Check Point Enterprise Security Framework Version 2

Published by the Check Point Strategic Consulting Group

March 2023

YOU DESERVE THE BEST SECURITY

Synopsis

This document details how the Check Point Enterprise Security Framework Version 2 can be used and includes scope, audience, and methodology. The paper is public and intended for cyber security leaders, architects, engineers, and stakeholders. No prior knowledge is required other than familiarization with the related documentation.

Author(s)	JP Edwards, Enterprise Security Architect
Contributors	Check Point Enterprise Security Architecture Team

Status: Published

Date	Status	Author	Comments
30/01/2023	Release	JP Edwards	Version 7.1

Related Documentation

Section	Title
CESF	https://www.checkpoint.com/support-services/security-workshop/

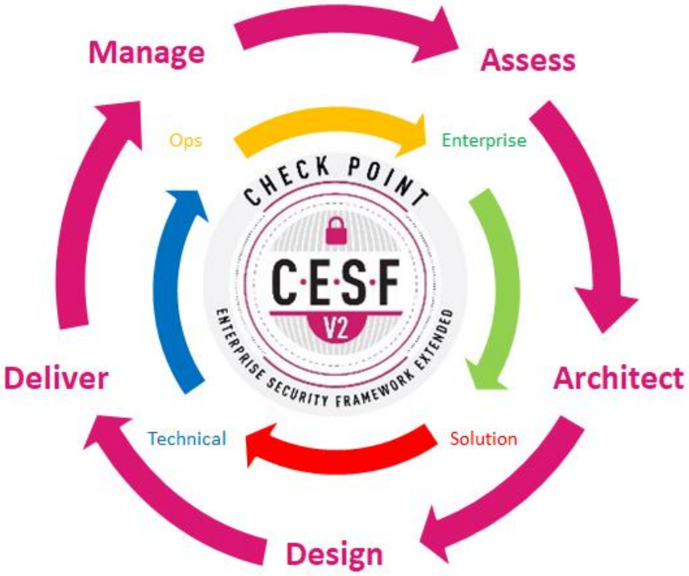
Contents

Executive Brief

Following the release of our first Check Point Enterprise Security Framework in 2019 and its widespread adoption throughout our architectural and engineering communities, constructive feedback has enabled us to compile a new and improved version. This version addresses the changing architectural landscape and aligns with a **risk-based consultative approach to cyber security**. Please note that the following paper supplements the Check Point Enterprise Architecture whitepaper.[1]

Our first CESF version was based on a process-led concept for security architecture development. In our latest version (CESFv2), we have introduced a governance and risk-led approach, which reflects the requirement to align architecture with impact, threat, and vulnerability analysis.

> ***"As a framework, CESFv2 uses qualitative analysis and a cross-functional approach to improve the efficiency and effectiveness of cyber security recommendations and advice."***



CESFv2 focuses on updates in the following core areas:

Leadership: CESFv2 includes features designed to support the C-suite in making more effective and efficient cyber security decisions and managing cyber security risks.

Risk-focus: CESFv2 supports using multiple assessment frameworks, such as NIST CSF, for control-based compliance and risk assessments.

Governance: CESFv2 has a built-in method to build governance and policy frameworks.

Strategic advisory and consulting: CESFv2 is cross-functional and supports the development of cyber security strategies delivered through the advisory and consulting approach.

Operations: CESFv2 defines operational roles, responsibilities, and the development of target operating models.

Delivery: The core delivery vehicle for CESFv2 is the **security workshop**, explicitly designed to focus on strategic cyber security discussions and cyber security risks.

What's New

Academic work, including cyber security frameworks, evolve the more they are tested in the real world. The CESF process is no different. Since its conception, the original framework has been continuously tested in live

[1] https://www.checkpoint.com/downloads/products/checkpoint-enterprise-security-framework-whitepaper.pdf[1].

environments. Based on data collected from real world use of our framework, we've been able to make improvements designed to provide enhanced support to our customers' leadership, architects, engineers, and operational teams.

We hope the enhancements have resulted in a more efficient and effective enterprise security framework. One that is agnostic at the point of use, more adaptable in its applications, more effective in delivering enterprise security architecture, and has a broader appeal and audience.

Below is a high-level list of the significant new components and their focus. We've worked hard to ensure that CESFv2 reflects the need within organizations to work in a cross-functional manner whereby multiple teams are stakeholders in the overall security posture, which is why each feature maps to a relevant audience.

Audience	New Features
Leadership	Strategic Consulting and Advisory / CISO Services
	Zero Trust Advisory
	Enhanced Cloud Transformation
	Cyber Security Risk Management and Consulting
Architecture	SABSA-Based Enterprise and Solutions Architecture
	NIST 1800-35 Zero Trust Architecture
	Check Point & CISA Zero Trust Architecture
	Automation and DevOps Code-Level Consultancy
Governance, Risk, and Compliance	NIST CSF Assessment
	CISv8 IG1,2,3 Assessments
	NIST 800-53 and RISK Management Frameworks
	NIST 800-82R2 - Industrial Control Systems (ICS) Security
	CISA Zero Trust Maturity Assessment
	MITRE Attack Modelling and Reverse Attack Mapping Using CIS-to-MITRE
	CCM Assessment (or cloud security assessments)
Operations	Target Operating Models (TOM) and Operational Architecture

Introducing CESF Version 2

The original CESF fulfilled the role of supporting architects engaged in cyber security architecture. In CESFv2, we broadened the scope by including support for GRC and cyber security leaders with services and features, such as cyber risk and control-based assessments.

The goal is to increase the effectiveness of the overall CESF process through a better understanding of the people, processes, and technology that make up our clients' security capability. In addition, we hope to deliver more informed advice and recommendations by increasing our knowledge of these components.

"The core new attributes for CESFv2 are the use of focused information gathering through RISK and CONTROL-BASED ASSESSMENTS, and the introduction of layered contextual information designed to support a cross-functional CYBER SECURITY STRATEGY."

This framework aims to empower the enterprise's cyber security conversation by applying the lens of governance frameworks, such as NIST CIS, combined with industry-standard risk assessments the output of which will support decision-makers looking to deliver real world solutions for real world risks.

We maintain that a solid understanding of cyber security risk is a powerful vehicle to affect change, ultimately leading to a more robust cyber security posture.

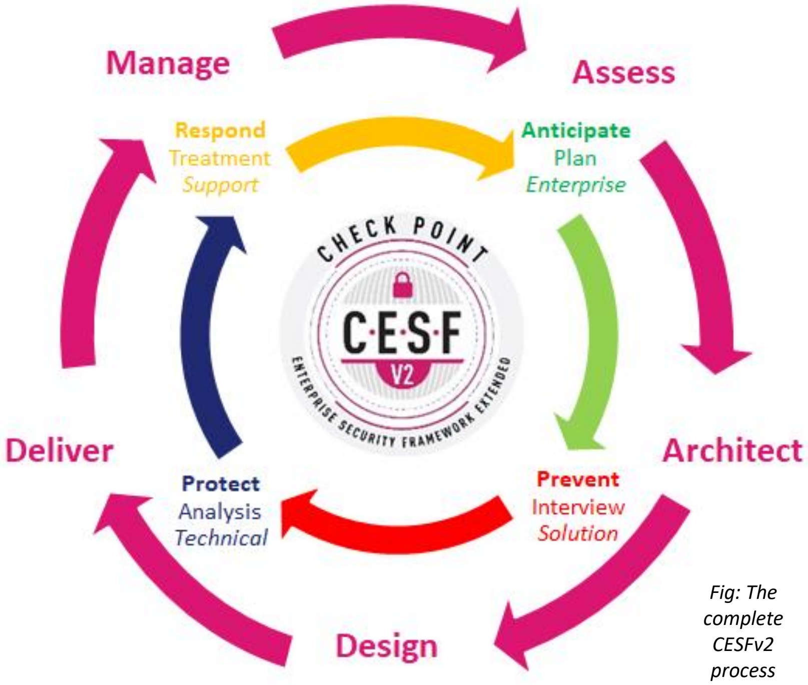


Fig: The complete CESFv2 process

We hope that through this paper, the audience will understand how and why to apply the CESFv2 process and how the framework can support improvements and change.

Key Drivers

We're proud to present the following new feature benefits:

- **Improved communication:** The language of risk is universally understood inside and outside of cyber security; using this commonality enhances our communication with C-suite and governance teams. In our experience, risk-based conversations reach a wider audience than those focused only on technology.

- **Business-focused approach:** Building a successful cyber security strategy today starts with a firm understanding of the business impact and cyber security risk before technology. CESFv2 focuses on understanding these core business concerns better so that decision-makers can make more informed and effective technology/product choices.

- **Top-down process**: All architecture, including enterprise security architecture, must follow a process, which is why CESFv2 has, at its core, a clearly defined **top-down** approach. The process starts with senior stakeholders but will capture the goals and requirements at multiple levels – each of which has an essential voice in the cyber security conversation. A significant influence on CESFv2 is the **SABSA** framework[2] , which we have heavily adapted to reflect our intended use. The table below shows the various layers of the cyber security conversation and there relevant discissions

The Cyber Security Conversation	
Business View	Contextual Discussion
Architect View	Conceptual Discussion
Engineer View	Logical Discussion
Builder View	Physical Discussion
Operations View	Security Services Management Discussion

- **Strategic engagement plan:** Good planning improves outcomes, which is why we've integrated the concept of SABSA layers into our CESFv2 process and aligned these with different stakeholders. We'll explore this alignment in detail through this paper; however, for now, we invite the reader to acknowledge the alignment and recognize its influence on our cross-functional methodology in which each organizational role is represented.

View	*SABSA Layer*	What (assets)	Why (motivation)	How (process)	Who (roles)
Business	*Contextual*	Business Goals, Processes, and Objectives	Business Risks and Impact	Risk Assessment	CIO, CISO, Security Officers
Architect	*Conceptual*	Business Knowledge and Risk Strategy	Gaps, Current State, Maturity, and Architecture	Security Framework and Modelling	Security Architects
Engineer	*Logical*	Informational Assets	Security Policies	Security Design	Security Experts
Builder	*Physical*	Security Policies	Security Design and Architecture	Security Technologies	Security Engineering
Operations	*Management*	Security Assets	Security Posture	Security Operations	Operations and Analysts

- **Assessment and RISK focus:** CESFv2 makes significant use of public control libraries such as NIST and CIS alongside industry-established cyber risk assessment practices. When combined with a solid

[2] https://sabsa.org/sabsa-executive-summary/

understanding of cyber security architecture and practical knowledge of implementation, the result is often a powerful tool to reduce overall risk and support the overall cyber security strategy.

- **Cross-functional capability:** Cyber security is a shared responsibility in any organization. The lines between those who are accountable, responsible, consulted and informed on cyber security decisions is often complex, which is why CESFv2 is designed so that different teams can interact with the overarching process in the most appropriate format. The example below shows how roles and responsibilities are aligned to various stages in the CESFv2 process.

Audience			
GRC and C-suite	**Architects**	**Operational**	**Assessors and Auditors**
GRC teams and those leadership functions that are looking to use the CESFv2 to help develop Governance models.	Enterprise, solution, and technical architecture teams looking to follow a SABSA-based process for security architecture.	Ops and incident teams developing workflow and processes for changes and incident handling.	Teams looking to perform control-based assessments based on known libraries such as NIST or CISv8.

Operational Model

In the previous section, we highlighted the influence of the SABSA framework on the development of both CESF and CESFv2. In this section, we introduce the mapping of these layers to the CESFv2 layers of assess, architect, design, deliver, and manage. The design decision behind the layered approach is to make the CESFv2 framework cross-functional in its application, meaning, the framework must allow different teams, both customer and Check Point, to complete different activities at different layers of an overall top-down process.

In order for the framework to be followed correctly it must start with some type of assessment and analysis. This ensures a solid dataset that acts as a foundation from which the correct architecture and cyber security decisions are drawn. The top-down approach doesn't work if the first layer is omitted.

The table below shows how the various CESF core layers are mapped to a defined process and the relevant stakeholders.

View	CESFv2 Layer	Activity	Customer	SMB / SME	Enterprise	Delivery Vehicle
Business	**Assess**	Business Goals, Security Assessment, Zero Trust Maturity, Cyber Risk Analysis	CISO / CIO / Directors	**Regional Architect / Security Engineers**	**Global Enterprise Architects /** **Field CISO**	**Security Workshop**
Architect	**Architect**	Gap Analysis, Architecture and CIS Review	Security Architects			
Engineer	**Design**	High-Level Design, Target Architecture, Technology / Products Mapping	Lead Engineers and Design Team	**Security Engineers**	**Security Engineers**	
Builder	**Deliver**	Low-Level Design and Configuration	Implementation Engineers	Professional Services Incident Response and Account Management		Security Services
Operations	**Manage**	Security Services	Operations and SOC Teams			

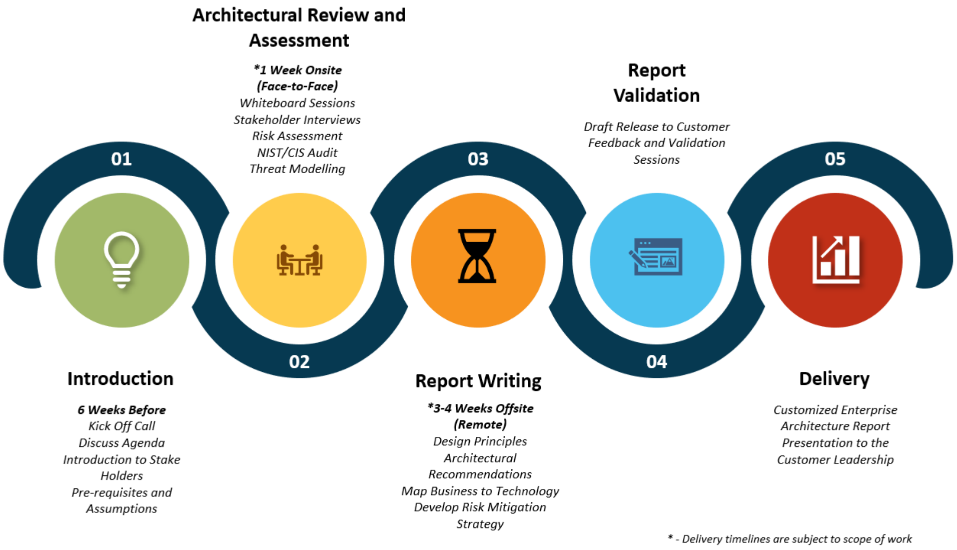
Security Workshops

The quality of the data collected through the CESFv2 process is essential, which is why, where possible, we always try and make sure the program includes some face-to-face workshop elements. These encourage an open-forum debate and collaboration. While each engagement is different and designed around clients' requirements, there are some general workshop focuses depending on where we are in the overall process.

The workshop will take a different form depending on the CESFv2 phase, as described in the table below.

CESFv2 Phase	Workshop Focus
Assess	Business risk-based discussion with CIO/CISO, interview and evidence gathering, business impact, vulnerabilities, likelihood of a significant cyber event, threats, attack profiles, compliance, governance, risk.
Architect	Whiteboard, conceptual discussion, controls gap analysis, design review, target and desired state, Zero Trust design principles, enterprise security architecture, mitigation.
Design	Product and component presentations and design focus, Zero Trust components, solutions architecture, HLD.
Deliver	Configuration and implementation discussions, technical architecture, LLD.
Manage	Incident response, operational management, operating models, MDR, PS.

We would also like to draw attention to the general chronology of engagements to highlight that the workshops' primarily focus on data gathering instead of presenting solutions. Doing so allows for the correct level of detail to be collected and for analysis to be done post-workshop.



01
Introduction
6 Weeks Before
Kick Off Call
Discuss Agenda
Introduction to Stake Holders
Pre-requisites and Assumptions

02
Architectural Review and Assessment
1 Week Onsite (Face-to-Face)
Whiteboard Sessions
Stakeholder Interviews
Risk Assessment
NIST/CIS Audit
Threat Modelling

03
Report Writing
3-4 Weeks Offsite (Remote)
Design Principles
Architectural Recommendations
Map Business to Technology
Develop Risk Mitigation Strategy

04
Report Validation
Draft Release to Customer
Feedback and Validation Sessions

05
Delivery
Customized Enterprise Architecture Report
Presentation to the Customer Leadership

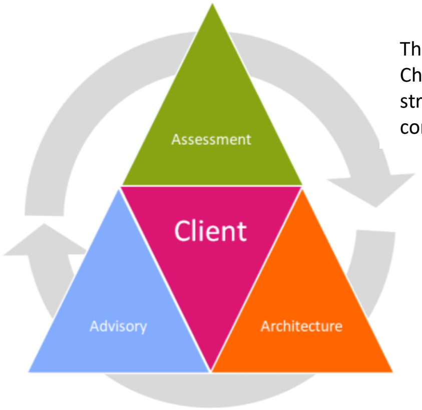
** - Delivery timelines are subject to scope of work*

Advisory, Assessments, and Architecture

Context helps, which is why we have included a section explaining who, where, and how the framework was developed and some of the supporting components derived from its use. Currently, the CESFv2 framework is used throughout the Check Point community, where a process is required to design, deliver, and support cyber security solutions and leadership. It is owned and maintained by the Check Point Enterprise Security group, for whom it represents the foundational guidance for all our work.

The Check Point Strategic Consulting group has made conscious improvements to the framework since its initial conception. We remain committed to ensuring the framework remains a high-level conceptual framework that can be interpreted and applied in multiple different scenarios depending on need, and that it acts as a foundation for other more technical or lower-level models.

Our consulting approach is driven by three CESF pillars: *Assessment, Architecture,* and *Advisory*. Each can be used in the CESFv2 process to help communicate concepts to customers, explain processes and methodologies, and ensure traceability and accountability. More information about these services can be found at https://www.checkpoint.com/support-services/security-consulting/.



The 3 "A" of Check Point strategic consulting

"The goal of strategic consulting is to perform advisory, assessment, and architectural work for, and on behalf, of our customers. We advise on all matters relating to cyber security, making assessments of the current security state and architecture to address gaps and improve overall posture."

While CESFv2 defines the methodology and principles used to help achieve certain cyber security goals, we also maintain that the process can effectively link leadership, architectural, and engineering teams in a common understanding of the "as-is" and "to-be." cyber security architecture In other words, using the features contained in the CESFv2 framework, architects, consultants, and advisors are better able to "glue" customer and business requirements to technology choices and thereby improve the efficiency and effectiveness of the cyber security program.

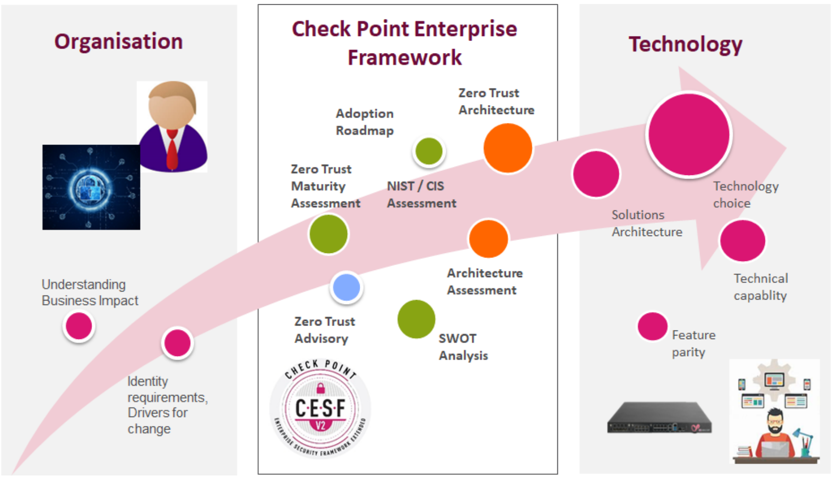
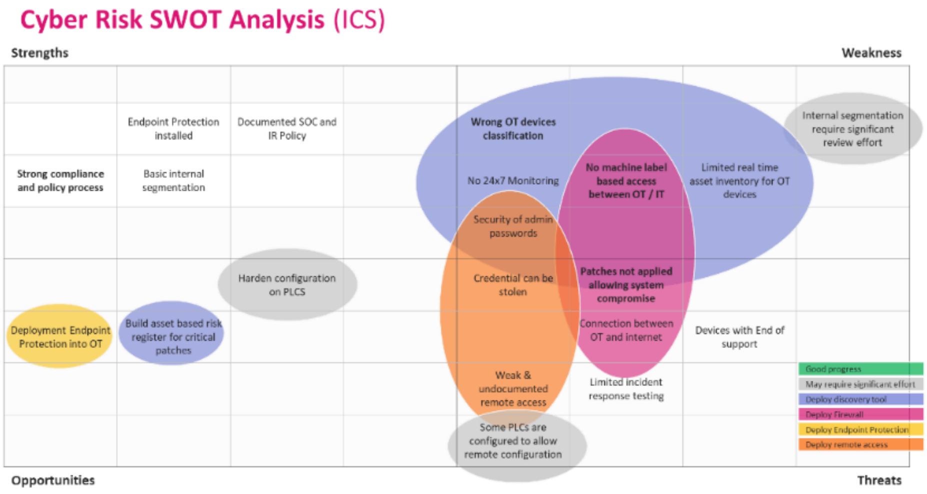


Fig: CESFv2 providing the linkage between business objectives and technology choices

In creating CESFv2, we wanted to increase the overall value that could be derived from following our process and therefore explored how different presentations and visualizations could complement the outcome. Since we're confident the new process will deliver better data inputs and outputs, we wanted to explore new ways to present the data.

Some of these new visualizations are described here:

Cyber Security SWOT analysis: We borrowed the SWOT (strengths, weaknesses, opportunities, and threats) analysis format and applied it to our work in cyber security. This visualization presents the internal and external issues identified as part of the assessment alongside our recommendations in a single view. It's a powerful single-page view we often use as part of an executive summary.


Cyber Risk SWOT Analysis (ICS)
Strengths
Weakness
Endpoint Protection installed
Documented SOC and IR Policy
Strong compliance and policy process
Basic internal segmentation
Harden configuration on PLCS
Deployment Endpoint Protection into OT
Build asset based risk register for critical patches
Wrong OT devices classification
No 24x7 Monitoring
No machine label based access between OT / IT
Limited real time asset inventory for OT devices
Internal segmentation require significant review effort
Security of admin passwords
Credential can be stolen
Patches not applied allowing system compromise
Connection between OT and internet
Devices with End of support
Weak & undocumented remote access
Limited incident response testing
Some PLCs are configured to allow remote configuration
Good progress
May require significant effort
Deploy discovery tool
Deploy Firewall
Deploy Endpoint Protection
Deploy remote access
Opportunities
Threats

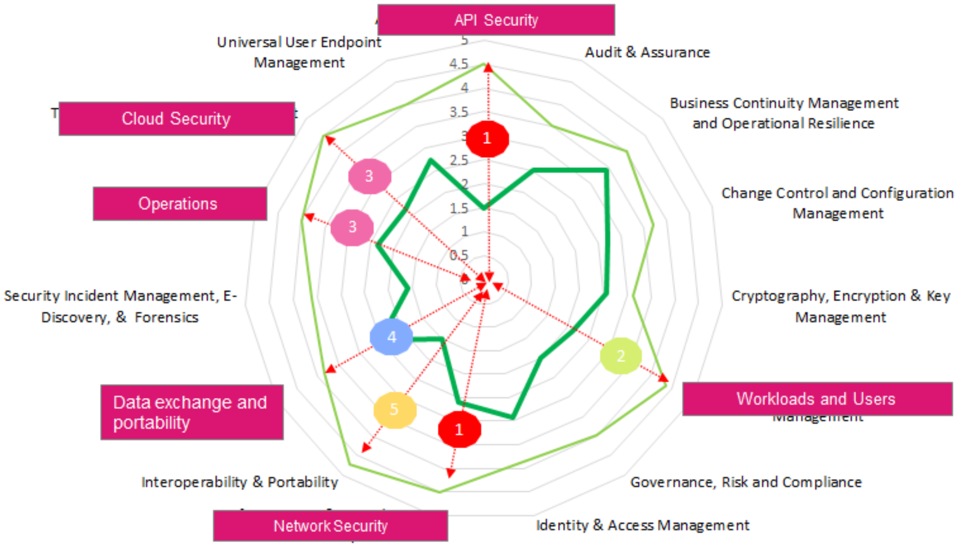
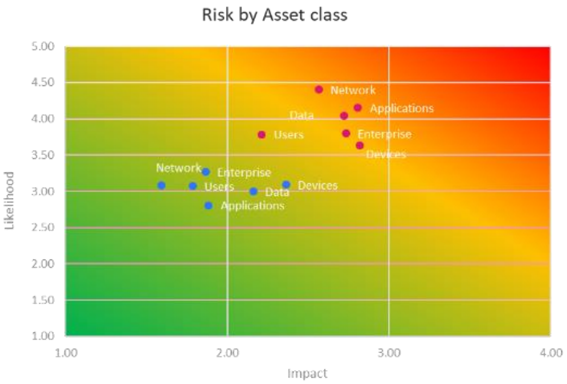


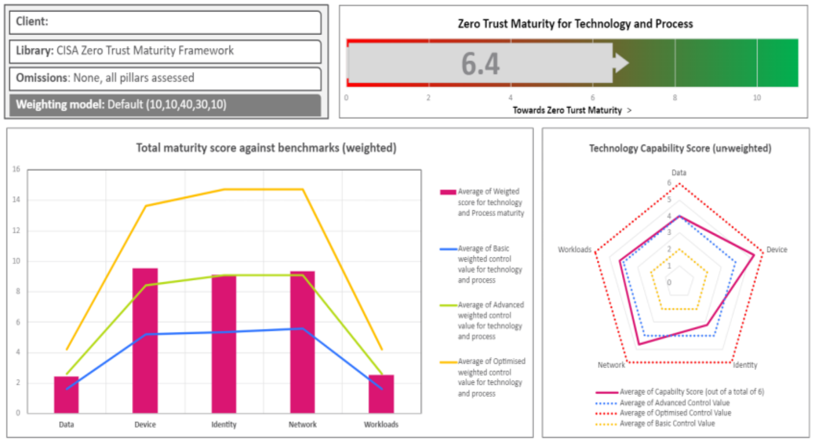
Fig: Example radar graph showing GAP analysis and priority weighting

Radar and priority graphs: The standard radar graph is a familiar tool used to show gaps identified as part of an assessment. We've compiled these graphs with other elements to add a priory rating linked to the complexity and return-on-investment analysis done as part of our engagement.

Risk heat maps: A risk heat map is a powerful visualization tool used with Enterprise Risk Management. Also known as a risk heat chart or risk matrix, it shows risk likelihood on the horizontal axis (X) and risk impact on the vertical axis (Y). We incorporate this view into our risk assessment work and show how various data points will move once the recommended treatment is actioned.



CISO dashboards: How data is presented is very important when communicating across various teams within a specific organization. We've therefore defined several presentations explicitly designed for different audiences. The table below shows how we construct these views. It's an example of a C-level Zero Trust dashboard showing the overall maturity score and various data representations.



Client:

Library: CISA Zero Trust Maturity Framework

Omissions: None, all pillars assessed

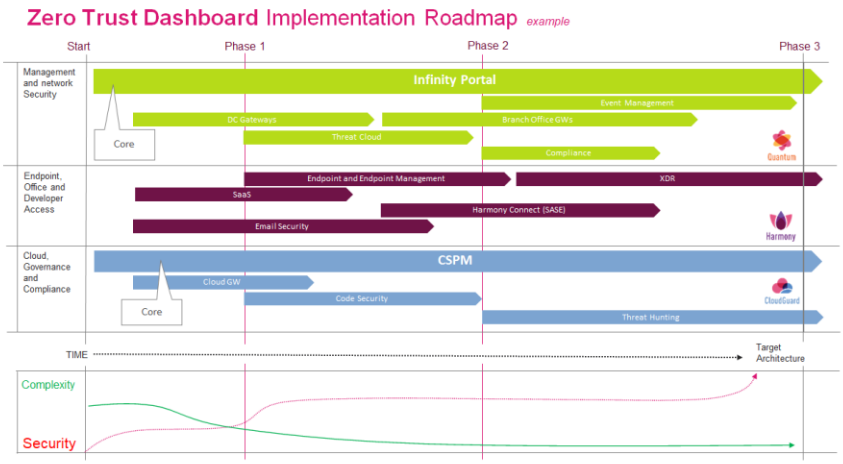
Weighting model: Default (10,10,40,30,10)

Zero Trust Maturity for Technology and Process
6.4
0
2
4
6
8
10
Towards Zero Turst Maturity >
Total maturity score against benchmarks (weighted)
16
14
12
10
8
6
4
2
0
Data
Device
Identity
Network
Workloads
Average of Weigted score for technology and Process maturity
Average of Basic weighted control value for technology and process
Average of Advanced weighted control value for technology and process
Average of Optimised weighted control value for technology and process
Technology Capability Score (unweighted)
Data
Device
Identity
Network
Workloads
6
5
4
3
2
1
0
Average of Capabilty Score (out of a total of 6)
Average of Advanced Control Value
Average of Optimised Control Value
Average of Basic Control Value

Fig: Zero Trust executive dashboard example

Security roadmaps: Planning technology adoption can be complex and, based on our work in the field, is a much-needed and requested component of any cyber security advice. To this end, we now ensure that GANTT-style charts are included in our reports when requested.

Plans, such as the one shown here, can be extremely useful when planning transformation exercises or adopting complex architectural changes such as Zero Trust adoption, whereby activities must be scheduled correctly.



Now that we've established the context and how CESFv2 is centrally positioned within our community, we can explore how it's used to articulate architectural, operational, and leadership aspects of cyber security. In the next section, we'll unpack the new components of the framework and explore how these additional features are used by us and our customers.

CESFv2 Layers

Even though our new framework evolved from the previous versions, the basic premise has not changed. There is still a need for a defined and repeatable process that is easy to follow and guides us to deliver accountable and traceable security architecture.

Introduction to Layers

The most significant change has been to append our previous version of CESF with new layers, which we did in order to increase the effectiveness of the process by allowing the sub-process to be included. We call this sub-process a "contextual layer". Its primary function is to provide context to different teams and stakeholders, all of whom play a role in the overarching enterprise security architecture.

The new layers are now described as follows:

Description	Detail
Outer Ring, Primary Function, Core	Refers to the core architectural process for which CESF was originally intended. The process starts with the ASSESS phase.
Inner Ring, Contextual Layer, Support Function	This ring refers to a contextual process, or function, that exists in support of the primary, or outer, process. The aim is for the addition of the context to support the overall process by allowing various sub-processes to be included. For example, "**Plan**" (as seen in the inner ring of the complete CESFv2 graphic) provides context when dealing with assessment planning i.e. it is the first phase in the process of starting an assessment.

The introduction of these additional layers has been driven by our knowledge that cyber security is an increasingly cross-functional activity. Therefore, by engaging with multiple different teams throughout the process, the quality of advice and recommendations significantly increases.

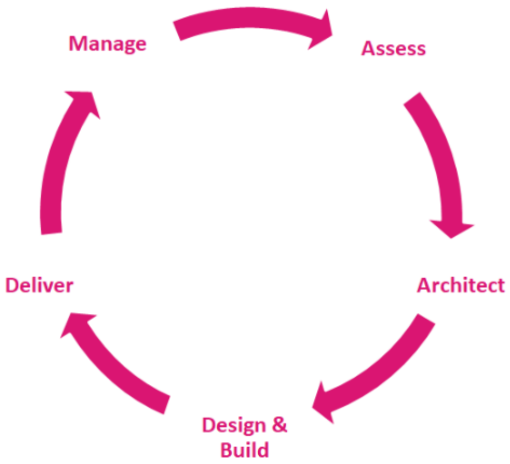
In the following section, we explore the components of each layer and describe how they were designed to work and how they could be further adapted to suit bespoke requirements.

The Core CESFv2 Layer

The outer ring of the CESFv2 communicates to stakeholders each of the various phases or steps that must be completed and the order in which they must be followed within an overall process. We draw the reader's attention to the fact that each step must be completed but in some cases some steps are imbued with greater significance. For example, one engagement may require protracted control-based assessment before the architectural work is completed, while other engagements may only require very lightweight data gathering.

- **Assess:** The first phase, in which business and security drivers are captured, and audits and assessments are completed. Depending on the nature of the engagement, this can be a high-level boardroom conversation or part of a workshop. The outcome should be a clear understanding of the target state. This core function maps directly to the assessment layer (more on this later).

- **Review:** The review focuses on the current and planned network and security architecture. Typically, this phase is done using interactive whiteboarding and a detailed design conversation. The outcome is a clearly documented "as is" and "to be" design.



- **Design:** The data captured is now used to inform a design that is aligned to Check Point's best practices. The architecture team will draw on experience, product specialists, and industry best practices to mitigate or remove the gaps which have been identified.

- **Delivery:** In this step, the system is physically built or deployed. It includes all operational testing, documentation, and acceptance into the final environment.

- **Manage:** A vital component of any design is to have the lifecycle of the service understood and managed. This is critical when defining the budget, and, also for making sure the solution performs its role as required.

Contextual Layers

CESFv2 introduces the concept of "contextual layers" into the framework. This concept allows the framework to appeal to various user groups and increases its scope and effectiveness. Depending on what you are looking to achieve, you can use the framework in a different manner.

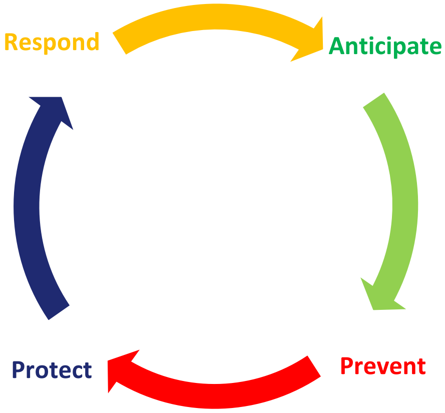
In some cases, the contextual layers are used independently from the core layers, such as in the table below:

Contextual Layer (adding additional information for specific audiences)				
Audience (view)	**Governance**	**Architect**	**Operational**	**Assessment**
Major Influence	**Gartner CAPTA**	**SABSA**	**SABSA**	**NIST/ CIS**
Contextual Layer	Anticipate	Enterprise	Enterprise	Plan
	Prevent	Solution	Solution	Interview
	Protect	Technical	Technical	Analyse
	Respond	Operations	Operations	Treatment

Now that we’ve established how the various layers are used, we will explore their function in more detail.

The Governance Contextual Layer

This view is designed for architects looking to build governance frameworks into the overall process. The rationale here is to reflect on how organizations are looking to develop frameworks that capture how a security function will be performed and the rules by which it will be delivered. The ethos is to describe the security function before it's implemented in a way that is understood by all stakeholders. For example, if there was a need to build a governance model for cloud security, then the user would follow this layer and start with defining what the security attributes for cloud security are in the “anticipate” phase.



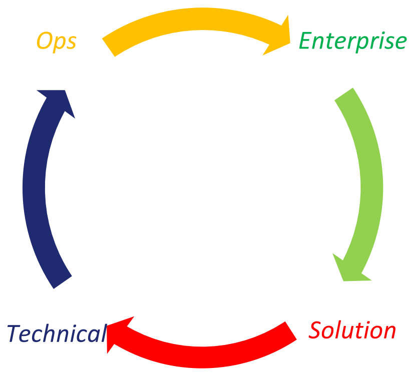
The phases are defined as:

- **Anticipate:** Anticipate needs and objectives, define business goals, and align them to technology deliverables. This part of the process is where we capture what the business expects from the security architecture and the security strategy.
- **Prevent:** Prevention through planning, architecture, threat profiling, cyber-risk analysis, best practices, and the selection of correct cyber security products and services. In cloud-like environments, we predict a reduction in the day-to-day operational management of systems and more focus on prevention through architecture. This means that a properly designed system can use a policy crafted at the design phase throughout its lifecycle with minimal production changes required.
- **Protect:** Delivery and management, or protection, through automation.
- **Respond:** Responding to breaches, security failures, and the evolving threat landscape.

The Architect and Operational Contextual Layer

This layer is used to describe the different architectural responsibilities that are typical design process, and highlights the cross-functional nature of the CESFv2 process:

- **Enterprise Security Architecture (ESA):** This team bridges business and technology. They function as a liaison between the C-suite and technology teams and are responsible for delivering justified solutions and services.



- **The ESA:** Responsible for defining which problem needs a solution and gathering the requirements from both business and security stakeholders. Their key objective is to ensure that all solutions meet clearly defined business goals.

- **Solution Architecture:** This team's function is concerned with converting requirements to design patterns that can be passed to the technical design team. The solution architect only deals with defined requirements and would engage in feasibility design and lab testing.

- **The SA[3]:** Responsible for translating the problem into a solution and describing the building blocks that should be used. This team deals with a known set of requirements. They must work closely with the ESA to ensure the response matches the organization's maturity, risk appetite, budget, and operational capabilities.

- **Technical Architecture (TA):** The TA delivers implementable design documents with a clearly defined technology specification, including sizing and configuration. They have a strong understanding of products, their roles, and their limitations.

- **Ops:** The role of this team is critical to the continued success of the architecture throughout its life cycle, as all systems require an operational element. In this phase, the expectation is that processes are defined and implemented alongside a collection of metrics and data to demonstrate the system's effectiveness.

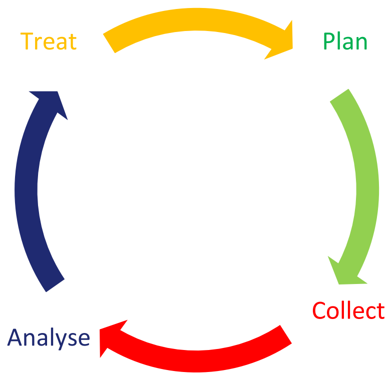
The Assessment Contextual Layer

A core component of our new framework is a focus on using assessments to improve the overall 18 effectiveness and architectural output of an engagement. This section looks at how we have integrated control libraries such as NIST and CIS intergrade into the overall process.

- **Plan:** Our consultants plan assessments with GRC and other cyber risk professionals with support from the client’s leadership. The assessments are designed to address cyber security gaps, map these to a risk score and present the findings in risk language understood by a C-level and executive audience. Our most common assessments are based on NIST CSF or CISv8.

[3] https://www.gartner.com/en/information-technology/glossary/solution-architecture

- **Collect:** Cyber risk assessments are conducted through interviews and observations with specific client teams. At the clients' request, we can also leverage Check Point's considerable expertise in data capture to produce detailed packet-level analysis.
- **Analyse:** Based on the dataset and controls from NIST and CIS, we use a qualitative risk-based score process to grade the controls and arrive at a cumulative risk and readiness score. When requested, these scores can be presented in classic '5x5' risk matrices or as part of a threat model.
- **Treat:** Once gaps and risks are identified, a risk register and treatment plan are built detailing what actions (if any) we recommend. Recommendations are aligned with the CESF values of EFFECTIVENESS and EFFICIENCY, i.e. there should be a clear and actionable treatment plan provided. practical



Now that we have completed an overview of the various layers and the reader has an appreciation of their function, we can explore the contextual layers in more detail. These layers represent the most significant new component of CESFv2, which are the use of a formalized assessment process and the use of cross-functional teams within architecture.

The Assessment Layer: Deep Dive

The following section is a deeper dive into how assessments are run within the overall CESFv2 process. The table below is a brief recap on how the CESFv2 core layers map to the contextual layer. The assessment layer is primary connected to the "assess" component showing that any assessment work is always completed at the beginning of an engagement and the output of the assessment is collected before we progress to the "architecture" layer of the core framework.

CESFv2 Core Layer	Description of Core Layer	Contextual Layer Mapping	Description of Contextual Layer
Assess	In CESFv2, everything starts with some level of assessment. This can be a total compliance/risk assessment or a more general conversation-led capture of current-state architecture. The decision as to what approach to take is often guided by factors such as compliance, effort and time.	**Plan**	Assessment selection and planning, understanding of threat groups.
		Collect	The collection of data through an interview, questionnaire or technology such as CSPM.
		Analyse	When dealing with control data, the analysis will build the GAP analysis. When dealing with risk assessment, the analysis will be based on the risk calculations
Architect	The phase whereby gathered data is transformed into a meaningful conceptual recommendations.	**Treat**	The action taken based on the risk register or the GAP analysis.
Design & Build	The concept is transformed into solutions that deliver on recommendations and are considered fit-for-purpose.		
Deliver	The practical step required to develop a solution. Scale and complexity must be considered at this phase.		
Manage	Production management and improvement of the solution.		

Running Assessments Using CESFv2

Using common frameworks is extremely useful for multiple reasons, not least that they act as a standard benchmark and that when completed there is a consistent report which can be generated on a yearly basis.

The main assessment frameworks are:

- **Check Point Enterprise Security Framework Assessment (CESF):** This is a proprietary assessment used to evaluate the security posture and understand the network security controls. The CESF frameworks allow us to translate NIST CSF controls into real-world security solutions.
- **NIST CSF v1.1**: NIST provides security

architects with an audit program designed to help technical and non-technical security stakeholders to visualize gaps in the organization's existing security posture.

- **CIS Controls v7.1 & v8**: The CIS Controls have internationally recognized cyber security best practices for defence against common threats. They are consensus-developed resources that bring together expert insight about cyber threats, business technology, and security.
- **Cyber Risk Assessment**: Based on the industry accepted risk equation: risk = likelihood x vulnerability. Typically, the assessment team will draw on information from MITRE ATT&CK and in-house sources to map the threat landscape to business impact.
- **SABSA:** SABSA is a framework and methodology for enterprise security architecture and service management.
- **NIST 800-53 rev5**: This document defines the standards and guidelines for federal agencies to design and manage their information security systems.
- **NIST SP 800-82r2**: This document guides how to secure Industrial Control Systems (ICS).
- **CISA Zero Trust Maturity Model**: We assess each pillar of the CISA model and rank the maturity, which, once combined with a weighting score, allows us to calculate a Zero Trust maturity score.
- **CIS Benchmarks:** CIS Benchmarks are best practices for the secure configuration of a target system.
- **SOC-CMM:** This framework is designed to deliver a continuous approach to measuring technical capability across the technology and services domains that are relevant to SOC capability.

Each framework brings a different value depending on the domain under assessment. For example, SOC-CMM is typically used to assess Secure Operations Centre capability. In contrast, NIST CSF will highlight gaps in overall cyber security capability.

Cyber Security RISK Assessment

Our Cyber Risk Assessment aims to address the challenges of implementing aspects of an effective cyber risk management strategy and propose recommendations that increase its efficiency. In addition, the program is geared towards supporting C-level decision-makers using industry-standard RISK calculations and tools.

The identification and management of cyber risk are what cyber security leaders deal with daily. It’s the natural evolution of any compliance-based assessment such as NIST of CIS. While we distinguish between the two activities, there is a cross-over. For the sake of clarity, we define the activities that relate to Cyber Risk assessments as those that include the following components which is different from a control-based assessment that is based purely on measuring compliance with a known control library, such as NIST.

Cyber Security Risk Assessment			
Assessment Component	Identity vulnerabilities	Model threats	Rank business impacts
Activity	Measure readiness (controls), test defences	Assess countermeasures, simulate attack groups and techniques	Define control outcome, perform qualitative and quantitative BIA
Outcome	Reduce risk		
Protected	Financial	Reputational / Operational	

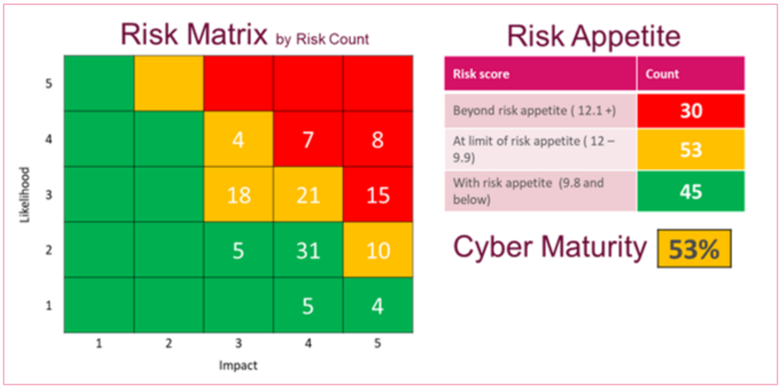
Reducing risk using quantitative analysis is sometimes a challenge. However, for those responsible for minimizing the financial impact of cyber security events, it's a necessary calculation and a valuable tool in communicating risk. The standard risk calculation we use is based on the following formula:

RISK (R) = LIKELIHOOD (L) x IMPACT (V)

- **LIKELIHOOD:** How likely is the attack to take place? What is the frequency we would expect to see this type of attack?
- **IMPACT**: If the attack was to succeed, how much damage could it do? Most importantly, could it cause the business to be impacted financially?

The example below is a 5x5 risk matrix produced as part of our RISK assessments. Based on the likelihood and impact calculation above, it acts as an effective tool to communicate those risks that we consider to be outside of acceptable thresholds and, therefore, pose a real risk to the business, both operationally and financially.

EXECUTIVE RISK DASHBOARD



Risk Matrix by Risk Count

Likelihood					
5					
4			4	7	8
3			18	21	15
2			5	31	10
1				5	4
Impact	1	2	3	4	5

Risk Appetite

Risk score	Count
Beyond risk appetite (12.1 +)	30
At limit of risk appetite (12 – 9.9)	53
With risk appetite (9.8 and below)	45

Cyber Maturity 53%

As cyber risk assessment is a core component of a process-driven architecture a dedicated publication will be made available on our website where we will deep dive into the threat modelling components not detailed in this paper.

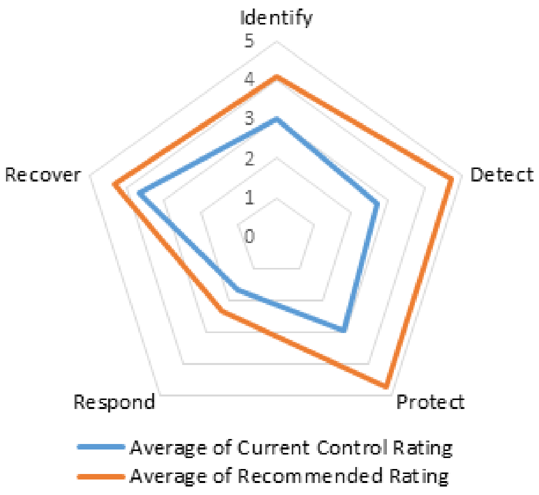
Fig: 5x5 risk matrix example

NIST & CIS Assessments

To ensure our assessment work meets industry-standards or where the client requests it, we will perform NIST and CISv8 assessments based purely on the published controls library. Check Point often perform such assessments for organizations looking for a third-party review of their posture and who understand the value of using engineering and architectural teams to add their point of view to the overall compliance conversation.

This approach allows the Check Point team to engage using a standard body of work and language that can be compared over iterations of the same assessment framework.

Typically, our clients will request that we present assessment findings in alignment with NIST in order for our work to be more easily understood by Governance, Risk, and Compliance teams. For example, this data visualization radar graph is a standard deliverable when performing NIST assessments.



CESF Assessments

In some instances, it’s more appropriate to use a customized set of assessment controls that better reflect the desired outcome. This flexible approach increases the assessment phase’s EFFICIENCY and EFFECTIVENESS as it removes the structure prescribed by frameworks such as NIST. We call this style of assessment a “CESF Assessment”. Some examples include:

Assessment Type	Description
CESF ICS Assessment	Set of 30 controls selected from NIST 800-82R2 that reflected the requirement to secure the IT/OT perimeter.
CESF Assessment DC Perimeter	Set of 5 controls selected from CISv8 IG3 that best reflected the requirement to assess the perimeter security.

Once the appropriate assessment frameworks have been selected, there is an assessment design phase that allows the frameworks (more specifically, the controls within the framework) to be edited to make them more relevant to the audience. For example, if the scope were to assess and recommend a cloud architecture, then it would be reasonable to use a section of controls from NIST CSF v1.1 such as:

"Control: PR.DS-5: Protections against data leaks are implemented."

This control could then be re-formatted in a manner that is more relevant to our advance, for example:

"CESF Control: Is the environment designed to restrict each container's access to shared resources so that information cannot inadvertently be leaked from one container to another?"

The second control would then be placed alongside similar controls and presented as a questionnaire.

Another example would be where the assessment scope includes perimeter security, for which the assessment designer can select controls such as this one from NIST 800-53:

"*SC-7: Boundary Protection: Monitor and control communications at the external managed interfaces to the system and key internal managed interfaces within the system."*

Once the process of building a bespoke and targeted assessment is completed, the controls are published as a questionnaire or hosted with our Cyber Security Assessment platform.

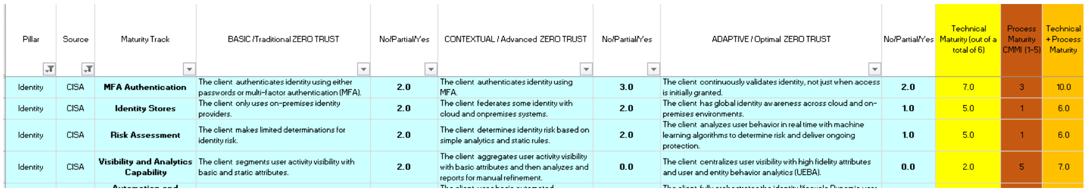
Control ID	Controls Class	Control Description	Control Detail
12.2	Boundary Defence	Scan for unauthorized connections across trusted network boundaries.	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections accessible across the boundary.
12.3	Boundary Defence	Deny communications with known malicious IP addresses.	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.

12.4	Boundary Defence	Deny communication over unauthorized ports.	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

Zero Trust Maturity Assessments (CISA)

Following the explosion of interest around Zero Trust and the work done by institutions such as Forrester, NIST and CISA, the Check Point consulting team developed a Zero Trust Maturity Assessment. It was designed to measure the "as-is" and "to-be" state of our customers' Zero Trust architecture and to use this information to help guide the development of capabilities that will ultimately improve the overall Zero Trust Maturity score.

To arrive at such a value, we selected the CISA Zero Trust model as our baseline. We maintain that it offers the most well-rounded and agnostic measure of maturity while remaining simple and consumable. The work done by CISA was formatted into an assessment, an extract of which is shown below:



Pillar	Source	Maturity Track	BASIC /Traditional ZERO TRUST	No/Partial/Yes	CONTEXTUAL / Advanced ZERO TRUST	No/Partial/Yes	ADAPTIVE / Optimal ZERO TRUST	No/Partial/Yes	Technical Maturity (out of a total of 6)	Process Maturity CMMI (1-5)	Technical + Process Maturity
Identity	CISA	**MFA Authentication**	The client authenticates identity using either passwords or multi-factor authentication (MFA).	**2.0**	The client authenticates identity using MFA.	**3.0**	The client continuously validates identity, not just when access is initially granted.	**2.0**	7.0	3	10.0
Identity	CISA	**Identity Stores**	The client only uses on-premises identity providers.	**2.0**	The client federates some identity with cloud and onpremises systems.	**2.0**	The client has global identity awareness across cloud and on-premises environments.	**1.0**	5.0	1	6.0
Identity	CISA	**Risk Assessment**	The client makes limited determinations for identity risk.	**2.0**	The client determines identity risk based on simple analytics and static rules.	**2.0**	The client analyzes user behavior in real time with machine learning algorithms to determine risk and deliver ongoing protection.	**1.0**	5.0	1	6.0
Identity	CISA	**Visibility and Analytics Capability**	The client segments user activity visibility with basic and static attributes.	**2.0**	The client aggregates user activity visibility with basic attributes and then analyzes and reports for manual refinement.	**0.0**	The client centralizes user visibility with high fidelity attributes and user and entity behavior analytics (UEBA).	**0.0**	2.0	5	7.0

Fig: Extract taken from Check Point CISA Zero Trust Maturity Assessment

We have chosen not to delve into the assessment workings within this paper other than to highlight the following;

Zero Trust means different things to different audiences. Some organizations will focus on specific Zero Trust principles above others; for example, a software application organization would most likely see Zero Trust in the context of application security. This organization-specific focus should be reflected in the "weighting" we give to the maturity score – it doesn't make sense to downgrade a maturity score if the control is irrelevant. We, therefore, added a weighting capability to our assessment. While we'll be able to fully explore the Zero Trust maturity assessment in another paper, the weighting calculation we use is based on the table below:

Weighting Table for Zero Trust Maturity Assessments			
	Network-Centric	Cloud-Centric	Application-Centric
Data	10	30	30
Device	15	5	5
Identity	50	30	20
Network	20	5	5
Workloads	5	30	40
Total	100	100	100

The concept behind weighting is that depending on the client's business activities, i.e., software development and manufacturing, etc. the approach to achieving Zero Trust will change slightly. For example, a software development company will focus on applying Zero Trust to workloads and containers and worry less about network security. This concept is fully explained in a dedicated whitepaper[4].

Zero Trust Architecture Using CISv8

The requirement to benchmark capability for specific architectural alignments is becoming increasingly important to organizations. Consequently, we've witnessed the CESFv2 framework being used to design and execute readiness assessments, such as Zero Trust architectural maturity. Therefore, we've included an example of how an organization that uses CIS controls as a standard can use these to align itself with Zero Trust architectural principles.[5]

The example below is a bundle of controls selected to gather a dataset of information about a network architecture which can then be used to generate a GAP analysis and report.

The process of designing such an assessment is as follows: firstly, the below CIS controls were selected because they are typically more technical. We then chose a set of CISv8 controls aligned with the Zero Trust principles displayed below. They reflected the client's appetite for change and security. This is also why some controls are taken from CIS Group 1 and others from CIS Group 3.

Zero Trust Principle	CIS v8 Controls	CIS Group
Asset Management	1,2,11,15	1
Account Management	5,6	1
Device and Endpoint Security	7,9,10	1,2
Logging and Visibility	8,12,17,18	1
Communication Security	3,4	1
Dynamic Policy	16,13	1,2,3

A Zero Trust assessment design example

Once we collect the controls from the table above, we can build our assessment. The example below is part of this:

[4] https://pages.checkpoint.com/the-ultimate-guide-to-zero-trust.html

[5] https://www.cisecurity.org/insights/blog/prioritizing-a-zero-trust-journey-using-cis-controls-v8

Control ID	Subject	Control
1	Perform automated application patch management.	Perform monthly (or more frequent) application updates on enterprise assets through automated patch management.
2	Establish and maintain an audit log management process.	Establish and support an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually or when significant enterprise changes occur, which could impact this safeguard.
3	Collect audit logs.	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.
4	Ensure adequate audit log storage.	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.
5	Ensure network infrastructure is up-to-date.	Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software or using currently supported Network-as-a-Service (NaaS) offerings. Review software versions monthly (or more frequently) to verify software support.

Fig: Zero Trust network questionnaire example

The architect scores each control in the table, and the data is used to complete the GAP analysis of the assessment type executed. This data visualization is core to effectively communicating where effort and spending is required.

Data Visualization for Zero Trust Assessments

This section's information is relevant to CISA, CIS, and other frameworks used to assess Zero Trust.

Once the assessor has completed their analysis and the dataset has been collected and analysed, it’s typically presented as a GAP analysis whereby the current and target state is presented. In the case of Zero Trust being able to benchmark the various pillars of capability against a known standards for compliance allows the customer a view on where effort and spending are required. The example below is taken from a Zero Trust maturity assessment:

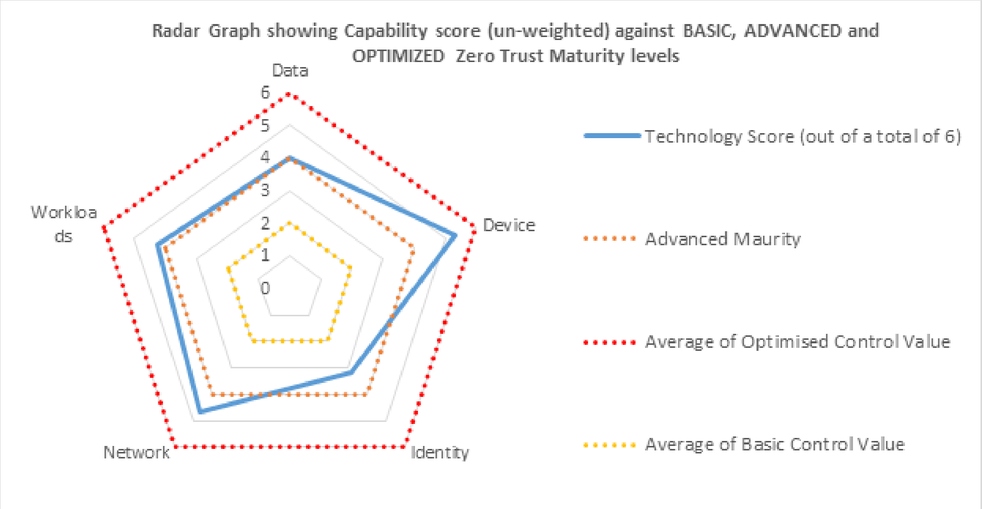


Fig: Data visualization is a core component of all assessment output

The Architect and Operational Layer: Deep Dive

This section looks in more detail at the architects' contextual view that is shown within CESFv2. This layer is designed to closely support the core layer by describing how different architectural capabilities are leveraged as we move through a design cycle. Good architecture requires input from multiple teams at various points in the process.

As discussed in the previous section, CESFv2 defines three different architectural functions. These are:

Title	Focus	Competencies
Enterprise Security Architect	Collecting defining requirements and mapping business requirements to technology choices.	GAP analysis, RISK assessments.
Security Solutions Architect	Mapping requirements to technology and defining solutions, and ensuring components are selected correctly.	Solution design in HLD format.
Technical Security Architect	Low-level configuration design and detailed technical knowledge to confirm the chosen technology delivers requirements.	Solution design in LLD format.

When each function is supportive and complimentary of the others, it means there is no architectural hierarchy but rather a symbiotic interaction of different disciplines. When done correctly, each step in the process will be represented by the most appropriate stakeholder and their counterpart within the architecture team (assuming all three architectural functions are represented):

CESFv2 Core Layer	Description of Core Layer	Contextual Layer Mapping	Architectural Responsibility
Assess	In CESFv2, everything starts with some level of assessment. This can be a total compliance/risk assessment or a more general conversation-led capture of current-state architecture. The decision as to what approach to take is often guided by factors such as compliance, effort, and time.	**Enterprise**	Enterprise Security Architect
Architect	The phase whereby data gathered is transformed into a meaningful convert or recommendation.	**Enterprise / Solution**	Enterprise and Solutions Security Architect
Design & Build	The concept is transformed into solutions that deliver on recommendations and are considered fit-for-purpose.	**Solution**	Solutions Architect
Deliver	The practical step required to develop a solution, scale and complexity must be considered at this phase.	**Technical**	Technical Architect
Manage	Production management and improvement of the solution.	**Ops**	Operations

By leveraging multiple different architectural disciplines, we can better support the development of quality architectural patterns and plans. Two critical deliverables from any architectural engagement should be a cyber security roadmap that defines the logical steps required to achieve the desired goal and a conceptual/HLD diagram that logically positions the security components into the broader ecosystem.

Network Diagrams

As discussed, a core deliverable of CESFv2 is to arrive at an actionable set of recommendations. More often than not, this is done through the production of conceptual architecture diagrams such as the example shown below.

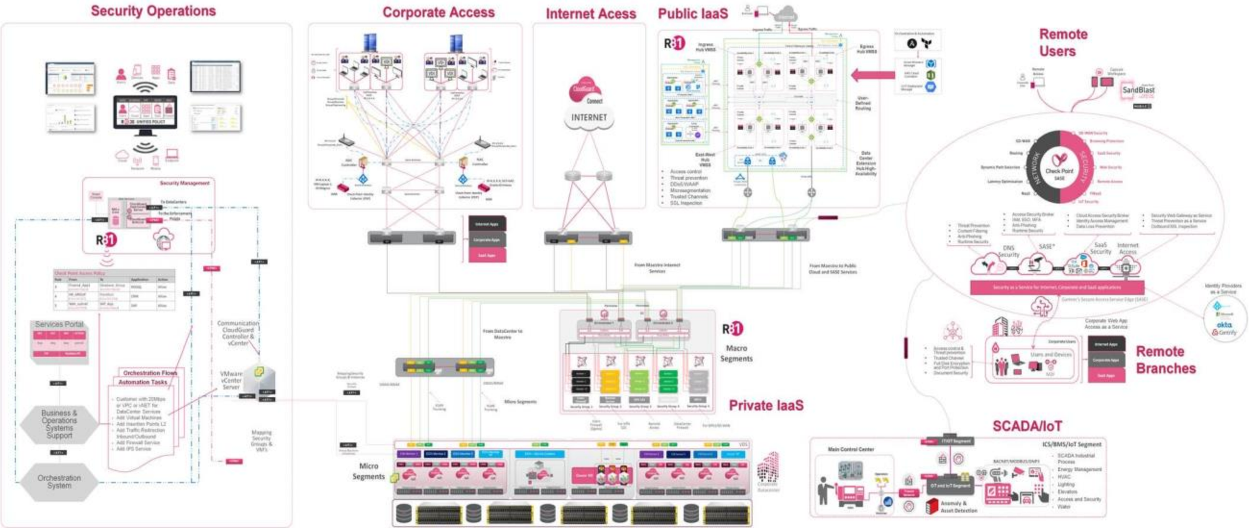


Fig: Network topology produced as part of the CESFv2 process and workshop

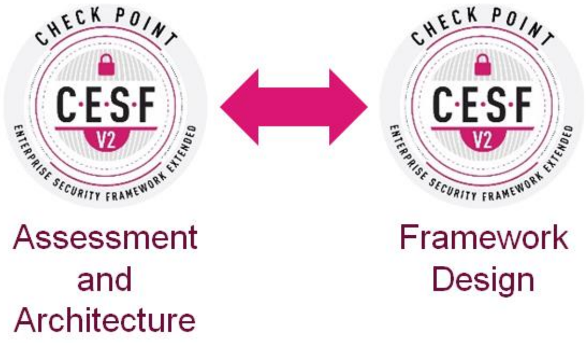
Building Governance Frameworks with CESFv2

The importance of a well-defined governance framework cannot be overlooked in an established cyber security strategy, which is why we have included this section, which describes how CESFv2 can be used practically to deliver a cyber security governance framework.

Before we start, we should define what a governance framework is and why we believe it to be important. For this, we reference the UK National Cyber Security Centre.

"A governance framework is vital to coordinate and direct the management of the service. An effective governance framework will ensure that procedural, personnel, physical and technical controls continue to work through the lifetime of service. It should also respond to changes in the service, technological developments, and the appearance of new threats."[6]

Based on this definition, we can start to adapt CESFv2 appropriately and use the adapted mode to build our governance framework.


CHECK POINT
C·E·S·F
V2
ENTERPRISE SECURITY FRAMEWORK EXTENDED
Assessment and Architecture
CHECK POINT
C·E·S·F
V2
ENTERPRISE SECURITY FRAMEWORK EXTENDED
Framework Design

Once completed, our framework will help conceptualize the link between security strategy, architecture, and functional security controls, and streamline communication from the boardroom to security engineers through a commonly understood framework.

Framework Design

In order to proceed, we first acknowledge that the original CESFv2 process needs to be re-formatted because a governance framework is not a process. We call this new format the "framework mode" so that there is a clear distinction between the CESFv2 process and the CESFv2 framework. It’s important to note that the following framework is only one interpretation based on our use case. If required, the framework can be mapped to other, more suitable functions.

Moving into the framework mode requires a restructuring of the CESFv2 layout and a redefinition of the process. The mapping is shown below:

[6] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-4-governance-framework

CESF Layers	CESFv2 Framework Mode	Description
Assess	Anticipate	Anticipate security requirements and deliverables
Architect		
Design	Prevent	Prevent loss (financial or Operational) events through architecture
Delivery	Detect	Detect threats and continuously improve and develop the system
Manage	Respond	Observe and respond based on threat intelligence

Fig: CESF governance mode and CESF layers

Once the concept of roles and layers is translated into the framework mode, we can apply our governance terminology and language to the new pillars, or, "anticipate, prevent, detect, respond". The critical design point is to define the roles of each pillar clearly, and they must document the goals of the governance model. In simple terms, an effective governance model clearly articulates the organization's goals, the key personnel and their responsibilities, and the tools they will use to achieve the strategic objectives.

A representation is shown below and should be used as a template for the following section, which involves populating the framework, starting with the "Anticipate" phase.

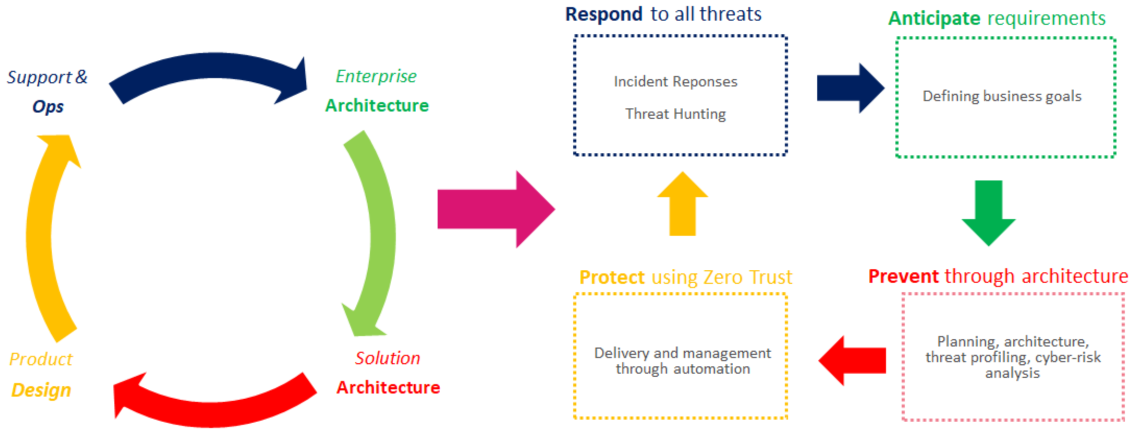


Fig: Using CESFv2 in framework mode

Framework Section Explained

The table below defines the roles for each position in the framework process. It allows the practitioner to fill in the gaps in order to build the framework. At this stage, it's important to note that the elements entered into the framework should be measurable in some form; doing so will increase the effectiveness of the final framework and allow maturity to be tracked . For example, if we define the adoption of a certain technology in the “Protect” element then we should also define at what point we expect this technology element to be completely deployed.

Framework Mode	Description	Example	Key Stakeholder
Anticipate	Anticipating what cyber security posture the organization needs to adopt in order to meet business objectives and define a strategy. Defining business goals and aligning them to technology deliverables.	Remote workforces require a secure Zero Trust-aligned security model that is not reliant on legacy DCs.	CISO and leadership need to anticipate and document the strategy.
Prevent	Prevent security failure by developing a policy that describes which process and technology are used and by whom, which is documented within a governance policy that includes a service catalogue. Prevention through planning, architecture, threat profiling, cyber-risk analysis, best practices, and selecting the correct cyber security products and services. Should detail functional and non-functional controls.	Hybrid SASE principles for user traffic. Create a single security policy for all users. Fully automate the onboarding of users' API and cloud-native-only components.	Enterprise Architects and GRC teams.
Detect	Protect all assets by deploying and managing the security policy and posture and providing a proportional response following the operational process. This includes monitoring, maintenance, and asset lifecycle management. Delivery and management, or protection, through automation and detection of changes in the posture of the environment, network, and workload.	Follow Zero Trust's “log everything” principle. Leverage observability. API-only change policy.	Engineers, implementation and operational teams.
Respond	Responding to events in a manner that can be adapted so that continuous improvement can be made to the overall security posture. Responding to changes in the threat landscape, offensive capabilities, and aggressor motivation to continuously update the security strategy. Responding to breaches, security failures, and the evolving threat landscape.	XDR and threat hunting. Ingression to dynamic threat intelligence.	Incident responses and cyber operation teams.

Finished Framework Example

While the development of frameworks to assist in solution delivery is customized to each organization, we have included the following example to illustrate how we designed a framework using CESFv2 components.

This example is taken from an organization adopting SASE architectural principles. Each section has been carefully completed to contain only those components which are of value to the organization. In productivity teams, the framework acts as a map for their SASE adoption.

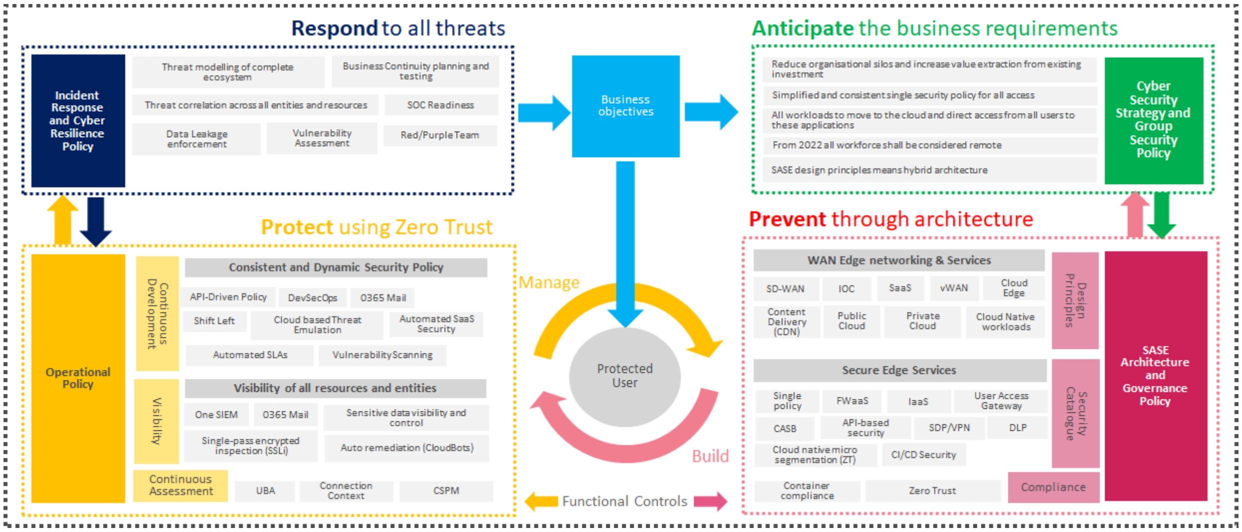

Respond to all threats
Incident Response and Cyber Resilience Policy
Threat modelling of complete ecosystem
Business Continuity planning and testing
Threat correlation across all entities and resources
SOC Readiness
Data Leakage enforcement
Vulnerability Assessment
Red/Purple Team
Business objectives
Anticipate the business requirements
Reduce organisational silos and increase value extraction from existing investment
Simplified and consistent single security policy for all access
All workloads to move to the cloud and direct access from all users to these applications
From 2022 all workforce shall be considered remote
SASE design principles means hybrid architecture
Cyber Security Strategy and Group Security Policy
Protect using Zero Trust
Operational Policy
Continuous Development
Consistent and Dynamic Security Policy
API-Driven Policy
DevSecOps
0365 Mail
Shift Left
Cloud based Threat Emulation
Automated SaaS Security
Automated SLAs
Vulnerability Scanning
Visibility
Visibility of all resources and entities
One SIEM
0365 Mail
Sensitive data visibility and control
Single-pass encrypted inspection (SSLi)
Auto remediation (CloudBots)
Continuous Assessment
UBA
Connection Context
CSPM
Manage
Protected User
Build
Functional Controls
Prevent through architecture
WAN Edge networking & Services
SD-WAN
IOC
SaaS
vWAN
Cloud Edge
Content Delivery (CDN)
Public Cloud
Private Cloud
Cloud Native workloads
Design Principles
Secure Edge Services
Single policy
FWaaS
IaaS
User Access Gateway
CASB
API-based security
SDP/VPN
DLP
Cloud native micro segmentation (ZT)
CI/CD Security
Security Catalogue
Container compliance
Zero Trust
Compliance
SASE Architecture and Governance Policy

Fig: Governance framework for SASE adoption example

Conclusion

The Check Point enterprise architectural process continues to develop and reflect our experience with customers, combined with our desire to help organizations manage their cyber risk through architecture.

In summary, this paper has:

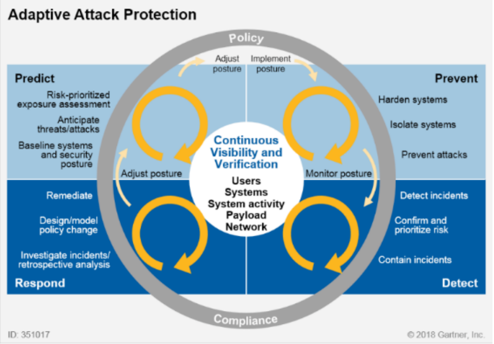
- Explained the update to the Check Point Enterprise Framework.
- Introduced the concept of context so that the framework is relevant to a broader audience, namely C-level and assessors.
- Detailed how the CESFv2 puts assessment as a core component of successful architecture.
- Shown how CESFv2 can be used to develop governance frameworks.
- Given examples of assessment and framework development using CESFv2.

This paper is written for the community, and we hope that it is of use for the betterment of security architecture in general. For more information, please see https://www.checkpoint.com/support-services/security-consulting/.

Appendix: CESFv2 and Other Frameworks

As with most architectural artifacts, there is, and should always be, influence from other bodies of work. In some senses being able to link multiple influences and sources add to CESFv2s overall credibility and allows the user to apply context to the process.

One of the key reference points in the development of the CESFv2 approach is the work done by Gartner within their CARTA approach. The original CESF framework design methodology was heavily influenced by SABSA, while for CESFv2, this influence is drawn from Gartner's ever-evolving Continuous Adaptive Risk and Trust Assessment (CARTA) model, as shown here.


Adaptive Attack Protection
Policy
Adjust posture
Implement posture
Predict
Risk-prioritized exposure assessment
Anticipate threats/attacks
Baseline systems and security posture
Prevent
Harden systems
Isolate systems
Prevent attacks
Adjust posture
Monitor posture
Continuous Visibility and Verification
Users
Systems
System activity
Payload
Network
Remediate
Design/model policy change
Investigate incidents/ retrospective analysis
Respond
Detect incidents
Confirm and prioritize risk
Contain incidents
Detect
Compliance
ID: 351017
© 2018 Gartner, Inc.

In simple terms, Gartner's CARTA framework has influenced our thinking in relation to both the CESFv2 core architectural principles and the CESF Framework Mode. These include:

- **Forward-thinking:** The CARTA model acknowledges that automation is a key requirement and that security should look to automation first and people second when it comes to responding to threats.
- **Continuous improvements and development:** This is aligned with cloud best practice principles and enables a feedback loop between architects and operations.
- **Chaining:** Refers to the use of multiple solutions, technologies and products aligned across different disciplines while working symbiotically. In such a framework, each part of the system contributes to the overall security posture.

The following mappings between CESFv2 to other frameworks are offered as examples of the flexibility designed into the CESFv2 framework:

Framework/ Model	Attribute	Attribute Description	CESFv2 Mapping	CESFv2 Ring
Gartner CARTA	Continuous improvement	Continuous cyber security assessments are key to moving at the correct speed, and that automation should be considered core to security.	Anticipate, protect and respond	Contextual
NIST	Definitions	Roles and responsibilities between different architectural functions.	Enterprise, solution and technical architects	Contextual
NIST RMF	Assessment planning	Phases of planning required for a cyber risk assessment.	Plan, interview, analysis, treatment	Contextual