



EXPOSURE MANAGEMENT

Compliance & Framework Alignment Guide

How Check Point Exposure Management aligns with the regulations, standards, and operational frameworks security and compliance teams navigate today.

Covering:

DORA · NIS2 · ISO/IEC 27001:2022 · PCI DSS v4.0 · NERC CIP · CJIS · SOC 2 · FISMA
CTEM · NCSC Cyber Assessment Framework · NIST CSF 2.0 · CIS Controls v8



WORKING DOCUMENT - Version 1.0 - September 2026

This guide will be updated as regulations, frameworks, and the Check Point Exposure Management product suite evolve.

About This Guide

Security and compliance teams are asked to answer to several regulations, standards, and frameworks, often at the same time and often with overlapping evidence requirements. This guide brings together, in one place, how Check Point Exposure Management supports eight of the most common: four compliance mandates and four operational or governmental frameworks.

Before mapping the specifics, it helps to be precise about the difference between a compliance mandate and a framework, since the two get used interchangeably in conversation but carry very different obligations.

Compliance Mandates vs. Frameworks

A compliance mandate is a legal, regulatory, or contractual requirement. Failure to meet it carries a defined consequence, such as a fine, a suspension of service, loss of certification, or loss of the right to process card payments. A framework is voluntary guidance: a shared structure or vocabulary for organizing a security program, with no direct penalty for non-adoption, though many regulators and customers now expect one anyway.

Compliances we will cover:

Item	Classification	Key Distinction
DORA	Regulatory Mandate (EU Law)	Digital Operational Resilience Act. Mandatory for financial entities in the EU. Focuses on ICT risk management and operational resilience.
NIS2	Regulatory Mandate (EU Directive)	EU-wide cyber security directive for critical and essential entities. Requires proactive risk management and incident reporting.
ISO/IEC 27001	Certifiable International Standard	Information Security Management System (ISMS) standard. Organizations are certified against Annex A controls.
PCI DSS v4.0	Contractual Industry Standard	Payment card data security standard enforced by acquiring banks and card networks. Mandatory for any entity handling cardholder data.
NERC CIP	Regulatory Mandate (FERC-Enforced)	Critical Infrastructure Protection standards for the North American Bulk Electric System. Mandatory for registered utilities and grid operators.
CJIS Security Policy	Regulatory Mandate (Federal)	FBI security policy governing Criminal Justice Information. Mandatory for law enforcement agencies and their contractors.
SOC 2	Attestation Standard (Contractual)	AICPA Trust Services Criteria. An independent CPA opinion on control design and effectiveness, not a government mandate but often contractually required.
FISMA	Regulatory Mandate (Federal)	Requires U.S. federal agencies and their contractors to implement and monitor NIST SP 800-53 controls under the Risk Management Framework.

Frameworks we will cover

Item	Classification	Key Distinction
CTEM	Operational Strategy / Methodology	Gartner's Continuous Threat Exposure Management model is the operational process Check Point Exposure Management automates.
NIST CSF 2.0	Voluntary Security Framework	High-level taxonomy - Govern, Identify, Protect, Detect, Respond, Recover - for organizing a cyber security program.
NCSC CAF	Government Assessment Framework	The UK NCSC's Cyber Assessment Framework, used for self-assessment under the UK's NIS Regulations and more broadly.
CIS Controls v8	Voluntary Security Framework	A prioritized set of 18 safeguards from the Center for Internet Security, focused on stopping the most common attacks.

How Check Point Exposure Management Is Organized

Check Point Exposure Management unifies five capabilities across a continuous loop of scoping, discovery, prioritization, validation, and remediation: Threat Intelligence , Cyber Asset Attack Surface Management (CAASM), Vulnerability Prioritization, Agentic Exposure Validation (AEV), and Safe Remediation.

PART ONE

Compliance Mandates

Regulators have moved from voluntary guidance to binding law, and they keep expanding who falls in scope. NIS2 and DORA now carry the full weight of EU statute. PCI DSS closed its transition period in March 2025, making 51 once-optional requirements mandatory overnight. NERC CIP added new vendor and supply chain rules for utilities in 2026. Compliances are growing in scope with tighter reporting windows, and accountability that reaches further up the org chart.

NIS2 now sets fines up to €10 million or 2% of global annual turnover, whichever is greater, and puts executives personally on the hook for failing to oversee risk measures. PCI DSS non-compliance can mean losing the right to process card payments entirely. NERC CIP violations bring FERC enforcement action against the operators of the power grid itself.

COMPLIANCE MANDATE

DORA

Digital Operational Resilience Act • Regulation (EU) 2022/2554 • Regulatory Mandate

The Digital Operational Resilience Act has applied directly across the EU financial sector since January 17, 2025, with no national transposition required. It rests on five pillars: ICT risk management, incident management and reporting, digital operational resilience testing, ICT third-party risk management, and information sharing.

Check Point Exposure Management gives financial entities continuous visibility, prioritization, and remediation across the whole attack surface, directly supporting these obligations.

Check Point Capability	DORA Provision	How It Feeds In
CAASM & EASM & Vulnerability Prioritization	Art. 5 - Governance and organisation	Gives the management body a single, current view of asset and risk exposure to support the board-level oversight and accountability DORA requires.
Threat Intelligence	Art. 8 - Identification (threat landscape)	Continuously identifies external threat sources, exploited vulnerabilities, and attacker infrastructure, feeding the entity's ongoing ICT risk identification process.
CAASM & EASM	Art. 8 - Identification (ICT asset inventory)	Maintains a live, complete inventory of ICT assets across cloud, on-premises, OT, and SaaS, the foundation Article 8 requires for risk identification.
Vulnerability Prioritization	Art. 9 - Protection and prevention	Correlates exploitability, reachability, asset criticality and business impact so teams act on the vulnerabilities most likely to be used against them, before formal patches land.
Safe Remediation & Brand Protection	Art. 11 - Response and recovery	Applies compensating controls and virtual patching across the multi-vendor stack, supporting faster containment and recovery of affected systems. Takes impersonating websites and social media profiles down.
Threat Intelligence	Art. 19 - Notification of major ICT-related incidents	Early detection of credential leaks, malware infections, impersonation, and attacker infrastructure shortens the time to spot an incident, helping meet the 4-hour initial notification deadline.
Agentic Exposure Validation (AEV)	Art. 24–25 - Digital operational resilience testing	Continuously and safely validates whether identified exposures are genuinely exploitable, closing the loop between testing programs and remediation evidence.
Supply Chain Intelligence	Art. 28 - ICT third-party risk, general principles	The Supply Chain Intelligence module continuously monitors vendor and third-party infrastructure for breaches, leaked credentials, and compromise, giving entities evidence-backed input for the Register of Information they must maintain on ICT third-party arrangements."
Threat Intelligence	Art. 45 - Information-sharing arrangements	Supplies structured threat intelligence, including indicators of compromise and active campaigns, supporting participation in sector information-sharing arrangements.

This is a high-level overview for information purposes only and does not constitute legal advice on DORA compliance. DORA applies directly as an EU regulation, but exact obligations vary by entity type, proportionality category, and regulatory technical standards issued by the European Supervisory Authorities. Organizations should consult qualified legal counsel and their DORA compliance program lead.

COMPLIANCE MANDATE

NIS2

Network and Information Security Directive • Directive (EU) 2022/2555 • Regulatory Directive

The NIS2 Directive requires essential and important entities to run risk-based, proportionate cyber security measures under Article 21, keep management accountable under Article 20, and report significant incidents within tight deadlines under Article 23 (a 24-hour early warning and a 72-hour notification).

Check Point Exposure Management gives organizations continuous visibility, prioritization, and remediation across the whole attack surface, directly supporting these obligations.

Capability	NIS2 Provision	How It Feeds In
CAASM & ASM	Art. 20 - Governance	Gives the management body a single, current view of asset and risk exposure to support the board-level oversight NIS2 requires.
Threat Intelligence	Art. 21(2)(a) - Risk analysis & policies	Provides continuously updated external threat context so risk registers and security policies reflect real, current exposure rather than a point-in-time assessment.
CAASM & EASM	Art. 21(2)(a) - Risk analysis (foundation)	An accurate, live asset inventory is the starting point for any risk analysis; CAASM & ASM supplies the asset context Threat Intelligence and Vulnerability Prioritization act against.
Supply Chain Intelligence	Art. 21(2)(d) - Supply chain security	Extends monitoring to vendors, partners, and third-party infrastructure, surfacing exposure that originates outside the organization's own perimeter.
Vulnerability Prioritization & Safe Remediation	Art. 21(2)(e) - Vulnerability handling & secure maintenance	Prioritizes and closes vulnerabilities safely across the multi-vendor stack, guiding compensating controls where patching is not immediately possible.
Agentic Exposure Validation (AEV)	Art. 21(2)(f) - Assessing effectiveness of measures	Continuously validates whether existing controls are actually mitigating live exposures, giving evidence that measures work rather than just exist on paper.
Safe Remediation	Art. 21(2)(g) - Basic cyber hygiene	Automates routine hardening and remediation actions across security tools already in place, reducing manual hygiene overhead.
CAASM & EASM	Art. 21(2)(i) - Asset management & access control	Shows ownership and connections for every asset, including unmanaged and shadow IT/OT, supporting asset management and access control policies.
Threat Intelligence	Art. 23 - Incident reporting	Early detection of credential leaks, impersonation, and attacker infrastructure shortens time-to-spot for an incident, helping meet the 24-hour and 72-hour deadlines.

This is a high-level overview for information purposes only and does not constitute legal advice on NIS2 compliance. NIS2 is transposed into national law by each EU member state, and exact obligations vary by sector, entity classification, and jurisdiction. Organizations should consult qualified legal counsel and their national transposition law.

ISO/IEC 27001:2022

Information Security Management System (ISMS) Standard • ISO/IEC 27001:2022 • Certifiable International Standard

ISO/IEC 27001:2022 sets out 93 Annex A controls across four themes:

- Organizational
- People
- Physical
- Technological

that organizations select from based on their risk assessment and record in a Statement of Applicability.

Check Point Exposure Management generates the live evidence an ISMS needs to keep those controls operating in practice rather than existing only on paper.

Capability	Annex A Control	How It Feeds In
Threat Intelligence	A.5.7 - Threat intelligence	Collects and analyzes live external threat data (leaked credentials, dark web chatter, active campaigns and information from 150,000+ Check Point Firewalls) so security decisions are based on current, real-world threats.
CAASM & EASM	A.5.9 - Inventory of information and other associated assets	Maintains a live, owned register of every asset, including unmanaged and shadow IT/OT, the foundation this control requires.
Supply Chain Intelligence	A.5.21 - Managing information security in the ICT supply chain	Extends monitoring to vendors, partners, and third-party infrastructure, surfacing exposure that originates outside the organization's own perimeter.
CAASM	A.5.23 - Information security for use of cloud services	Gives continuous visibility into cloud assets and how they connect, supporting oversight of cloud service use as it changes.
Threat Intelligence	A.5.24 - Incident management planning & preparation	Early detection of credential leaks, impersonation, and attacker infrastructure feeds directly into incident response playbooks, giving preparation teams a head start.
CAASM	Clause 8.2 - Information security risk assessment	An accurate, current asset inventory is the starting point for any risk assessment; CAASM keeps the risk register and Statement of Applicability current.
Vulnerability Prioritization & Safe Remediation	A.8.8 - Management of technical vulnerabilities	Prioritizes and closes vulnerabilities safely across the multi-vendor stack, guiding compensating controls where patching is not immediately possible.
Safe Remediation	A.8.9 - Configuration management	Identifies risky misconfigurations across security tools already in place and helps bring systems back to a secure, documented baseline.
Safe Remediation	A.8.9 - Configuration management	Continuously validates whether existing controls are actually mitigating live exposures, giving auditable evidence that measures work rather than just exist on paper.

This is a high-level overview for information purposes only and does not constitute certification or legal advice. Annex A is a reference set of controls; organizations select and justify applicable controls in their own Statement of Applicability based on their risk assessment. Organizations should consult their ISMS lead or certification body for scope-specific guidance.

COMPLIANCE MANDATE

PCI DSS v4.0

Payment Card Industry Data Security Standard • PCI DSS v4.0.1 • Contractual Industry Standard

PCI DSS is a contractual standard maintained by the PCI Security Standards Council and enforced by acquiring banks and payment networks. It applies to any organization that stores, processes, or transmits cardholder data. Version 4.0 is fully in effect: as of March 31, 2025, every previously future-dated requirement became mandatory.

The standard's 12 requirements are grouped into six objectives, from building secure networks through maintaining an information security policy. Check Point Exposure Management supports the exposure-facing half of that program, meaning knowing what is in the cardholder data environment, what is exposed to it, and closing gaps quickly.

Capability	PCI DSS v4.0 Requirement	How It Feeds In
CAASM	Req. 1 - Install and maintain network security controls	Maps every asset connected to or adjacent to the cardholder data environment, including undocumented and shadow assets that firewall rules and segmentation reviews would otherwise miss.
Safe Remediation	Req. 2 - Apply secure configurations to all system components	Identifies default credentials, risky configurations, and drifted baselines across the multi-vendor stack, and applies compensating controls while hardening is completed.
Threat Intelligence	Req. 3 - Protect stored account data	Monitors the open, deep, and dark web for leaked or offered-for-sale cardholder data, giving early warning if stored account data has already been exposed.
Vulnerability Prioritization & Safe Remediation	Req. 6 - Develop and maintain secure systems and software	Correlates exploitability, reachability, and business impact to guide which vulnerabilities in custom and third-party software need fixing first.
Threat Intelligence	Req. 8 - Identify users and authenticate access	Surfaces exposed and leaked credentials tied to the organization, so compromised access can be revoked before it is used against the cardholder data environment.
Threat Intelligence	Req. 10 - Log and monitor all access to system components and cardholder data	Extends monitoring beyond internal logs to external indicators of compromise, phishing infrastructure, and threat actor chatter targeting the environment.
Agentic Exposure Validation (AEV)	Req. 11 - Test security of systems and networks regularly	Continuously and safely validates whether exposures identified by scans and tests are genuinely exploitable, complementing periodic penetration testing with always-on validation.
Threat Intelligence & CAASM & EASM	Req. 12 - Support information security with organizational policies and programs	Gives risk owners a current, evidence-backed view of external exposure and asset inventory to keep security policies and the annual risk assessment grounded in reality.

This is a high-level overview for information purposes only and does not constitute a PCI DSS compliance determination. PCI DSS scope, applicable Self-Assessment Questionnaire, and required compensating controls vary by merchant level and environment. Organizations should consult their Qualified Security Assessor (QSA) or Internal Security Assessor (ISA) for scope-specific guidance.

COMPLIANCE MANDATE

NERC CIP

Critical Infrastructure Protection Standards • NERC CIP-002 through CIP-015 • Regulatory Mandate (FERC-Enforced)

The NERC Critical Infrastructure Protection standards are mandatory, FERC-approved requirements for entities that own or operate the North American Bulk Electric System (BES). Thirteen active standards, CIP-002 through CIP-014 plus the newer CIP-015, cover everything from asset categorization and personnel screening to electronic and physical security perimeters, configuration change management, supply chain risk, and incident reporting. Regional Entities audit and enforce compliance in the field.

Because CIP governs operational technology, uptime constraints and extended equipment lifecycles matter as much as the security outcome itself. Check Point Exposure Management supports the layers of CIP most dependent on knowing what is out there, what is exposed, and closing gaps without disrupting the Bulk Electric System.

Capability	NERC CIP Standard	How It Feeds In
CAASM & EASM	CIP-002 - BES Cyber System Categorization	Maintains a live inventory of cyber assets, including OT and ICS components, giving entities the accurate foundation every impact-rating decision and downstream requirement depends on.
Threat Intelligence & Agentic Exposure Validation	CIP-005 - Electronic Security Perimeters	Monitors external-facing infrastructure and third-party remote access points tied to the BES environment, flagging exposure before it reaches the electronic security perimeter.
Vulnerability Prioritization	CIP-007 - System Security Management	Correlates exploitability and active threat activity against system components, guiding which patches and hardening actions matter most where limited patch windows are the norm.
Threat Intelligence	CIP-008 - Incident Reporting and Response Planning	Early detection of attacker infrastructure and credential leaks shortens time-to-detect, feeding incident response plans and mandatory reporting timelines.
Safe Remediation	CIP-010 - Configuration Change Management & Vulnerability Assessments	Applies compensating controls and virtual patching so exposures are closed without the extended downtime operational technology environments cannot absorb.
Agentic Exposure Validation (AEV)	CIP-010 - Vulnerability Assessments / CIP-015 - Internal Network Security Monitoring	Continuously and safely validates whether an identified exposure is genuinely exploitable before any change touches a production control system.
Supply Chain Intelligence	CIP-013 - Supply Chain Risk Management	Monitors vendors and third-party infrastructure connected to the BES for breaches, leaked credentials, and compromise, supporting vendor risk assessments and the newer CIP-003-9 vendor remote access provisions.

This is a high-level overview for information purposes only and does not constitute a NERC CIP compliance determination. CIP scope, applicable requirements, and evidence standards depend on each BES Cyber System's impact rating under CIP-002 and on the entity's registration. Check Point Exposure Management contributes primarily to asset visibility, threat intelligence, vulnerability prioritization, and remediation; it does not replace OT-specific protocol monitoring or a formal NERC CIP compliance program. Organizations should consult their CIP Senior Manager and Regional Entity for scope-specific guidance.

COMPLIANCE MANDATE

CJIS Security Policy

Criminal Justice Information Services Security Policy • FBI CJIS Security Policy v6.0 • Regulatory Mandate (Federal)

The FBI's CJIS Security Policy sets minimum security requirements for any entity that creates, views, modifies, transmits, or stores Criminal Justice Information (CJI), including law enforcement agencies, criminal justice agencies, and the contractors and non-criminal-justice service providers that support them. The policy is organized into 13 policy areas covering everything from access control and incident response to configuration management, audits, and mobile devices.

Non-compliance can mean denial of access to FBI CJIS systems, contract loss, or criminal liability, which makes continuous, evidence-backed controls as important as the written policy itself. Check Point Exposure Management supports the policy areas most dependent on external visibility and fast, safe remediation.

Capability	CJIS Policy Area	How It Feeds In
Supply Chain Intelligence	Policy Area 1 - Information Exchange Agreements	Monitors vendors and subcontractors named in information exchange agreements for breach and compromise, supporting oversight of the broader partner ecosystem.
Threat Intelligence	Policy Area 3 - Incident Response	Early external warning, leaked data, attacker infrastructure, and impersonation, feeds incident response playbooks and the reporting timelines the policy requires.
Threat Intelligence	Policy Area 5 / 6 - Access Control & Identification and Authentication	Detects leaked or exposed credentials tied to accounts with CJI access, enabling revocation before compromised credentials are used against CJIS systems.
CAASM	Policy Area 7 - Configuration Management	Maintains a live inventory and configuration baseline of systems and networks that touch CJI, the foundation configuration management and change control depend on.
Safe Remediation	Policy Area 10 / 7 - Systems Protection & Configuration Management	Applies compensating controls and virtual patching to close exposures without waiting on formal patch cycles, keeping CJI-handling systems within policy continuously.
Vulnerability Prioritization	Policy Area 10 - Systems and Communications Protection and Information Integrity	Prioritizes vulnerabilities in systems and network boundaries that protect CJI in transit and at rest, based on real exploitability rather than static severity.
Agentic Exposure Validation (AEV)	Policy Area 11 - Formal Audits	Continuously validates that controls are actually holding, generating audit-ready evidence between the CJIS Systems Agency's periodic formal audits.

This is a high-level overview for information purposes only and does not constitute a CJIS Security Policy compliance determination. Formal compliance is assessed by the CJIS Systems Agency (CSA) or the relevant state Compact Officer, not by Check Point. Organizations should consult their CSA and CJIS Information Security Officer for scope-specific guidance.

COMPLIANCE MANDATE

SOC 2

System and Organization Controls 2 • AICPA Trust Services Criteria • Attestation Standard (Contractual)

SOC 2 is an AICPA attestation standard built around five Trust Services Criteria: Security (mandatory in every report), Availability, Confidentiality, Processing Integrity, and Privacy. Rather than a certification, a SOC 2 report is an independent CPA firm's opinion on whether an organization's controls are suitably designed (Type I) and operating effectively over a review period (Type II).

Because Security is the mandatory baseline and the most commonly extended criterion is Confidentiality, Check Point Exposure Management's continuous external visibility maps directly onto the evidence auditors look for.

Capability	Trust Services Criterion	How It Feeds In
CAASM & EASM	Security - Risk Assessment & Logical Access (CC3, CC6)	Grounds the risk assessment and access control scoping in a live inventory of the systems actually in scope for the audit.
Agentic Exposure Validation (AEV)	Security - Monitoring Activities (CC4, CC7.1)	Continuously validates that controls are operating effectively, generating evidence that spans the entire Type II review period rather than a point-in-time snapshot.
Threat Intelligence	Security - System Operations Monitoring (CC7)	Extends monitoring beyond internal logs to external indicators of compromise and leaked credentials targeting in-scope systems.
Vulnerability Prioritization	Security - Vulnerability Identification (CC7.1)	Correlates exploitability and business impact for vulnerabilities affecting the system boundary under audit, rather than treating every finding equally.
Safe Remediation	Security - Change Management (CC7.2, CC8)	Closes vulnerabilities through compensating controls and virtual patching, supporting timely remediation evidence without disrupting the availability customers were promised.
Threat Intelligence	Confidentiality	Monitors the open, deep, and dark web for leaked or offered-for-sale confidential data, directly supporting the Confidentiality criterion when it is in scope.
Safe Remediation	Availability	Reduces unplanned downtime from unpatched vulnerabilities, supporting uptime commitments when Availability is included in the report.

This is a high-level overview for information purposes only and does not constitute a SOC 2 attestation. SOC 2 scope, criteria selection, and the Type I or Type II opinion are determined by the engaging CPA firm; Check Point does not issue SOC 2 attestations. Organizations should consult their auditor for scope-specific guidance.

COMPLIANCE MANDATE

FISMA

Federal Information Security Modernization Act • 44 U.S.C. § 3551 et seq. (2014); NIST SP 800-53 • Regulatory Mandate (Federal)

FISMA requires U.S. federal agencies, and the contractors and service providers operating systems on their behalf, to implement and continuously monitor security controls drawn from NIST SP 800-53, selected according to the Risk Management Framework (RMF): Categorize, Select, Implement, Assess, Authorize, and Monitor. The 2014 modernization shifted the law's emphasis from periodic, paper-based certification toward continuous monitoring, and gave CISA operational authority over federal civilian cybersecurity.

Check Point Exposure Management supports the RMF steps most dependent on knowing the current asset inventory and threat exposure, turning FISMA's annual reporting cycle into continuous, evidence-backed monitoring between formal reauthorizations.

Capability	RMF Step / NIST 800-53 Family	How It Feeds In
CAASM & EASM	Categorize (RMF Step 1) / CM - Configuration Management	Maintains a live system and asset inventory that supports FIPS 199 categorization and keeps the System Security and Privacy Plan (SSPP) current.
Threat Intelligence	RA — Risk Assessment / SI - System and Information Integrity	Provides continuously updated external threat context, keeping risk assessments current between formal reauthorization cycles rather than relying on a point-in-time snapshot.
Vulnerability Prioritization & Agentic Exposure Validation (AEV)	RA-5 - Vulnerability Monitoring and Scanning	Correlates exploitability, reachability, and business impact, guiding remediation priority beyond static CVSS severity scores.
Safe Remediation	SI-2 - Flaw Remediation / CM-3 - Configuration Change Control	Applies compensating controls and virtual patching, supporting continuous monitoring (RMF Step 6) in the gap between formal authorization cycles.
Agentic Exposure Validation (AEV)	CA-7 - Continuous Monitoring / CA-8 - Penetration Testing	Continuously and safely validates whether identified exposures are genuinely exploitable, generating evidence for Plans of Action and Milestones (POA&Ms) and ongoing authorization.
Threat Intelligence	IR - Incident Response	Early detection of credential leaks and attacker infrastructure feeds the incident reporting agencies must provide to CISA under FISMA's breach notification requirements.

This is a high-level overview for information purposes only and does not constitute a FISMA compliance determination or authorization decision. Authorization to Operate (ATO) decisions rest with the agency's Authorizing Official, and NIST 800-53 control selection and testing must be validated by the agency's assessment team. Organizations should consult their agency CISO and Authorizing Official for scope-specific guidance. For current CISA guidance, see <https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act>.

Frameworks

CTEM, the NCSC Cyber Assessment Framework, NIST CSF 2.0, and CIS Controls v8 are voluntary or operational models organizations use to structure and communicate their security posture.

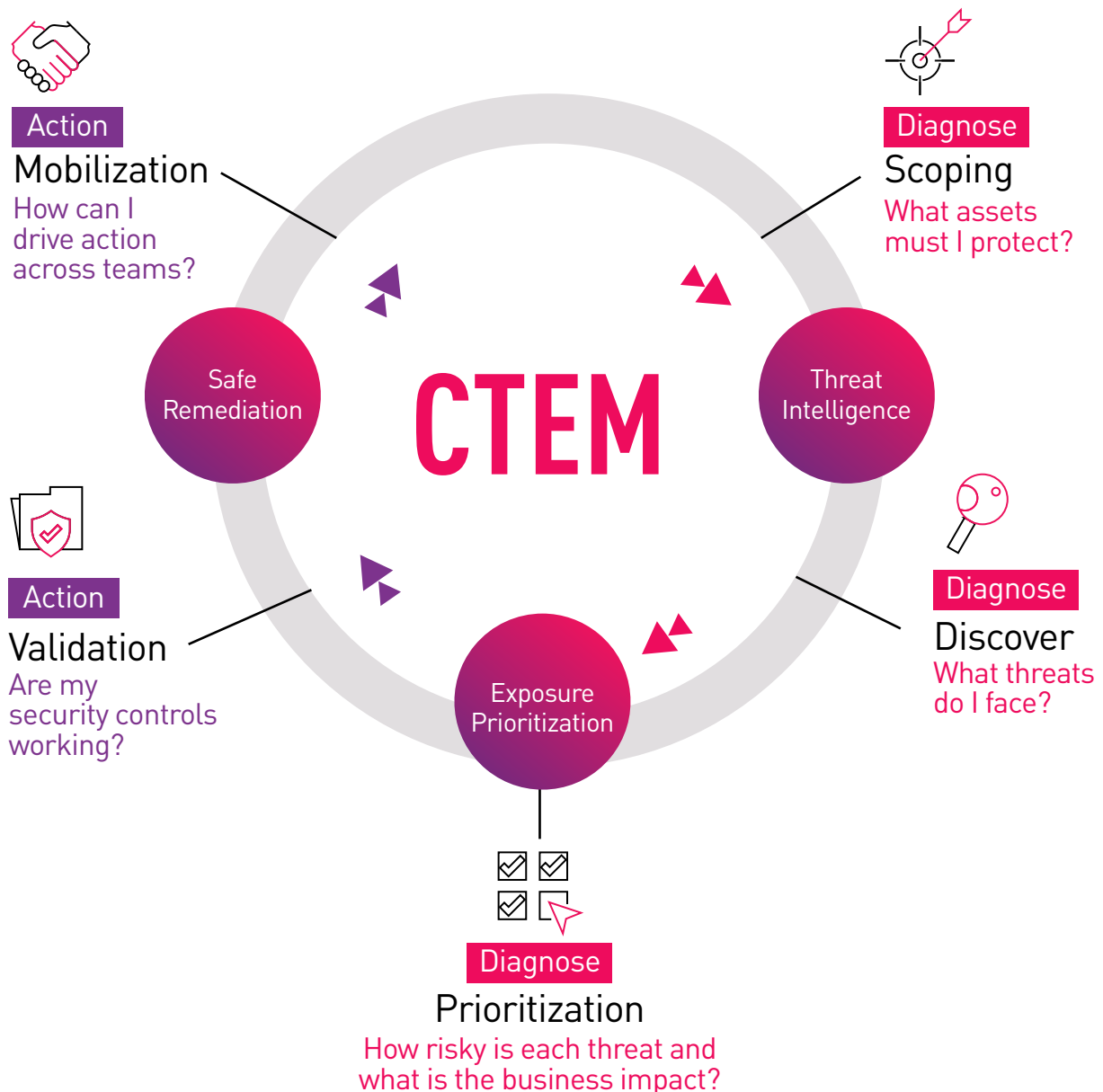
OPERATIONAL FRAMEWORK

CTEM

Continuous Threat Exposure Management • Gartner-originated model • Operational Strategy / Methodology

CTEM is the operational model Gartner introduced to describe how organizations should continuously scope, discover, prioritize, validate, and mobilize against exposure, rather than relying on periodic point-in-time assessments.

Check Point Exposure Management is built to operationalize CTEM directly: each stage of the lifecycle maps to a specific capability, so exposure moves from being merely known to being fixed.



CTEM Stage	Check Point Capability	What Happens
Scoping	CAASM & EASM	Maps the extended attack surface, including lookalike domains, supply chain vendors, cloud assets, and shadow IT/OT, so nothing relevant sits outside the program's view.
Discovery	Threat Intelligence	Surfaces risks tied to those assets, including leaked credentials, exposed services, misconfigurations, and brand or phishing abuse, across the open, deep, and dark web.
Prioritization	Vulnerability Prioritization & CAASM & Agentic Exposure Validation (AEV)	Correlates exploitability, reachability, active threat activity, asset criticality and business impact with cross-tool deduplication, so teams work the handful of exposures that actually matter.
Validation	Agentic Exposure Validation (AEV)	Actively and safely tests whether a proposed fix or a flagged exposure is real and whether remediation will disrupt the business before anything changes in production.
Mobilization	Safe Remediation & Brand Protection	Safely closes validated exposures through virtual patching, IPS activation, IoC dissemination, and takedowns, coordinated across the security stack without downtime.

CTEM is a strategic approach described by Gartner, not a certifiable standard or regulatory requirement. This overview reflects how Check Point Exposure Management operationalizes the model; organizations should consult their own risk program for how CTEM fits their broader security strategy.



NCSC CAF

NCSC Cyber Assessment Framework • UK National Cyber Security Centre • Government Assessment Framework

The UK's Cyber Assessment Framework was developed by the National Cyber Security Centre (NCSC) to help essential service providers and other organizations assess and improve their cyber resilience. It is especially relevant to those operating under the UK's NIS Regulations, though its principles apply across sectors.

CAF consists of four top-level objectives, broken into 14 principles, each with a set of outcomes an organization can assess itself against. Check Point Exposure Management contributes visibility, context, and early warning across multiple principles, reducing risk before it becomes an incident.

CAF Objective	CAF Principle	Check Point Contribution
A. Managing Security Risk	A.2 Risk Management	Threat-led insight into relevant attack trends, a live threat landscape view, and malware and threat actor intelligence that keep risk registers current.
A. Managing Security Risk	A.3 Asset Management	CAASM & EASM inventories digital assets and their connections; Threat Intelligence layers on alerts tied to exposed domains, assets, and credentials.
A. Managing Security Risk	A.4 Supply Chain	Continuous monitoring for third-party mentions, supplier breaches, and supplier-linked credential leaks or phishing domains.
B. Protecting Against Cyber Attack	B.2 Identity & Access Control	Compromised credential detection and exposure alerts flag access risks before they are used against the organization.
B. Protecting Against Cyber Attack	B.3 Data Security	Discovery of data leakage and data offered for sale across underground channels, giving early warning of exposure.
B. Protecting Against Cyber Attack	B.4 System Security	Vulnerability Prioritization tracks exploitability of flaws in software connected to external assets; Safe Remediation closes them without waiting on patch cycles.
C. Detecting Cyber Security Events	C.1 Security Monitoring	Continuous surface and dark web monitoring for attacker activity, infrastructure reuse, and campaign evolution.
C. Detecting Cyber Security Events	C.2 Threat Hunting	A threat hunting capability with access to a threat knowledgebase and raw data for faster hypothesis development.
D. Minimising Impact of Incidents	D.1 Response Planning	Playbooks tailored to ransomware, advanced persistent threats, and fraud scenarios support faster, more informed response. Safe Remediation to close risks ahead of time. Takedowns of ongoing brand impersonations and phishing.
D. Minimising Impact of Incidents	D.2 Lessons Learned	Analyst support for post-incident review and threat modeling strengthens the next iteration of defenses.

This is a high-level overview for information purposes only. The CAF is a self-assessment framework maintained by the NCSC; formal alignment and any regulatory determination under the UK NIS Regulations rests with the responsible regulator, not with Check Point.

VOLUNTARY FRAMEWORK

NIST CSF 2.0

NIST Cybersecurity Framework, Version 2.0 • National Institute of Standards and Technology •
Voluntary Security Framework

NIST CSF 2.0 provides a high-level, outcome-based taxonomy for managing cybersecurity risk, organized into six functions: Govern, Identify, Protect, Detect, Respond, and Recover. It is voluntary and sector-agnostic, widely used as a common language between security teams, executives, and boards.

Check Point Exposure Management maps naturally onto this taxonomy because its five capabilities already follow the same identify-protect-detect-respond arc, extended outward to cover the external attack surface.

CSF 2.0 Function	Check Point Capability	How It Feeds In
Govern	CAASM & EASM & Threat Intelligence	Give the management body a single, current view of asset inventory and external exposure, supporting risk-informed decisions and board-level oversight.
Identify	CAASM & EASM	Builds and maintains a live inventory of assets across cloud, on-premises, OT, and SaaS, the foundation any risk assessment needs to identify what could be affected.
Identify	Threat Intelligence	Identifies external threat sources, exploited vulnerabilities, and attacker infrastructure relevant to the organization's sector and footprint.
Protect	Safe Remediation	Applies compensating controls, virtual patching, and secure configuration fixes across the multi-vendor stack, protecting systems without waiting on patch cycles.
Protect	Vulnerability Prioritization	Guides which protective controls matter most by correlating exploitability, reachability, and business impact.
Detect	Threat Intelligence	Continuously monitors the open, deep, and dark web for leaked credentials, phishing infrastructure, and threat actor activity targeting the organization.
Respond	Agentic Exposure Validation (AEV) & Safe Remediation	Validates whether a finding is genuinely exploitable and coordinates safe, fast remediation across security tools already in place.
Recover	Safe Remediation	Automates routine hardening and remediation actions that restore systems to a secure baseline after an exposure is closed.

This is a high-level overview for information purposes only. NIST CSF 2.0 is voluntary guidance, not a certifiable standard; organizations determine their own target profile and tier based on risk tolerance and resources.

VOLUNTARY FRAMEWORK

CIS Controls v8

CIS Critical Security Controls, Version 8 • Center for Internet Security • Voluntary Security Framework

The CIS Critical Security Controls are a prioritized set of 18 safeguards designed to stop the most common and impactful cyber attacks. They are widely used as a practical, implementation-focused complement to higher-level frameworks like NIST CSF.

Check Point Exposure Management directly supports the controls most dependent on knowing what exists, what is exposed, and closing that gap quickly.

CIS Control	Check Point Capability	How It Feeds In
CIS Control 1 - Inventory and Control of Enterprise Assets	CAASM & EASM	Builds a live, owned inventory of every asset across cloud, on-premises, OT, and SaaS, including unmanaged and shadow IT.
CIS Control 5 - Account Management & CIS Control 6 - Access Control Management	Threat Intelligence	Surfaces leaked and exposed credentials tied to the organization, enabling revocation before compromised accounts are used.
CIS Control 7 - Continuous Vulnerability Management	Vulnerability Prioritization & CAASM & Agentic Exposure Validation (AEV)	Correlates exploitability, reachability, threat activity, asset criticality and business impact across the multi-vendor stack, replacing static severity scores with real prioritization.
CIS Control 8 - Audit Log Management	Threat Intelligence	Extends monitoring beyond internal logs to external indicators of compromise and threat actor infrastructure targeting the organization.
CIS Control 15 - Service Provider Management	Threat Intelligence	Continuously monitors for third-party and supply chain risk, including supplier breaches and vendor-linked credential leaks.
CIS Control 16 - Application Software Security	Vulnerability Prioritization & Safe Remediation	Flags exploitable flaws in externally facing software and applies compensating controls or virtual patching while a permanent fix is developed.
CIS Control 17 - Incident Response Management	Threat Intelligence & Safe Remediation	Early detection of credential leaks, impersonation, and attacker infrastructure feeds directly into incident response playbooks and speeds containment.
CIS Control 18 - Penetration Testing	Agentic Exposure Validation (AEV)	Complements periodic penetration testing with continuous, automated validation of whether exposures are genuinely exploitable.

This is a high-level overview for information purposes only. CIS Controls v8 is voluntary guidance maintained by the Center for Internet Security; organizations should map their own Implementation Group and control selection to their risk profile.

CONCLUSION

The twelve mandates and frameworks in this guide differ in almost everything that matters legally: who they apply to, what they require, and what happens on failure. What they share is a dependence on the same underlying questions. What exists. What is exposed. What's critical and exposed. What can be fixed, safely, before it is exploited.

Check Point Exposure Management answers those questions once, continuously, through Threat Intelligence, CAASM, Vulnerability Prioritization, Agentic Exposure Validation, and Safe Remediation.

Organizations do not need a separate program for every regulator or framework; they need one continuous exposure management loop that produces evidence all of them recognize.

As DORA's regulatory technical standards mature, as EU member states finish transposing NIS2, as PCI DSS enforcement continues under v4.0.1, and as new frameworks emerge, this guide will be updated to keep the mapping current. Teams using this guide for a specific audit, assessment, or board report should confirm the latest requirement language with the source regulator or standards body, and treat the chapter disclaimers as a starting point for that conversation, not a substitute for it.

ABOUT CHECK POINT EXPOSURE MANAGEMENT

Check Point's exposure management changes the game.

We combine billions of internal telemetry points with billions of external signals from the open, deep, and dark web to deliver a unified intelligence fabric. This provides clear visibility across the full attack surface, including brand risk.

The industry is moving from fragmented feeds to real context and real priorities. We support that shift through active threat validation, confirmation of compensating controls, and deduplication across tools, so teams can focus on what actually matters.

With safe-by-design remediation, fixes aren't just assigned, they're implemented. Every fix is validated before enforcement, enabling measurable risk reduction without downtime.

Gartner predicts organizations adopting continuous threat exposure management with mobilization will see 50% fewer successful attacks by 2028. We're leading that shift with action, not just tickets, and Fortune 500 organizations across major industries already rely on Check Point Exposure Management.

For more information visit: checkpoint.com/exposure-management

© Check Point, 2026. All Rights Reserved.