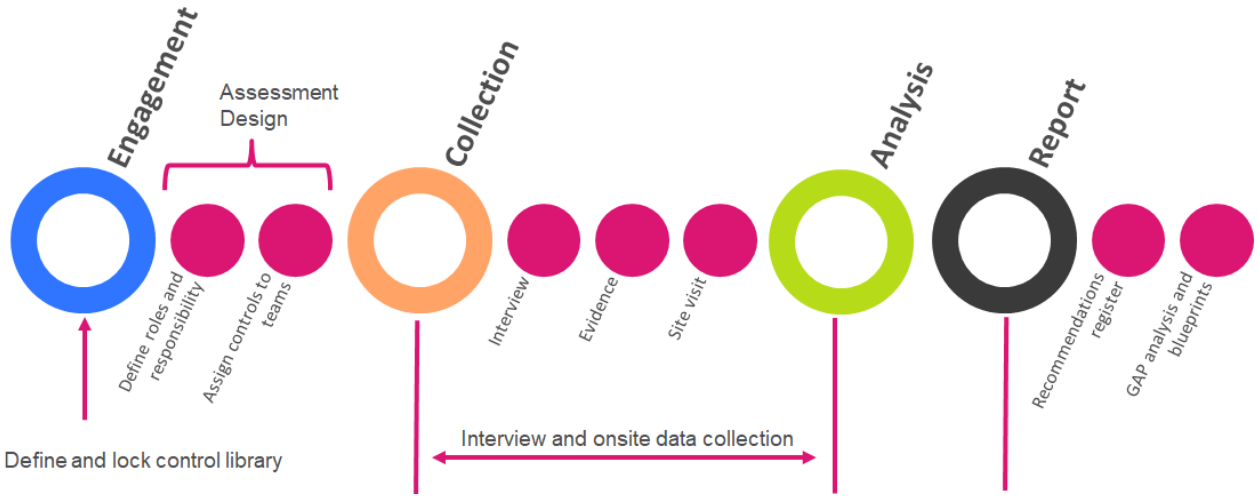
NIST CSF Assessment

With over three decades of unparalleled experience in cyberspace, Check Point brings a wealth of knowledge and expertise to the forefront. This extensive history allows us to excel in the realm of pure-play consultancy, offering unparalleled guidance and solutions to address your cybersecurity needs with confidence and precision. Check Points Control-led Compliance Assessment is designed to assess how well an organization seeks alignment with industry standard NIST CSF.



NIST CSF Assessment benefits

Our assessments are based on the NIST CSF v1 framework (CSF version 2 is also available upon request) and are vendor-agnostic and evidence-led. The entire process and engagement is designed to help you translate your current compliance and cyber security posture into a universal gap analysis that can assist with key decision-making and communication to a wider audience of cyber security stakeholders.

The assessment will focus on the following key areas:

- Organisation-wide assessment based on industry standards (NIST CSF) for managing compliance and control gaps within information security, and from this, infer the likelihood of a loss event.
- Baseline the “as-is” and “to-be” cyber security controls to correctly define what improvements can be made and how effective the actions will be.
- Analyze the client’s Detect, Protect, Response, and Recovery controls and make practical recommendations for improvements.
- Define a mitigation plan as to how ‘control’ failures can be remediated so that the overall security posture is uplifted.

The assessment follows a proven and leading industry process (methodology):

- **Design Assessment Parameters**: Assess clients' current cybersecurity maturity levels based on the CSF Implementation Tiers (Partial, Risk Informed, Repeatable, Adaptive)
- **Identify and Prioritize Assets**: Identify and prioritize critical assets, systems, data, and processes within the client's organization. Understanding what needs protection is important and of value is an important first step, as is not applying controls to non-critical assets.
- **Conduct the Current State Assessment**: Evaluate the current state of clients' cybersecurity practices and, where necessary, collect evidence. This involves assessing existing policies, procedures, controls, and technologies based on observation and interview.
- **GAP Analysis:** Develop a GAP analysis representing the desired state of cybersecurity (target architecture) that can be mapped to the existing state. This involves setting specific goals and outcomes for each CSF core function based on your risk appetite, priorities, motivation, and cost.
- **Identify and Implement Improvements**: Develop a roadmap for implementing improvements based on the framework profile. This may involve updating policies, enhancing technical controls, or implementing new processes.

The process:

Define the likelihood of a loss event based on the capabilities and motivation of real-world bad actors

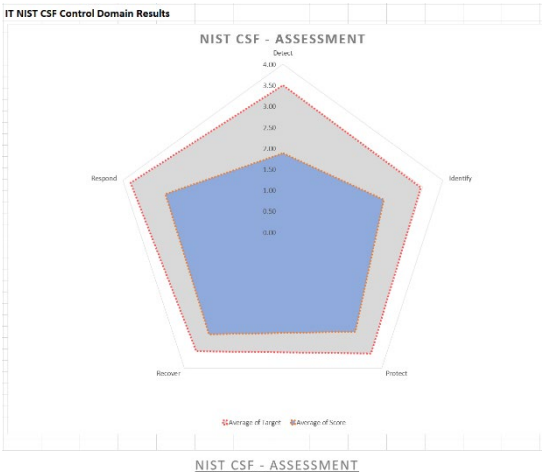
SCOPE	Plan and collect	Assessment	ANALSYIS	REPORT
NDA signed and controls aligned with relevant internal teams	Collect preliminary data, including attack surface scan data	Onsite interview and evidence gathering	Data gathering and interviews Whiteboarding and review.	Report delivery with findings analysis and remediation, includinggap analysis and detailed recommendations.
4-6 weeks before	1 days	3 days	10 days	1 day

Deliverables

The delivery of our assessment includes a commitment by the consulting team to deliver the following artifacts and services.

1. The workshops will be conducted on-site as agreed upon between the Customer and Check Point.
2. Complete the NIST Assessment Report (Industry standard format).
3. Technology gap analysis

4. Failed control Register and recommendations to high-level design) technical depth. Where possible, the team will endeavor to provide a plan of action and milestones (POAM) that can be achieved using known or available resources.
5. C-level / Board room presentation delivered in person by the lead consultant
6. Access to the Check Point Assessment portal (valid for 1 year) to allow the client team access to all controls and analysis tools.



Control Family	Control Description	Control Label	Question	Remarks	Current Score	Target Score
Protect	Identity Management, Authentication and Access Control	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	Current infrastructure is based on a flat network which is shared between the all assests including users and servers. Efforts are being made by the team to increase network segmentation and new data flows are being documented accordingly	2	4
Protect	Data Security	PR.DS-1	Data-at-rest is protected	HP drive lock is used for laptops and computers, but encryption is by user/master password, no ability to change passwords frequently. Servers have no data encryption.	2	4
Protect	Data Security	PR.DS-5	Protections against data leaks are implemented	By policy no data is to be saved on devices, but this policy is not enforced. No DLP is being used.	1	4
Protect	Data Security	PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity	No automatic tools, just manual checks	2	4
Protect	Information Protection Processes and Procedures	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	IT and OT are seperated by network, but no security controls on the ICS side are implemented	1	3

Most Relevant for

- Organizations seeking compliance with the NIST CSF
- Security datelining and confidence planning
- C-level are reporting
- Digital Transformation Planning

Contact Us

Schedule a consultation to discuss how we can fortify your cyber defenses.
https://www.checkpoint.com/services/infinity-global/contact-security-expert/