effectiveness of controls
 - Create roadmaps for rolling out and continuously developing controls
 - Process support and competency areas required for the defined controls and capabilities

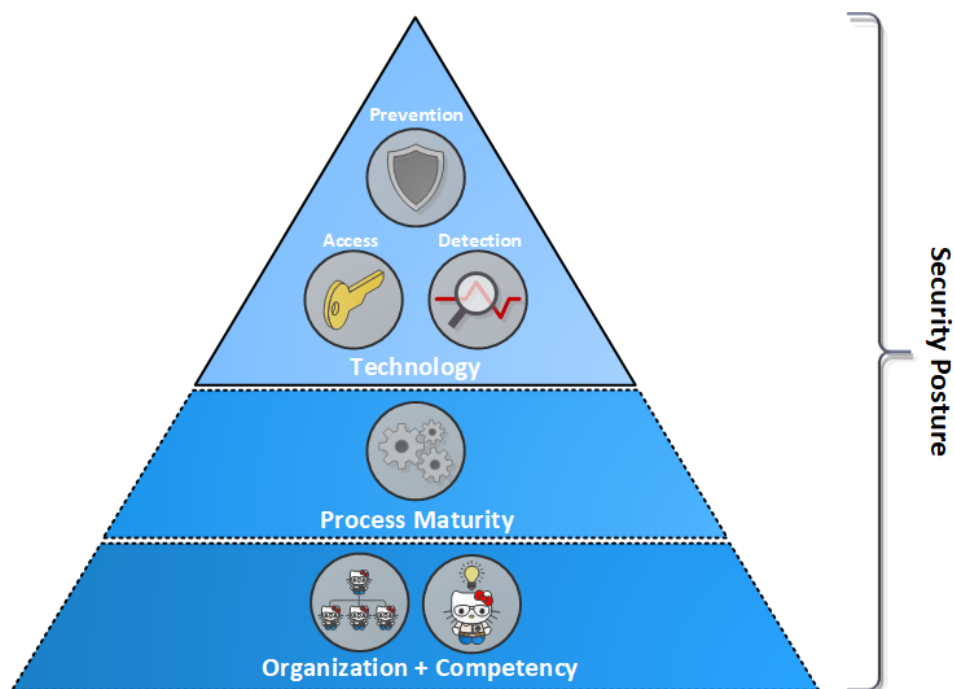


Figure 5. Security Architecture domains and areas

Although while a complete security posture for an enterprise need to cover all the aspects of security technology, processes and people, It is however mainly guidance of implementing the technology area set of controls that is covered by the security architecture as part of the defendable architecture guideline series. The ambition is to provide detailed guidance of deploying and implementing the right level of controls and capabilities to mitigate potential threats.

A high level overview of how to do threat modelling, assessing threats, business risks and how to identify attack surfaces supported by using threat intelligence is given as an introduction in the DA-2020-002. This document is the foundation principles of Defendable architecture detailing the entire process on

Defendable Architecture Guideline

Developing an effective security strategy and architecture

threat modelling. Identifying the threat actors along with their techniques, tools and procedures (TTP), analyzing their most commonly used vectors of attack and then mapping them against the discovered vulnerabilities allows the organization to design and implement security controls. These controls will then be tailored for the most likely threats it is facing and bring risk down to tolerable levels meeting business, regulatory or any industry sector standards that might apply.

A set of key security controls have been pre-defined in DA-2020-002 as a baseline for foundational controls and capabilities and are divided into three main areas. The following functional defendable architecture areas under the technology domain are defined:

- Capabilities and controls for Prevention
- Capabilities and controls for Detection
- Capabilities and controls for Secure Access

Within each of the areas are described detailed descriptions and requirements for different security controls and capabilities with example implementations and solution designs and blueprints.

Security Principle 001-18: *security control design prioritization and implementation shall be based on a risk assessment process and gap analysis to be as effective as possible*

Security Principle 001-19: *Security protection, detection and access security controls shall be designed to deliver on CIS control objectives*

Security Principle 001-20: *a business driven and threat intelligence driven design process shall be applied when designing security controls*

Security Principle 001-21: *Security controls shall be interlinked and overlapping to support defense in depth but still modular to be implemented individually*

Security Principle 001-22: *Methodologies shall be developed to measure the effectiveness of designed and implemented security controls*

Security Principle 001-23: *Processes for continuously developing security controls and roadmaps for implementing them shall be created and maintained*

Security Principle 001-24: *Process support and competency areas are required to be developed for each defined security controls and capability*

Defendable Architecture Guideline

Developing an effective security strategy and architecture

4.4.1 CIS control to architecture mapping

The tables below provide an overview of the current coverage and scope of a documented reference security architecture towards the CIS control mappings. As the security architecture is developed and matured, all basic and foundational controls should be covered. Although, the priority on developing controls should be as mentioned earlier based on the overall risk assessment as not all areas are considered to be of equal importance.

<i>ID</i>	<i>Basic CIS controls</i>		<i>Scoped</i>	<i>DOC ID</i>
CIS1	Inventory and Control of Hardware Assets	Partially addressed under automated discovery for vulnerability management and CMDB integration	Yes	DA-2020-005
CIS2	Inventory and Control of Software Assets	Addressed under vulnerability management as well as software security , configuration and patch management	Yes	DA-2020-005 DA-2020-007
CIS3	Continuous Vulnerability Management	Addressed under automated discovery for vulnerability management and CMDB integration.	Yes	DA-2020-005
CIS4	Controlled Use of Administrative Privileges	Addressed, covered under Identity and Access Management, AD section and privileged access management	Yes	DA-2020-006 DA-2020-010
CIS5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	Servers covered under software and application security and for configuration auditing under detection & monitoring of endpoints and device configuration audit, EUC devices in EUC documentation	Yes	DA-2020-007 DA-2020-011
CIS6	Maintenance, Monitoring and Analysis of Audit Logs	Addressed and covered under monitoring, Audit and compliance	Yes	DA-2020-005

Table 1. Basic CIS controls mapped to architecture scope

Defendable Architecture Guideline

Developing an effective security strategy and architecture

<i>ID</i>	<i>Foundational CIS Controls</i>		<i>Scoped</i>	<i>DOC ID</i>
CIS7	Email and Web Browser Protections	Targeted for EUC documentation	Yes	DA-2020-011
CIS8	Malware Defenses	Addressed both under endpoint security in security monitoring and platform advanced security boundaries	Yes	DA-2020-004 DA-2020-005
CIS9	Limitation and Control of Network Ports, Protocols and Services	Addressed both under platform security boundaries and resource isolation with security zone model	Yes	DA-2020-003 DA-2020-004
CIS10	Data Recovery Capabilities	Addressed under business continuity on defining policy on acceptable values based on classification of services	Yes	DA-2020-012
CIS11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	Addressed under configuration management, hardening of network devices.	Yes	DA-2020-007
CIS12	Boundary Defense	Addressed under prevention/zone model and platform and perimeter security boundaries	Yes	DA-2020-004
CIS13	Data Protection	Controlling access to data, and protecting data at rest and in transit. Partial coverage, data loss policies RTO-RPO defined for services. Data access under identity and access management, and endpoint protection under Systems and EUC systems	Yes	DA-2020-007 DA-2020-011 DA-2020-012
CIS14	Controlled Access Based on the Need to Know	Scope of identity and access management and privileged access management	Yes	DA-2020-006 DA-2020-010
CIS15	Wireless Access Control	Covered in wifi specification, will be addressed in EUC documentation	Yes	DA-2020-011
CIS16	Account Monitoring and Control	Addressed under identity and access management and security monitoring for user behavior analysis	Yes	DA-2020-005 DA-2020-010

Table 2. Foundational CIS controls mapped to architecture scoped

Defendable Architecture Guideline

Developing an effective security strategy and architecture

ID	Organizational CIS Controls		Scoped	DOC ID
CIS17	Implement a Security Awareness and Training Program	Out of scope for defendable architecture framework	No	
CIS18	Application Software Security	Covered under software security, devops sections	Yes	DA-2020-007
CIS19	Incident Response and Management	Covered under security operations guideline documentation	Yes	DA-2020-013
CIS20	Penetration Tests and Red Team Exercises	Out of scope for defendable architecture framework	No	

Table 3. Organizational CIS controls mapped to architecture scope

4.4.2 Plan and structure security architecture development

In addition to understanding what assets and data that is required to be safeguarded, it's essential to understand how and where assets and data is being protected through the design of security controls. These controls are addressing the various areas of the organization and its assets ranging from storage and data at rest to end user compute and email services to protect against phishing attempts. Below is a visual presentation of the access, preventive and detection controls that are scoped or planned within the defined security architecture.

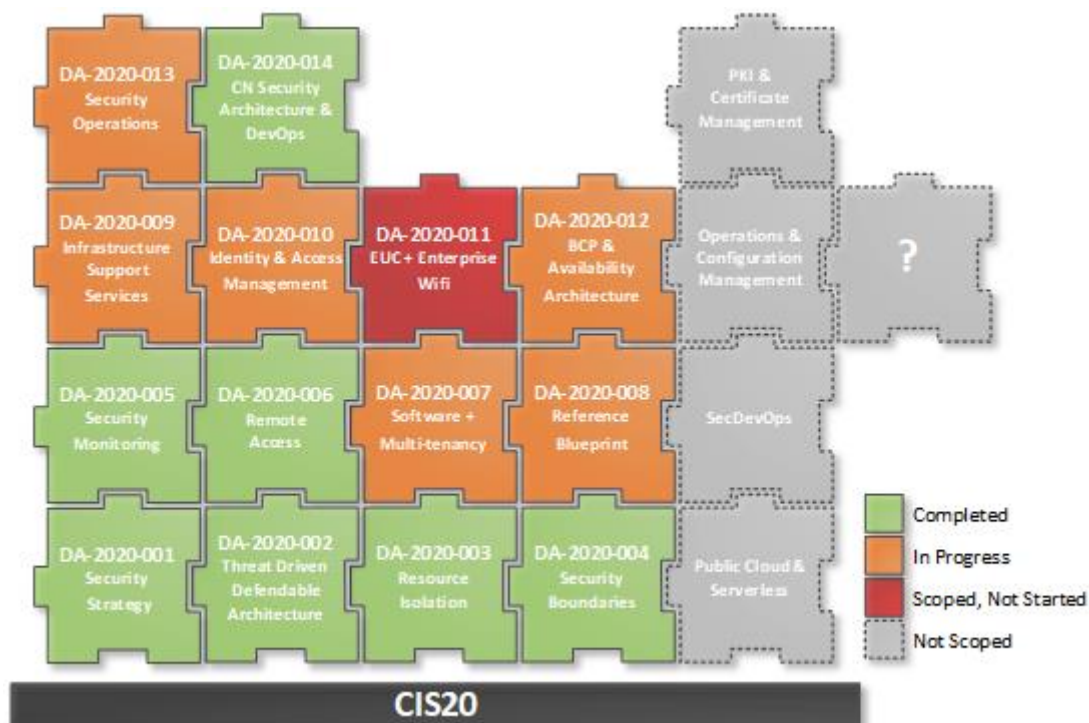


Figure 6. Security Architecture Development Structure

The security architecture which have its foundation in the CIS20 controls as shown in the tables above, provide the necessary target architecture and blueprints on how to implement the different controls. In

Defendable Architecture Guideline

Developing an effective security strategy and architecture

some cases, controls which logically belong together may be covered in the same document, or neighboring technologies and blueprints relevant to improve the effectiveness of the control should also be added as required. Rome was not built in a day and neither is the development of a mature and end to end security architecture, so the different sections of the documentation should be developed in accordance to the priority as given in the strategy and the organization's need. Structuring the development process makes it clear what the deliveries will be and make the resource allocation easier to plan, and the development faster so if a specific project or task needs supporting architecture documentation, resources can be pooled and delivery can be speeded up.

The item blocks shown above belong to the defined Defendable Architecture Framework which is currently in development and is available to organizations that seek guidance on specific control blueprints or implementation.

Security Principle 001-25: *Architecture development should be according to clearly defined priorities as per established strategy*

4.4.3 Technology & Vendor strategy for security control design



As part of the security architecture and design of security controls, a clear strategy should also be developed for the different suppliers and technologies to use when creating the blueprints. This commercial strategy must not only take into account the feature sets and functionality but also address topics such as regulatory limitations. Some vendors may be forbidden by national legislation and regulatory authority to be utilized as components of service providers, in particular those that find themselves with Critical Information Infrastructure (CII) labels. As an example, Pakistan's regulatory authorities forbid the use of components with Israeli origins which may pose a problem since many key products in the cyber security sector

are either developed by or sold by Israeli companies such as Checkpoint or CyberArk. Similarly the limitation of usage of Chinese products from Huawei and ZTE in the telecom sector in several western countries is well-known in later years as a regulatory blocker in using these suppliers in CII deployments. While the topic of geo-politics itself is well outside the control of most organizations that only want to develop their security posture, the fallout of international politics may result in regulatory policies being applied that may impact the organization and build risk. Suddenly having to replace large parts of the infrastructure as a result of changed policies due to the selection of the "wrong" vendor is a major business risk that should be acknowledged and accounted for as part of the security control design process in the architecture development.

Security Principle 001-26: *Suppliers of technology for security controls used in critical information infrastructure shall be vetted against any regulatory constraints*

When evaluating the different vendors and suppliers for technology to be used in the design of security controls commercial strengths and weaknesses as well as supply chain risk should be part of the evaluation criteria. In some cases threat actors have been known to target suppliers to gain insight into their technology so that any relevant weaknesses can be exploited at the threat actors primary target which makes use of that technology in one or more of their security controls.

It should also be noted when using various software services the accountability of confidentiality, integrity and availability of any asset owned or used by the organization it is accountable for. Commercial contractual framework and risk and audit processes should take this into account and regularly measure any kind of security control that is not managed directly by the organization.

Observation 001-3: *Security functions can be outsourced for cost efficiency, accountability can not.*

Defendable Architecture Guideline

Developing an effective security strategy and architecture

4.5 Establish contingency plans

As a mandated part of the ISMS scope, an important item which needs to be included as a part of the security strategy is to develop contingency and response plans to address potential incidents. Once risks and threats have been identified, controls have been put in place to mitigate threats against potential impacts on the organizations assets. The important thing here is to assume and plan for the worst and set up plans in advance to counter incidents and highlights the need for proper Incident response plans, disaster recovery plans and business continuity plans. It is usually a matter of “when” and not “if” a serious incident either security related or otherwise. An incident response plan is the best chance at defending the organization from suffering the effects of an incident, either operational or security related. The time to plan and prepare a response to incidents, whatever form they may come in, is long before they happen, but awfully short, should the plan need to be developed when the incident actually happens as part of the response.

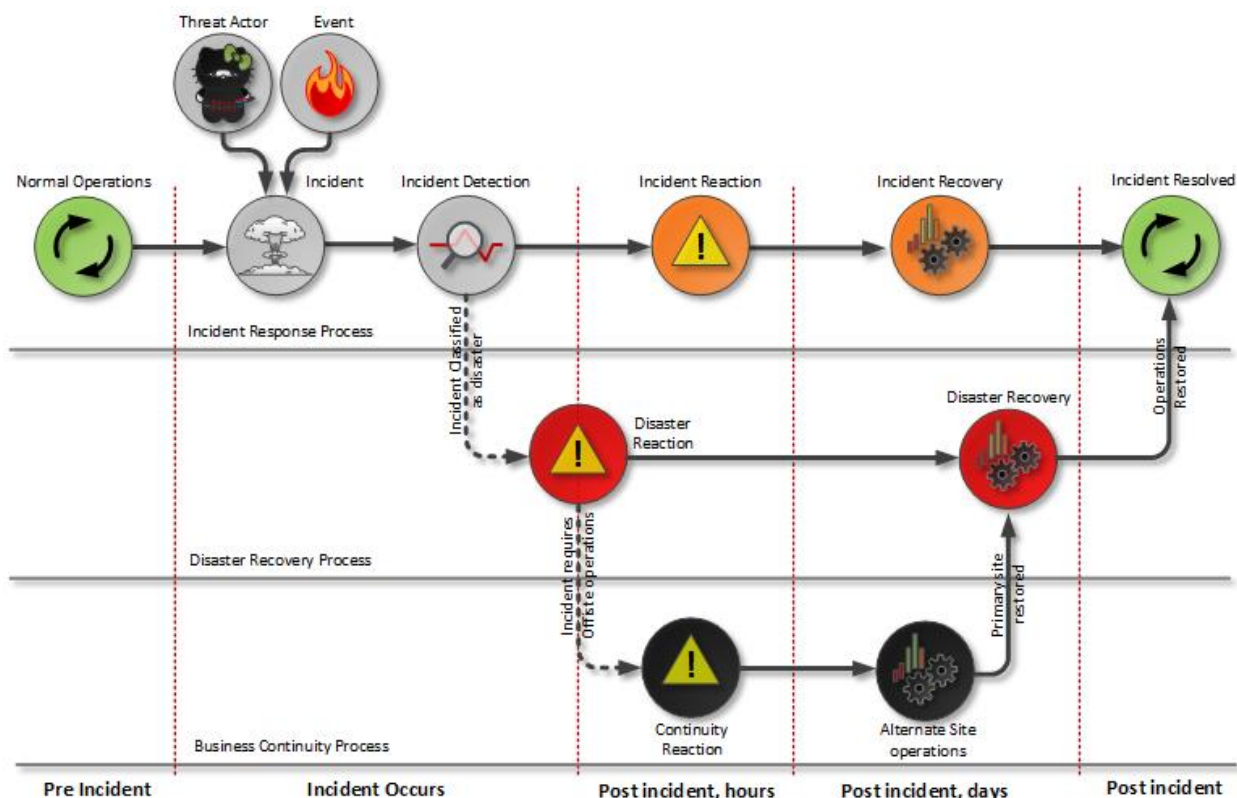


Figure 7. Integrated Incident, Disaster & Business Continuity Response Planning

Incidents, disasters and continuity follows a hierarchy. An incident may occur which is either resolved or may trigger an event classified as a disaster, which in turn requires business continuity. An important item as part of the security strategy is to develop these contingency plans. A classic study case for a catastrophic security incident is that of Maersk, that suffered a near extinction level event after its entire IT infrastructure was destroyed by an attack of the infamous NotPetya worm. Ransomware⁵ keeps topping the list of potential disastrous events organizations are facing and should prepare and plan for. Other types of incidents such as natural disasters in the form of fire or flooding, or geo political ones such as social unrest terrorist attacks can quickly require a business to suddenly require to operate either its personnel or its services outside its primary location.

⁵ <https://www.sdxcentral.com/articles/news/ibm-security-vp-ransomware-can-destroy-your-business-playbooks-are-key/2020/07/>

Defendable Architecture Guideline

Developing an effective security strategy and architecture

An incident response plan is a set of instructions, or playbook that is created to help in the preparation of, detection, response to, and recovery from an incident, security related or otherwise. Most IR plans and playbooks are focused around specific technology usecases and address issues like anomaly detection by one or more of the detection capabilities, confirmed breaches or service outages.

Disaster recovery and business continuity planning is generally used to describe the ability of a system to continue operating and provide resources to its users when a failure occurs in one or more of the following categories in a infrastructure fault domain such as hardware, software, or application. The level of availability is defined as a measure of the percentage of time that a system is continuously operational to support business functions. The required level of availability varies according to the business value of the service.

Disaster Recovery usually means that the organization's services are "restarted" in a new location. Time to recover the application is mainly dictated by the mission and business criticality levels. Recovery happens manually or automatically after an uncontrolled situation such as power loss, natural disasters, etc. and requires multiple sites available for data center locations or use public cloud providers as secondary sites for productions.

With business continuity its about countering extinction level events. The BCP process kicks in when critical assets that are required for operating the main business services of the organization, gets taken off the air by an incident, security related or otherwise. The main objective of a BCP is how mission critical services can be made to be operational outside the primary production sites.

A business continuity plan consists mainly of continuity/recovery strategies to follow and how/where to integrate off-site equipment (data storage, servers and offices). For service production much of the DR and BCP capabilities can be automated at infrastructure and / or service level as described in the section below under high availability architecture

Incident response plans, disaster response plans and business continuity plans should be integrated with each other within a single policy domain rather than being kept separate as shown above in **Figure 7**. The integrated plan It should support concise planning by developing, testing and using Contingency Planning.

Security Principle 001-27: Incident response plans, disaster response plans and business continuity plans shall be created and practiced on regular intervals

Security Principle 001-28: Incident response plans, disaster response plans and business continuity plans should be an integrated response plan and development process

4.5.1 High availability architecture

For the scope of the technical security architecture, the implications is to provide the tools required to classify applications, and define acceptable downtime and data loss for these applications. Based on these requirements, the infrastructure team can create high availability architecture for both the infrastructure as well as for the specific applications as required, and thus ensure that both disaster recovery and business continuity is ensured for the organizations provided services and data. Ideally the most critical services should have automated disaster prevention and disaster recovery built into them, so if an incident is triggered

Automatic recovery may require additional technology capabilities in the form of infrastructure components to be efficient such as Intelligent DNS, route host Injection, hypervisor live migration etc. Interconnection and service load distribution are achieved using intelligent network services using dynamic protocols

A traditional DR scenario assumes that the hosts/applications/services will be changed to match the new location. With intelligent orchestration through cloud management platforms (CMP) and network

Defendable Architecture Guideline

Developing an effective security strategy and architecture

services available, migrating and locating infrastructure components without any configuration parameter changes and without network LAN extensions is possible.

Disaster Recovery (DR) or Disaster Avoidance (DA) solutions are required for the overall infrastructure and services and provides the basis of availability and business continuity. With multiple data centers and technologies to offer business continuity and disaster recovery, it is useful to provide a defined framework to help understand which solution fits better for the services in question as redundancy can be built on multiple levels. Avoiding building in redundancy levels at both service, application, platform and infrastructure layers will provide an overall cost efficiency to the infrastructure.

Availability architecture, DR/DP planning and application classification guideline is highlighted in detail in DA-2020-012.

Security Principle 001-29: *All Applications and services shall be classified and have tolerance levels applied to them for availability, acceptable data loss, and recovery time*

4.5.2 Supporting the security incident response process

As highlighted earlier, the development process of the security strategy and architecture must interlink with and also supporting the incident response process. This means that defined detection capabilities & controls are developed as required by the security operations teams. The main bulk of the developed capabilities for the detection area are directly supporting the SOC to provide them with visibility and telemetry data from the organization's infrastructure in the form of log data, endpoint telemetry, user behavior analysis, flow based networking and others and are measured by their effectiveness in using them to responds to the threat.

The security operations teams should also respond to security threats that are realized by using the developed response plans, whether they are incidents, disasters or continuity reactions.

Observation 001-4: *Security response plans are sometimes also referred to as playbooks, and well-defined playbooks for security incidents are key for automating the response process which again is a must to maintain an effective security operations.*

Since the development of the capabilities are continuous, the impact effectiveness of the capabilities and response plans should be practiced and rehearsed frequently, assessed, and then and re-assessed for threats and vulnerabilities continuously and in particularly as part of the recovery phase of an incident to address short comings in existing controls and response plans.

Security incident response and supporting processes is covered in detail in DA-2020-013 about security operations.

4.6 Planning, prioritization & building

4.6.1 Short time planning

As part of the strategy, foundational items, quick wins, and high risk items should be identified through the risk analysis process which requires these items to be addressed as foundational from the very beginning. Further, identify what is also fundamental to the relevant **future** steps of your plan, and prioritize these actions first. The recommendation is to first look at the basic CIS controls along with the security awareness program. As an example, proper functioning log collection is a key building block for many other security controls and analytic and automation capabilities. The CIS6 covers the very basic things that are required and which is required to address other controls that can be implemented, either as quick wins or as elements that are part of the future planning.

Quick wins are in the context of security strategy implementation defined as identified gaps in the security control space that are considered easy to fix and/or require few resources. In the first phase of

Defendable Architecture Guideline

Developing an effective security strategy and architecture

implementation, a combination of both foundational tasks and quick wins should be part of the implementation roadmap.

4.6.2 Long term planning

For the longer term, defined roadmaps and security maturity development plans needs to be made with clear targets in mind. The implementation of security controls should follow the priority as set by the risk assessment process and deployed over time according to available resources and available budgeting. Planning ahead and constant evaluation of effectiveness of controls.

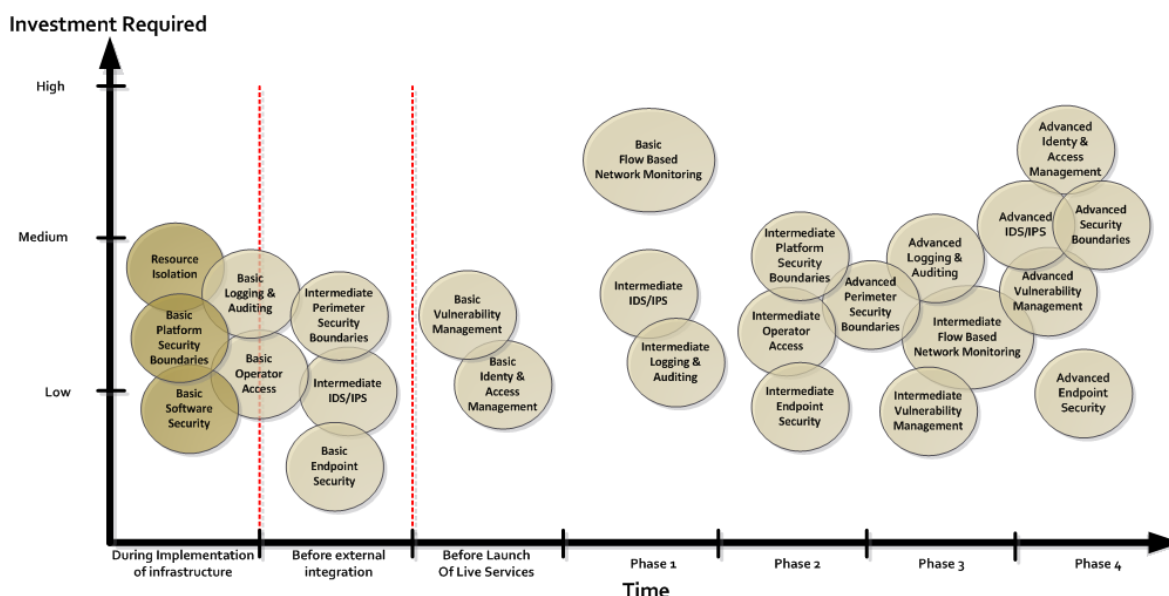


Figure 8. Sample implementation plan of security controls

It is important to keep in mind that the controls implemented also have requirements in the process and people domains as will be highlighted in the security maturity assessment. Competent people must be hired or developed internally, and clear processes and playbooks created for the controls to remain effective.

4.7 Security maturity & measurement

An effective security strategy should have processes that are repeatable and measurable and the architecture should have clearly defined effectiveness goals and requirements as part of the designed controls. This helps ensure the effectiveness of the controls that have been implemented throughout the environment and that processes and competency is in place to make proper use of them. The overall measured effectiveness of the combination of people, technology and processes is referred to as security maturity.

Security maturity matters, a lot, since the combined efforts of these areas impacts the organizations ability to secure its assets and its ability to perform incident response to mitigate any threat actors that manage to breach the preventive controls.

Security maturity it not built overnight either. As an example, It is required to be able to crawl before being able to walk, and you have to be able to walk before it is possible to run. Similarly, security maturity needs to be built up over time since organizations can not, contrary to popular belief rapidly adopt advanced controls and effective make use of a defense-in-depth security architecture when there

Defendable Architecture Guideline

Developing an effective security strategy and architecture

are few or no similar controls already established. Different parts of the organization working together have to develop both individually and together through gradually maturing.

4.7.1 Developing different levels of maturity

The concept of security maturity refers to an organizations adherence to security best practices and processes. Measuring security maturity helps identifying gaps and areas for improvement and the organization's security maturity level should be regularly evaluated. Whether this analysis is done through self-assessment or through an external analyst, ensure that the measurement process is repeatable so when repeated in the future, there will be easy to do an apple to apple comparison between results and track progress

What is the maturity of the organization in regards to control effectiveness, process support and general organization and competencies.

The model shown below in **Figure 9** is based on that from the Cyber Security Maturity Model (CSMM) from US department of defense⁶. The defined levels follow the maturity levels which are used to measure an organization's overall security maturity. The US department of defense evaluation framework provides a good starting point for beginning to develop an organization specific evaluation model for security maturity.

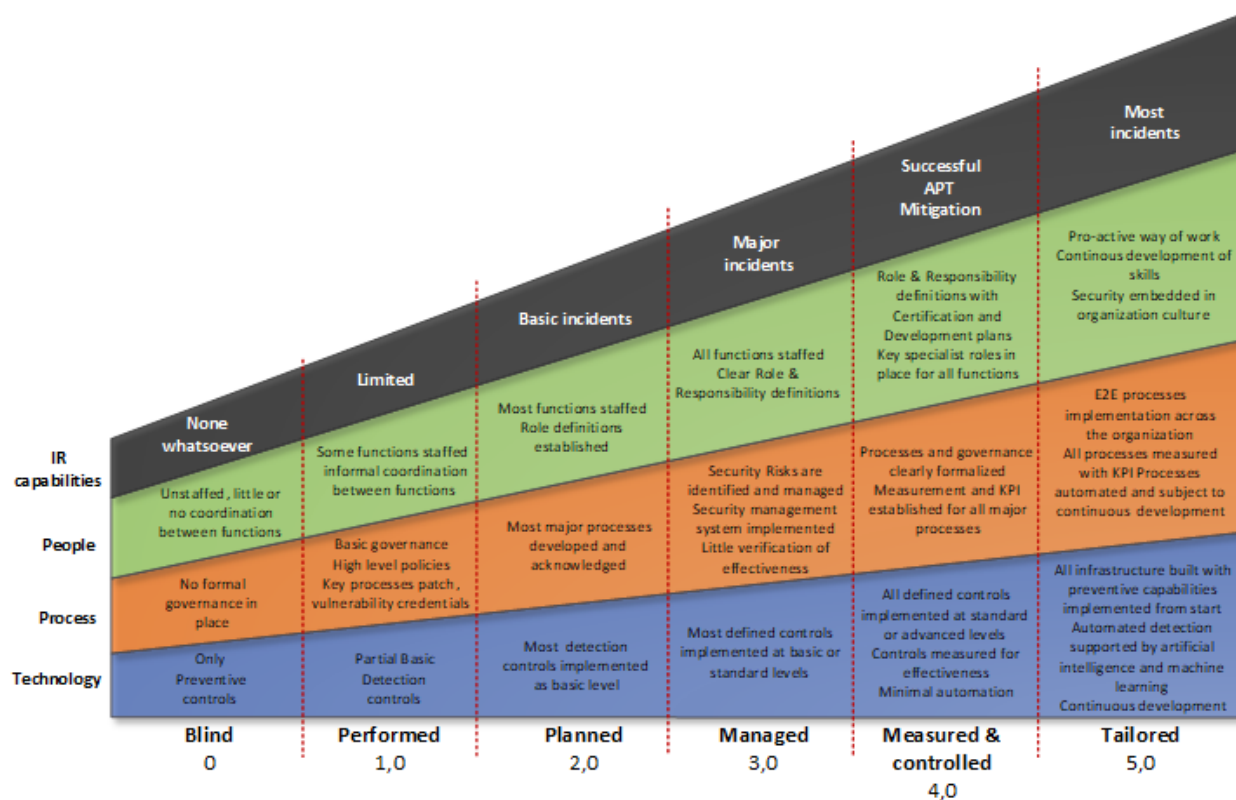


Figure 9. Security Maturity levels

The technology aspect can be assessed for their efficiency by evaluating at the controls that are currently in place, how they are being used, and controls and functions not being used to their full potential. Underutilized or inefficient controls or other tooling may be costly in regards to resources and time while not decreasing the organization's attack surface. Identify the controls to see if they are fulfilling their

⁶ <https://www.acq.osd.mil/cmm/draft.html>

Defendable Architecture Guideline

Developing an effective security strategy and architecture

original purpose, and if there is possible to obtain better efficiency or results from them. If not, consider phasing them out or replacing them with a different type of control or technology solution.

Security Principle 001-30: A security maturity evaluation framework shall be created

Security Principle 001-31: Security maturity shall be evaluated regularly and no less than 1 per year

5 Security Governance structure

For a security strategy to be effective, it must be delivered on, and to be delivered, the security strategy needs to be aligned with business strategy and distributed to different functions of the organization for execution. Since the different functional units all have their own primary functions, it is critical that they are aligned and coordinated in delivering security into their respective areas, this is where the aspect of security governance comes into play.

NIST describes governance as: “the process of establishing and maintaining a framework to provide assurance that security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk”

Security governance consists of determining whom within the organization, which will be responsible for what. Information is required to flow between both the strategy, tactical and operational levels. Each level of governance within the organization should be associated with a specific set of responsibilities and formalized decisions bodies established with the right people being assigned to them. The most important aspects of the governance structure is that it is established, with definition of roles, assigned responsibilities, accountability.

Security Principle 001-32: Security governance shall be clearly defined with roles and responsibilities

Security Principle 001-33: Formalized decision bodies shall be established within the different tiers of the organization with a clear mandate and the empowerment to execute on decisions made

5.1 Security governance decision forums

To have governance of the security strategy and the architecture through its entire lifecycle there should be an established process and forums where to develop, control and manage the different aspects and levels of the security strategy. Formal decision bodies is required to be established at each organization level with a clear mandate to execute on their assigned roles.

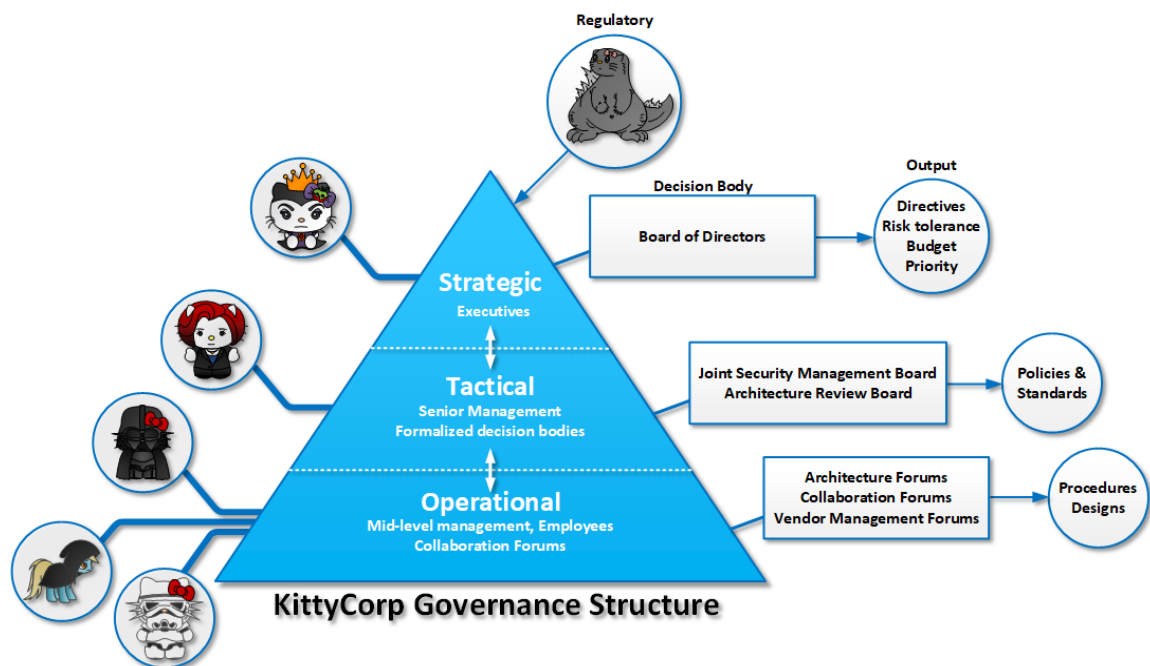


Figure 10. Security governance tiers and formalized decision bodies

Defendable Architecture Guideline

Developing an effective security strategy and architecture

The different levels of the organization have different interests and views thing based on their primarily role. The board of directors are typically entirely business oriented, while the engineering teams at the working level of the organization are typically more detailed and technology oriented. The architects and the technology leaders in the middle layer need to work as “translators” mapping the business requirements from the executive management into technology and security related strategies that can be handed over to the operational level. It is important that these key people can speak both the business language of the management as well as the tribal language of the technical and security subject matter experts and thus act as a bridge between business and technology.

External stakeholders to the organization such as regulatory authorities relate to the executive management which then takes any external relevant requirements into account via the business strategy and the security objectives so that any required mitigation can take place in the other parts of the organization that plans and executes on the strategy.

<CxO forum?>

Defendable Architecture Guideline

Developing an effective security strategy and architecture

5.2 Security governance ecosystem

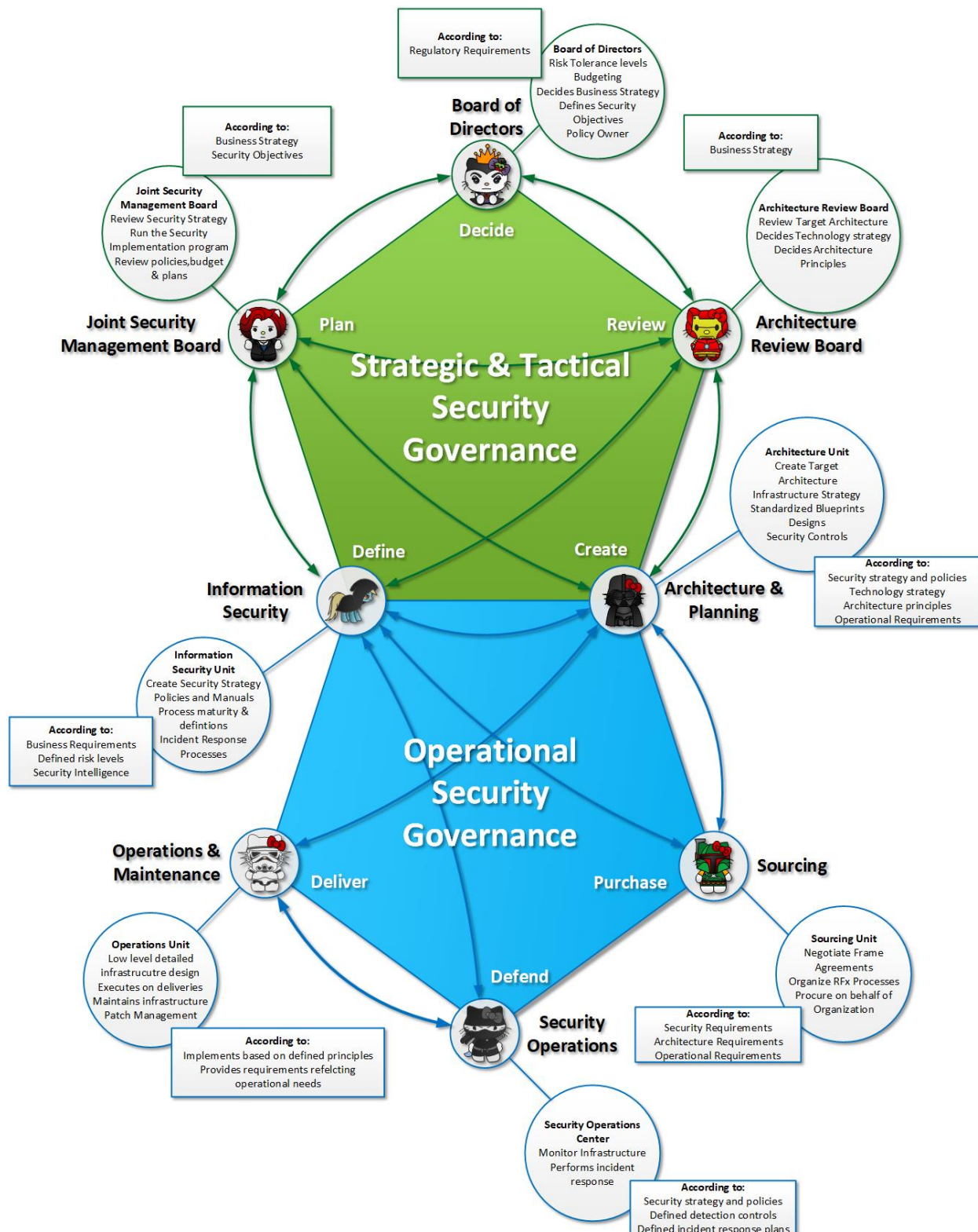


Figure 11. Security governance ecosystem

Depending on the size of the organization multiple of these functions may be on the same team, or there may be multiple teams of highly competent specialists. Security is all about teamwork and it is not all of the roles and units that perform security related functions which are directly attached to the security

Defendable Architecture Guideline

Developing an effective security strategy and architecture

functions either. Specialists may be working in the technology domain or be in governance functions outside the environment of operational security but still play a crucial role in maintaining key security related functions across the organization.

The figure above shows the interaction and dependencies between the formalized bodies at the different levels in the organization at strategic and tactical levels as well as the organizational units that are responsible for developing security and technologies strategy and architectures at the operational level.

Within a large organization, the governance of security functions are usually divided between the strategic level & tactical governance and the operational level which takes care of operations planning and execution as shown in this example with the main 5 relevant entities each and a partial overlap in the middle on the information security and architect functions. At strategic level, it's the formalized decision bodies in the form of boards with appointed senior or executive managers such as the board of directors, (BOD) , Joint Security Management Board (JSMB) and the architecture review board (ARB).

On the operational level within the organization there are multiple teams with various roles that also needs to interact with each other and all are required to pull in the same direction for an organization's security posture and incident response capability is to be at sufficient levels.

At operational level the Information Security (IFS), Architecture & Planning (AP), Operations and maintenance (OAM), security operations (SOC) and sourcing & procurement (SP) units regularly interact with each other. The governance ecosystem and the relations between the functions require some detailing as to which entity should be responsible for what. The field of security is quite wide and it is important to attach clear roles and responsibilities to clarify which entity is responsible and governs what and the relations and dependencies they may have to the other units, functions and formalized decision bodies.

5.2.1 Executive management and board of directors



The executive management are the formal owners and also approvers of the organization's top level policies and strategies. At this level, it is all about business, whether it is risk, budgets or prioritization. For any security strategy and implementation program to succeed, it is paramount that it is properly anchored and sponsored at the executive level

The formalized decision body at the strategic tier of the organization is typically the board of directors. The board of directors can execute their responsibilities by continuously providing a strategic oversight on all aspects relating to security. The oversight can be executed by evaluating, monitoring and directing the strategic security initiatives and by being accountable and responsible for the following:

- Understanding the importance of security to the organization.
- Reviewing investments as part of the security strategy to ensure alignment with the organization's risk appetite and business goals
- Endorsing the creation of a security strategy and implementation program.
- Request reports from joint security management board of the strategy's effectiveness.
- Prioritize relevant security risks to maximize protection of business value
- Request budget estimates and implementation road maps to execute on the security strategy

Any changes or updates to security strategy or other top level policies to support the security strategy or the security architecture shall be advised by the joint security management board and approved within this forum.

Defendable Architecture Guideline

Developing an effective security strategy and architecture

5.2.2 The Joint Security Management Board



The joint security management board (JSMB) is the decision body where senior management from the different parts of the organization meet to scope and drive the execution of the defined security strategy as given by the board of directors.

Typically chaired by the Chief Information Security Officer (CISO), the JSMB must be staffed with personnel who have the authority to both represent and speak on the behalf of their respective units in the organization. The same people also need to serve as advocates for security initiatives. The ideal people to sit on the JSMB are department unit leaders at SVP or director level, and an ideal size for the steer-co is 6 to 8 members.

The primary objective of the joint security management board is to get the business side involved, and not only informing the rest of the organization of what happening, but getting input and discussing what they want.

The main tasks of the JSMB is to define and maintain the defined high level security objectives as per the directive of the executive management. These objectives are the overview of the main priorities to ensure the organizations' overall security where all sides of the business should pull their weight by the information security department helping to define and locate the organization's crown jewels, HR offering insight into the ongoing security awareness training, legal on relevant compliance issues etc.

For a start the following items should be among the defined responsibilities of the JSMB:

- Review, and recommend security strategy, policies and manuals
- Review the effectiveness of policy implementation and report to executive management
- Provide a clear direction with visible management support for ongoing security initiatives
- Initiate and drive plans and programs to maintain organization-wide security awareness
- Ensure that security activities are executed in compliance with established business strategy, security objectives and defined policies
- Review and propose budgets for security related initiatives to executive management for approval
- Identify and recommend how to handle non-compliance issues
- Approve methodologies and processes for security governance or security operations
- Identify significant changes of identified threat and/or vulnerabilities
- Assess the adequacy and efficiency of security controls and coordinate their implementation
- Promote security education, training and awareness throughout the organization
- Evaluate relevant information and defined KPI's received from the security operation team's detection processes
- Review security incident information and recommend follow-up actions

These tasks will lead to an effective, workable and evolving security strategy. Having a dynamic and adaptive mindset is extremely important as security strategies will evolve as the business grows and as threats continuously evolve and increase. New solutions and new methods come to market. New regulations will come and the organization need to be ready for them.

The JSMB communicates regularly on the tasks above to the executive management to update them on the current state of affairs.

Security Principle 001-34: *A joint security management board composed of senior business leaders across the organization should be established*

Security Principle 001-35: *The joint security management board is responsible for creating, delivering on the security strategy and measure its effectiveness*

Defendable Architecture Guideline

Developing an effective security strategy and architecture

5.2.3 Architecture review board



Parallel to the joint security management board but equally important to the governance of security is the architecture functions which sits at the heart of the technology units of the organization. The formalized decision body for all aspects of technology and architecture is the architecture review board (ARB). The Architecture Review Board serves as a governance body ensuring various technology initiatives align with the enterprise architecture and ultimately align with technology goals, strategies, and objectives.

Defining appropriate technology strategies and ensuring that project deliveries and development activities alignment with the objectives of those strategies is a continuous process and the main driver of the ARB function. The process is responsible for validating, recommending, and approving solutions and ensuring they are supporting the business goals along a set of defined criteria as per the technology strategy. Alignment is executed through a set of formalized review processes to manage outcomes, exceptions and the output and all decisions that will be cataloged as either formalized documents, or minuted decisions to support future decision making.

Since the ARB is the main body for approval of technical architecture in the organization and all final approval of changes and updates to architecture documents, including technology related security architecture. The ARB is an excellent meeting point to make sure that all the various initiatives that happens around in the organization is adhering to the defined security policies. All architectural decision shall be done in this forum as it have representatives from all parts of the organization including the information security team, and any other security specialists functions as required.

The architecture board is responsible for the following:

- Own architectural principles
- Own technology direction and strategy
- Review target architectures and approve relevant changes to it
- Review project deliveries and verify they are according to target architecture and architectural principles

Above should be defined according to:

- Business requirements

An ARB would include a dedicated security architecture responsibility and can thus can have proper overview on major changes broader than a single project scope and is able to ensure alignment within the different architecture domains.

Security Principle 001-36: *An architecture review board shall be in place to control changes in the security architecture.*

Security Principle 001-37: *Security architecture responsible shall be a part of the architecture review board*

5.2.3.1 Architecture change management

Changes in the architecture shall be made with ensuring that adequate level of security remains in place to support relevant business objectives. It needs identifying and addressing relevant risks and opportunities. Deviations from the adequate level of security are resulting in risks to business objectives that shall be identified and addressed. As threats and risks are changing by time, approved existing deviations shall be reviewed and followed up.

Security Principle 001-38: *Changes in the architecture must be linked to the risk management process.*

Security Principle 001-39: *The risk management process must include the assessment, evaluation and treatment of security related risks and opportunities.*

Defendable Architecture Guideline

Developing an effective security strategy and architecture

Security Principle 001-40: *Deviations must trigger the risk management process which requires a sign-off by the relevant line function which has authority over the costs of relevant risks.*

5.2.4 Information Security



The Security governance function is typically the information security office of the organization and is the formal policy owner of the security **architecture**. The formalization of this ownership should be defined in the mandate as given from senior management and the board which in turn are the formal owners of the security **strategy**. The security governance guidelines are technology agnostic, general and universal, and lay down the foundation and define what areas to cover. Infrastructure architecture principles and requirements are more

technology specific. They are still vendor & platform neutral and create blueprints for different solutions to meet security governance requirements. All aspects of information security guidelines are also the sole responsibility of the security governance unit.

Information security is responsible and accountable for the following within the security governance:

- Develop Information Security strategy
- Develop Information Security Policies and Manuals
- Develop Security KPI's
- Security Maturity and Definition
- Security Operations and Incident Response (through SOC and CSIRT teams).
- IR/DR/BCP plans

Above should be defined according to:

- Business Requirements
- Defined Risk Levels
- Security Intelligence (Internal and External)

These responsibilities above have dependencies on the input from the OAM and architecture teams to ensure value to the organization.

Security governance is also responsible for assisting the OAM teams and the architecture team with security intelligence, skills and other knowledge to ensure that the security strategy, policy and manual is implemented in the architecture globally supporting the organizational technology and business strategy.

As part of supporting the organization's business strategy, security governance will also support sourcing with input on requirements to secure commercial deliveries, and to follow up on strategic and contractual security KPI's for vendors to ensure the fulfilment of the organization's security policy through defendable architecture.

Security requirements is also required to be included in all contracts with vendors and suppliers that are providing products or services involving accessing or managing the organization's assets or information.

The vendors which are delivering products and services need to provide an adequate level of security within the contractually defined scope of the delivery. The organization, in the form of the information security unit is responsible for stating the necessary information security requirements based on identified risks or best practice. Any contractual documents will address how the vendor will guarantee that adequate security will be implemented, maintained and managed throughout the lifetime of the contract,

Security Principle 001-41: *Security shall be an embedded part of vendor management.*

Defendable Architecture Guideline

Developing an effective security strategy and architecture

Security Principle 001-42: Security requirements shall be included in contracts with vendors providing products or contracts for services involving accessing or managing the organization's assets or information.

Security Principle 001-43: Vendors delivering products and services to the organization shall provide adequate security within the scope of the delivery.

Security Principle 001-44: The organization is responsible for stating the necessary security requirements based on identified risks or best practice.

Security Principle 001-45: Contracts shall address how the Vendor will guarantee that adequate security will be implemented, maintained and managed through the contracts lifetime

5.2.5 Architecture & Planning



The Architecture & planning (AP) team creates standardized blueprints by taking the security requirements from security governance, combines them with technology strategy and requirements to provide functional high level designs and reference architectures as input to implementation projects or be the baseline for more detailed requirements in RFI/RFP processes

AP Team is the main responsible for the technology strategy and its implementation through target solution architecture and blueprints. For security architecture or blueprints the AP team is required to follow the organization's defined security strategy along with relevant policies, manuals and the requirement as stated within them.

AP are defined to have the following responsibilities and accountability with the security architecture, to develop:

- Target Architecture
- Technology & Infrastructure Strategy
- Architecture principles and requirements
- Standardized blueprints
- Functional requirements for use in projects and sourcing processes
- DR/BCP blueprints and solutions

Above should be defined according to:

- Security governance defined principles and policies
- OAM requirements and need
- Technology Strategy

The Architecture & planning teams have dependencies towards the operations and maintenance teams to get input on local strategies and business opportunities, and on information security to have an understanding of threats, requirements and risk toward the architecture and business.

Architecture also have the responsibility to provide input/information on strategy and objectives towards the information security and sourcing units to enable these functions to support the business objectives and develop their governance to be balanced and effective in supporting the future business of the organization.

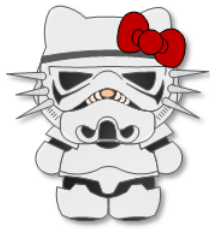
Detailed requirements both functional and technical security requirements is also required to be included in all contracts with vendors and suppliers that are providing products or services for the organization

The architecture and planning teams are responsible for stating the necessary technical security requirements based on identified risks or best practice to develop security controls and technical solution blueprints.

Defendable Architecture Guideline

Developing an effective security strategy and architecture

5.2.6 Operations & Maintenance



The operations and maintenance unit are those responsible for the main deliveries within the organization in the form of implementation, documentation and running the various functions and controls at the more detailed level. OAM teams create the low level solution level infrastructure architectural blueprints are more specific with additional details, but shall be compliant with the global principles and requirements, from both security governance and architecture.

It is the OAM teams that will execute and deliver the specific solutions from the blueprint to implement various parts of a defendable infrastructure. The operational experience of the OAM teams, provides excellent input to the governance, architecture and sourcing teams to ensure that policies, blueprints and requirements reflect reality, and are implementable and will do the job at hand. It is therefore expected that assistance on compliance issues on both policies and blueprints is given from governance and architecture if required, and that input on requirements are given from the OAM teams and security governance back to architecture to improve the quality of the designed controls and blueprints.

OAM and SOC teams also work closely together, both in sharing operational responsibilities for tools and infrastructure components used by the SOC team, but also directly cooperating during incident management providing detailed insight into the deployed infrastructure.

The OAM teams are those executing on and delivering the architecture and defined blueprints, and in the process of doing so, ensures that the defined security policies are fulfilled and in the process giving valuable input to the development of the security architecture by the architecture unit.

OAM teams are defined to have the following responsibilities and accountability with the security strategy, to own and/or develop;

- Low Level Detailed Design
- Execute on delivery projects
- Maintain the infrastructure through secure operations procedures (e.g. ITIL)
- Document and report on deviations from the defined architecture principles
- Support Incident Response

Above should be defined according to:

- Security governance, Architecture principles and technology strategy reflecting the organizations specific needs

OAM teams have dependencies with the responsibility towards security governance, architecture and sourcing to give input on needs and future plans so that Architecture, Sourcing Strategy and Policies are developed to support OAM teams service deliver and the future business of the organization.

5.2.7 Sourcing & Procurement



It might come as a surprise to many people, but commercial aspects of an organization also plays a major role in the security posture of the organization. The sourcing and procurement function (SP), are ensuring cost effective sourcing of the components and services necessary to implement a Defendable Architecture. Whenever something needs to be bought whether it is HW, SW or services, a process is started where the requirements for the functionality and the scope of the purchase is added. SP then normalizes bids, adds relevant penalties for risk and non-compliance from the different

vendors and then signs a contract with the bidder with the best price. It is paramount that the functional requirements for security that goes into every purchase is relevant and precise so that the components bought can be used in the way it is intended. Usually requirements are created by the architecture and planning teams with relevant support from OAM and/or IFS teams.

Defendable Architecture Guideline

Developing an effective security strategy and architecture

The SP function is defined to have the following responsibilities and accountability with the security strategy:

- Procure on Behalf of organization
- Negotiate commercial agreements
- Organize RFX Processes
- Develop sourcing Strategy

Above should be defined according to:

- Security Requirements
- Architecture Requirements
- OAM Requirements
- SOC Requirements

The SP unit have dependencies towards security governance, architecture and OAM teams to receive inputs to receive requirements supporting the technology, security and the BU's local strategies to realize the business goals of Telenor at best possible cost for value and quality.

5.2.8 Security Operations



The security operations teams are the eyes and ears of the organization in the security space. The main function of the SOC team is to protect the infrastructure and the confidentiality, integrity and the availability of the data either stored, processed or transported through it. In achieving this target is the role of the SOC needs to be considered in more detail, then the number of people and their competency and any specializations if applicable in the SOC and finally the process and procedures that are needed for a SOC to function properly. The exact roles and

responsibilities is determined by the overall security maturity of the organization as highlighted earlier as well as the size of the organization itself.

Monitoring and incident management can be considered to be the core responsibilities of the SOC. In the context of the security strategy ecosystem, the SOC is responsible for monitoring any security aspect of the organizations IT systems and other assets.

SOC teams are defined to have the following responsibilities and accountability with the security strategy, to own and/or develop;

- Perform security monitoring of all infrastructure assets
- Investigate indicators of attack and indicators of compromise
- Perform Incident Response on confirmed compromises
- Playbooks for incident response

Above should be defined according to:

- Security strategy
- Security policies and manuals
- Incident response plans

There is also an overlap with other parts of the OAM team, especially when it comes to issues of operations of the various tools and functions which the SOC may use in their daily work, which can be the shared responsibility of both the SOC team and the OAM team. As an example OAM teams may make sure that the firewalls are connected to the network and is functional properly but does not react to any security related alerts coming from it which is handled by the SOC team. Similarly the OAM team is responsible for maintaining the network tapping solution and uses it for operation debugging, but the SOC team is taking care of the security related usecases and ensures that 24/7 tapping of the network traffic of relevant assets takes place. SOC team frequently requires the assistance from the OAM team

Defendable Architecture Guideline

Developing an effective security strategy and architecture

during security incidents, gathering documentation or assisting with subject matter experts throughout the investigation phase.

5.2.9 Other non-decision making Forums

In large organizations there are usually several other collaboration arenas established, that doesn't necessarily have decision authority, but which acts as advisors to those decision bodies that do. These forums may either be formalized sub-forums to the decision bodies and act as their advisors and provide recommendations to formal decisions or they can be of a more informal nature, but act as regular meeting arenas to address a particular cross domain challenge, or the sharing of ideas.

5.2.9.1 Architecture Forums

These are the formal sub forums to the architecture review board for technology functions. All cases going to the review board for formal approval needs to pass the architecture sub-forums and be endorsed and approved by a majority of the participants. Any development of, or changes to, architecture that may impact also impact security architecture is to be raised, discussed and approved in this forum, prior to presentation in the architecture review board.

5.2.9.2 Coordination Forums

A coordination forum is where the different units and functions meet to share information and coordinate actions where there are conflicts, incidents or where a shared view need to be established. This forum should be small and include only stakeholders and resources directly involved in the different topics. There are assumed to be several of these forums, where the different functions meet to collaborate. It may be technology and sourcing units discussing vendor strategy, it may be security and technology discussing implementation planning or the operations teams collaborating on a challenge

The forums should be owned by department mandated leads, typically VP position or equivalent. As shown in the governance model described above and displayed in **Figure 11**, the recommended setup is to have a forum for each of the arrows connecting the functions and which indicate regular collaboration between the two functions. Having regular meeting arenas give transparency into ongoing activities that may have relevance or impact to neighboring functions.

5.2.9.3 Vendor Management forum

While the contractual security obligations of the suppliers are handled by the information security and sourcing teams vendor management is also an important part of the development for the development of security architecture and the design of security controls. The technology aspects of security are developing at a very rapid pace with a lot of innovation, and its required to regularly update the insight into this area by regularly interacting with relevant vendors.

This should be done in a suitable forum with the responsibility to:

- Develop the vendors security capability to support the security architecture
- Arrange technology workshops and roadmap sessions to inform on new developing technology and the capabilities of the suppliers in current vendor landscape
- Escalation of security and technical shortcomings or issues
- Inform the vendors on the organization's strategy and vision for technology and security
- Establish a secure and KPI based way of work for governance

The vendor management forum would, depending on the vendor size and criticality for the organization, typically be set up in a tiered fashion similar to the security governance model explained earlier. The organizations' subject matter experts and architects would engage with the suppliers' counterparts to

Defendable Architecture Guideline

Developing an effective security strategy and architecture

look at technical details, roadmap development or other technical issues. In case of escalations or business strategic discussions, the organization and the supplier have their own separate forums to discuss matters of strategic importance between the two entities. CEO's would not sit down and discuss software bugs, but rather strategic relation building and mutual business strategy.

5.3 Documentation

A fact that cannot be stressed enough, is that documentation is extremely valuable across all levels of the organization. Not only to bring a common understanding of architecture, designs, and solution across multiple functional but also during an incident response where the CSIRT and SOC teams needs to understand how various HW and SW components are put together and the thought processes behind it. Armed with good documentation and an understanding of the affected systems and the underlying infrastructure they are deployed on, the response teams can best fight the ongoing battle with a threat actor that have managed to breach the outer defenses.

Documentation becomes even more critical when the day-to-day operations of infrastructure or systems have been outsourced in whole or in parts. The relative "distance" to the operational resources makes it harder to communicate or to extract relevant information as internal operative resources may not have been involved in the setup of the solutions. The lack of direct local involvement makes a successful incident response much more complicated and less efficient.

For this reason all documentation relating to the relevant parts of security strategy and security or technology architecture are the responsibility of each governance function that are directly involved at their level

5.3.1 Information Security team

The information security team are responsible for drafting and developing policies and manuals governing information security or physical security as well as drafting the security strategy before they are sent to the JSMB for review and alignment with other parts of the business. The information security team is responsible to update, maintain and making available:

- Organization top level security policy
- Information security and physical Security policy and manuals

It should be noted that these documents will be valid and in force when reviewed and approved by the relevant strategic decision bodies such as the board of directors for any organization top level policy, or the JSMB for security policies and manuals

5.3.2 Architecture team

The architecture team's main tasks are drafting and developing technology strategies, standardized blueprints and architectural principles. As part of this process the architecture team is responsible to update, maintain and making available:

- Architectural principles
- Formalized technical documents outlining and defining the approved target architecture for various technical domains
- Defined technology strategy

Other relevant documents supporting the operational units in the execution of implementing the security architecture such as guideline documents on specific solutions or implementation scopes may also be within the responsibility of the architecture team.

Defendable Architecture Guideline

Developing an effective security strategy and architecture

It should be noted that these documents should only be valid and in force as official documents after being reviewed and approved by the architectural review board.

5.3.3 Operations and Maintenance

OAM teams are responsible to develop, maintain and on request making available;

- High Level Designs and blueprints
- Low Level Designs and blueprints
- Network drawings and communication diagrams related to the implantation of systems
- Documentation of implemented security controls

Other documents not mentioned above that are part of the security architecture, and/or supporting Incident Response, may also be required to be developed, and maintained by the OAM teams.

5.3.4 Security Operations

There is a long list of things that security operations team is responsible for and needs to do properly so that the organization's assets and data are protected and threat actors are detected and evicted as quickly as possible with minimal impact. To do this, the SOC teams needs to create and document the overall processes for detection and incident response along with specific procedures and detailed technical playbooks for the different types of incidents.

- Security Incident response plans
- Playbooks
- Procedures

The documented processes and in particular the playbooks becomes extremely valuable and a necessity if trying to automate the security response capabilities later.

5.3.5 Sourcing and procurement

The sourcing unit needs to develop and document the strategy and corresponding roadmaps that are required for security related technology and services vendors that are deliver the necessary components to design and implement the security controls as defined by the security architecture. After a frame agreement is negotiated with a vendor, price books should be maintained for the products and services in scope. Insight into these price books should be limited though, since knowledge about the actual products and technologies that are used to design and build certain key security controls in an organization, can be very valuable for a threat actor that can use the information to exploit weaknesses to evade the deployed controls. This applies in particular for detection controls.

Sourcing and procurement unit is responsible to document, update, maintain and make available on request:

- Sourcing strategy related to, and roadmaps from vendors providing security related technology and services
- Price books for security capabilities that are included in the security architecture
- Other documentation e.g. contracts and annexes may be included in the above on a need basis for audit, KPIs or other purposes.

5.3.6 Strategic governance bodies

The decision bodies of the executive and senior management also have a job to do when it comes to produce documentation of their activities at the strategic level. Meeting Minutes and support documents for decisions should be used for action tracking, reporting and accountability. This

Defendable Architecture Guideline

Developing an effective security strategy and architecture

documentation does not necessarily become public but is relevant for backtracking, compliance or internal or external audits.

- Public parts of the business, security or technology strategies
- KPIs and progress reports related to the implementation of strategies
- Meeting minutes and supporting memos for decisions

The security strategy in its entirety is not meant for widespread public distribution in the organization but the non-confidential parts of it, such as mission statements or security objectives should be clearly communicated so it is well-known throughout the entire organization and not only inside the security organization and its immediately connected neighboring units. KPIs and progress from the reports is also a good idea to make public to showcase for the organization that security both is important and that it is working

6 Definitions, Abbreviations and Legend

6.1 Definitions

This document adheres to requirement definitions as described in [RFC 2119](#):

Term	Synonym(s)	Meaning
MUST	REQUIRED, SHALL	The definition is an absolute requirement of the specification.
MUST NOT	SHALL NOT	The definition is an absolute prohibition of the specification.
SHOULD	RECOMMENDED	There may be valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood, documented and carefully weighed before choosing a different course.
SHOULD NOT	NOT RECOMMENDED	There may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood, documented and the case carefully weighed before implementing any behavior described with this label.
MAY / OPTIONAL	OPTIONAL	An item is truly optional.

Table 4. Definitions

6.2 Abbreviations

Abbreviation	Full Term
AP	Architecture & Planning unit
ARB	Architecture Review Board
BCP	Business Continuity Planning
BOD	Board of Directors
CIA	Confidentiality, Integrity, Availability
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CMP	Cloud Management Platform
CSF	Cyber Security Framework
CSIRT	Cyber Security Incident Response Team
DA	Defendable Architecture
DP	Disaster Prevention
DR	Disaster Recovery
EVP	Executive Vice President
HLD	High Level Design
HR	Human Resources
HW	Hardware
IFS	Information Security unit

Defendable Architecture Guideline

Developing an effective security strategy and architecture
















IR	Incident Response
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Standards Organization
IT	Information Technology
JSMB	Joint Security Management Board
KPI	Key Performance Indicator
LAN	Local Area Network
LLD	Low Level Design
NFVi	Network Functions Virtualization Infrastructure
NIST	National Institute of Standards and Technology
OAM	Operations and Maintenance
PASTA	Process for Attack Simulation & Threat Analysis
RFI	Request for information
RFP	Request for
RFx	Request for X (relevant commercial process)
SOC	Security Operations Center
SP	Sourcing and Procurement
SVP	Senior Vice President
SW	Software
TTP	Tactics, Techniques, Procedures
VP	Vice President

Table 5. Definitions

Defendable Architecture Guideline

Developing an effective security strategy and architecture

6.3 Legend

 Component associated with Exposed Service Class	 Component associated with Access Management Class	 Component associated with Legacy environment	 Component associated with Service Domain
 Component associated with Non-Exposed Service Class	 Component associated with Service Management Class	 Component associated with uncontrolled environment	 Component associated with Management Domain
 Component associated with Secure Service Class	 Component associated with Platform Management Class		 Component associated with EUC Domain
 Component associated with In-Band Management of Secure Service Class	 Component associated with Device Management Class		
 Component associated with In-Band Management of Secure Service Class			
 Component associated with In-Band Management of Secure Service Class			

 Baremetal Workstation	 Physical Firewall	 Linux Host OS	 IDS/IPS Sensor	 NTP Function
 Baremetal Server	 Virtual firewall	 Windows Host OS	 Log Event	 DNS Function
 Virtual Workstation	 Web Application (L7) Firewall	 Application	 Log Forwarder	 Active Directory
 Virtual Server	 Router	 API Function	 Network Traffic Tapping Function	 Copper based Network Port
 Hypervisor	 Virtual router or Routing domain (vrf)	 Protective Software Agent	 Network Traffic Flow Data	 Fiber based Network Port
 X86 Based Hardware	 Layer 2 switch	 Detective Software Agent	 Vulnerability Scanner	 Webportal
 ARM Based Hardware	 Virtual Layer 2 switch or Virtual LAN	 IR Forensics Software Agent	 Policy	 Multi Factor Authentication
 RISC based Hardware	 Physical Load Balancer	 Session Manager	 Access Gateway	 Secure Credential Vault
 Storage Device	 Virtual Load Balancer	 Base Station	 AI Capability	 Session Recording Functions
 Backup Device	 Network Security filtering function	 Wireless Access point	 Intelligence feed	 Identity & Access Management

 Tier 6 Threat Actor	 Tier 3 Threat Actor	 Disaster Level Incident	 Incident Response Team	 Advanced Persistent Threat	 Application Developer
 Tier 5 Threat Actor	 Tier 2 Threat Actor	 Major Incident	 Security Operations Team	 Platform Operator OAM Team	 3rd party tenant Operator
 Tier 4 Threat Actor	 Tier 1 Threat Actor	 Minor Incident	 Managed Services Provider	 Business User	 3rd party guest Business user
 Architecture Unit	 Information Security Unit	 Sourcing Unit	 Vendor or supplier	 Manager	 Senior Manager

Table 6. Legend

7 List of references

- [1] Francesco Cipollone, [Defining a Security Strategy](#)
- [2] László KOVÁCS, [National Cyber security as the cornerstone of national security](#)
- [3] Center for Internet Security, [v7.1 of CIS controls](#)
- [4] NIST, [Cyber Security Framework](#)
- [5] Tucker Bailey, Josh Brandley, and James Kaplan, [How good is your cyber incident-response plan?](#)
- [6] Secuvant, [Implementing CIS Controls and benchmarks](#)
- [7] Abi Tyas Tunggal, Upguard, [What are the CIS Controls for Effective Cyber Defense?](#)
- [8] Wisegate, [5 Essential steps for developing a security strategy](#)
- [9] Brian Krebs, KrebsOnSecurity, [Whats Your Security Maturity Level](#)
- [10] US Department of Defense, [Cybersecurity Maturity Model Certification](#)
- [11] Michael R. Brown, [Security Maturity Models](#)
- [12] Tara Seals, Infosecurity Magazine, [NIST, CIS Security Frameworks See Mainstream Adoption](#)
- [13] Charles Lim, [ICION 2016 - Cyber Security Governance](#)
- [14] Compliance Council, [ISO 27001 vs NIST Cybersecurity Framework](#)
- [15]

8 List of directional statements

In this section, all the key objectives of this document are summarized in the form of principle statements and observations.

8.1 Summarized Security Principles

Security Principle 001-1: *The information security management system shall act as a framework for the organization security strategy and its implementation*

Security Principle 001-2: *The information security management system shall be scoped based on ISO27001*

Security Principle 001-3: *Areas in the ISMS which are heavily dependent on technology related controls more than policies, should be considered to have the development of those areas delegated to the technology division under the oversight of information security governance functions*

Security Principle 001-4: *The security strategy needs to be a continuous process that is able to identify all critical assets, prevent them from attack, detect threat actors attacking the assets, respond to incidents caused by threat actors or natural events and be able to recover from them*

Security Principle 001-5: *Security strategy should be realistic and balanced between security, quality and price effectiveness and be based on a threat and risk based methodology addressing the requirements of the organization*

Security Principle 001-6: *The external security threats to the organization must be acknowledged and understood*

Security Principle 001-7: *The internal security threats posed by inappropriate use and lack of awareness must be acknowledged and understood*

Security Principle 001-8: *The consequences of a security threat to the organizations assets must be acknowledged and understood*

Security Principle 001-9: *The capabilities and limitations of existing protection measures must be acknowledged and understood*

Security Principle 001-10: *The likelihood of vulnerabilities being exploited by external threats must be determined*

Security Principle 001-11: *The likelihood of vulnerabilities being exposed by inappropriate use must be determined*

Security Principle 001-12: *The security and business impact of any individual or combination of vulnerabilities being exploited must be determined*

Security Principle 001-13: *Overall security strategy and information security management system shall follow the ISO27000 framework*

Security Principle 001-14: *Defendable Security architecture, scope, design and implementation of controls shall follow the CIS20 framework*

Security Principle 001-15: *Security controls relevant for the security architecture not addressed by CIS20 should follow NIST CSF*

Security Principle 001-16: *CIS control implementation and priority shall be based on overall risk assessment process outputs*

Security Principle 001-17: *Security Architecture framework should document relevant basic and foundational CIS controls as defined by the security strategy*

Defendable Architecture Guideline

Developing an effective security strategy and architecture

Security Principle 001-18: security control design prioritization and implementation shall be based on a risk assessment process and gap analysis to be as effective as possible

Security Principle 001-19: Security protection, detection and access security controls shall be designed to deliver on CIS control objectives

Security Principle 001-20: a business driven and threat intelligence driven design process shall be applied when designing security controls

Security Principle 001-21: Security controls shall be interlinked and overlapping to support defense in depth but still modular to be implemented individually

Security Principle 001-22: Methodologies shall be developed to measure the effectiveness of designed and implemented security controls

Security Principle 001-23: Processes for continuously developing security controls and roadmaps for implementing them shall be created and maintained

Security Principle 001-24: Process support and competency areas are required to be developed for each defined security controls and capability

Security Principle 001-25: Architecture development should be according to clearly defined priorities as per established strategy

Security Principle 001-26: Suppliers of technology for security controls used in critical information infrastructure shall be vetted against any regulatory constraints

Security Principle 001-27: Incident response plans, disaster response plans and business continuity plans shall be created and practiced on regular intervals

Security Principle 001-28: Incident response plans, disaster response plans and business continuity plans should be an integrated response plan and development process

Security Principle 001-29: All Applications and services shall be classified and have tolerance levels applied to them for availability, acceptable data loss, and recovery time

Security Principle 001-30: A security maturity evaluation framework shall be created

Security Principle 001-31: Security maturity shall be evaluated regularly and no less than 1 per year

Security Principle 001-32: Security governance shall be clearly defined with roles and responsibilities

Security Principle 001-33: Formalized decision bodies shall be established within the different tiers of the organization with a clear mandate and the empowerment to execute on decisions made

Security Principle 001-34: A joint security management board composed of senior business leaders across the organization should be established

Security Principle 001-35: The joint security management board is responsible for creating, delivering on the security strategy and measure its effectiveness

Security Principle 001-36: An architecture review board shall be in place to control changes in the security architecture.

Security Principle 001-37: Security architecture responsible shall be a part of the architecture review board

Security Principle 001-38: Changes in the architecture must be linked to the risk management process.

Security Principle 001-39: The risk management process must include the assessment, evaluation and treatment of security related risks and opportunities.

Defendable Architecture Guideline

Developing an effective security strategy and architecture

Security Principle 001-40: Deviations must trigger the risk management process which requires a sign-off by the relevant line function which has authority over the costs of relevant risks.

Security Principle 001-41: Security shall be an embedded part of vendor management.

Security Principle 001-42: Security requirements shall be included in contracts with vendors providing products or contracts for services involving accessing or managing the organization's assets or information.

Security Principle 001-43: Vendors delivering products and services to the organization shall provide adequate security within the scope of the delivery.

Security Principle 001-44: The organization is responsible for stating the necessary security requirements based on identified risks or best practice.

Security Principle 001-45: Contracts shall address how the Vendor will guarantee that adequate security will be implemented, maintained and managed through the contracts lifetime

8.2 Summarized Observations

Observation 001-1: An Information Security Management System gives the organization the ability to recognize the full range of risks that the organization or its data may encounter in a short to medium time frame and is a pre-requisite for implementing the relevant mitigating measures in the form of security controls

Observation 001-2: Making the technology units accountable and responsible for security in all the development, project deliveries and line functions within their scope of responsibility while measuring progress, effectiveness and security maturity is an excellent catalyst and a major step in making security embedded into all aspects of the organization

Observation 001-3: Security functions can be outsourced for cost efficiency, accountability can not.

Observation 001-4: Security response plans are sometimes also referred to as playbooks, and well-defined playbooks for security incidents are key for automating the response process which again is a must to maintain an effective security operations.

9 Document history

Document version	Version description	Version Responsible	Date
0.1	Inception	Erik Kvarvåg	14.05.2020
0.4	First Completed Draft	Erik Kvarvåg	03.07.2020
0.5	First, peer review	Erik Kvarvåg	14.07.2020
0.8	Second draft, feedback incorporated	Erik Kvarvåg	23.07.2020
0.9	Second, public review	Erik Kvarvåg	01.08.2020
1.0	Final version	Erik Kvarvåg	04.08.2020
1.01	Minor update	Erik Kvarvåg	xx.xx.2020
1.1	Major update	Erik Kvarvåg	xx.xx.2020

Appendix 1. Further development and Next Steps

The defensive capabilities have be organized differently as opposed to earlier distributions of the defendable architecture framework. They are now organized into 3 main areas and a set of capabilities in total. Each volume of the defendable architecture documents highlights one more of the capabilities within each of the documents.

A1.1 Updates for next major version

Map CIS20 Sub controls to relevant DA documents and specific sections.