Stack

Stack Cybersecurity Maturity Assessment

- Sample Report

Introduction to Stack's Sample CSMA Report

Stack's Cybersecurity Maturity Assessment (CSMA) provides a structured way to evaluate and improve your organization's Cybersecurity posture. Our assessment focuses on:

- Gathering a snapshot of current capabilities across key areas
- Identifying gaps compared to Cybersecurity best practices
- Providing a prioritized roadmap to strengthen defences

Our CSMA is based on leading industry frameworks, including:

- NIST Cybersecurity Framework (CSF) - provides a model to assess and manage Cybersecurity risks across operational technology and business systems.
- Center for Internet Security (CIS) Controls - a concise, prioritized set of cyber defense measures with focus on real-world attacks.
- C2M2 Maturity Model - methodology to evaluate Cybersecurity maturity across 10 domains of operations.
- ISO 27001 - international standard for implementing and operating an information security management system.
- UK Cyber Essentials - government-backed certification focusing on 5 key technical controls.

Through interviews, document review, discussions, and tools, we evaluate your current maturity across the 10 C2M2 domains. This allows us to quickly identify major gaps.
We then map those gaps to Cybersecurity Framework Functions and the targeted security outcomes they support. Remediation priorities are based on mapping to the CIS Controls. This allows us to provide a pragmatic roadmap.

For this assessment spanning 7 working days, we focus on high-level reviews of each domain, major gap identification, and an initial 12-month roadmap centred on the most important CIS Controls. We recommend recurring assessments every 6 months to track progress. This combined methodology allows for quick but comprehensive benchmarking against industry best practices - resulting in a risk-focused, priority-driven plan to strengthen your Cybersecurity.

Stack

CONTENTS

CONTENTS

INTRODUCTION

[Client] has partnered with Stack to assess its Cybersecurity maturity and identify areas for improvement. Stack conducted interviews and workshops with key [Client] staff to gauge current security practices and controls across the organisation. This report summarises Stack's findings, highlights gaps, and provides prioritised recommendations to enhance [Client's] cyber resilience. The goal is to establish a clear roadmap for [Client] to methodically strengthen its security posture in line with industry best practices.

STACK'S APPROACH TO CYBERSECURITY

Effective Cybersecurity requires a structured approach that balances people, process, and technology controls. At Stack, our methodology is based on the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework and the U.K. Cyber Essentials Scheme.

We use the Cybersecurity Capability Maturity Model (C2M2) to evaluate current maturity across key domains based on established practices set out under the model. The Centre for Internet Security (CIS) Critical Security Controls (CSC) provide the technical control baseline aligned to the top threats.

This combined approach allows us to:

- Quickly identify gaps in people, process, and technology controls
- Prioritise high-impact, high-value improvements
- Develop an incremental roadmap tailored to the client's risk profile
- Track progress through iterative maturity assessments
- Demonstrate compliance with UK regulatory requirements

CYBERSECURITY MATURITY ASSESSMENT

The C2M2 assessment provides a snapshot of [Client's] current security capabilities across 11 domains. Overall, many foundational practices are in place, though some key enhancement opportunities exist.
The results highlight strengths in Identity and Access Management, Workforce Management, and Asset Management. Gaps appear primarily in formalising processes, implementing managerial controls, and developing a Cybersecurity program strategy.

With the recommended improvements, [Client] can reach a Cybersecurity maturity level of 2 across critical domains within 18 months. This lays the groundwork for proactive, adaptive security.

GAP ANALYSIS FEEDBACK

[Summarise key gaps discovered across the 11 C2M2 domains]

RECOMMENDATIONS BY DOMAIN

Risk Management (RM)

- Develop an overarching Cybersecurity strategy based on business risks
- Perform cyber risk assessments tied to business processes and assets
- Prioritise risks and document risk treatment plans
- Implement a risk register and monitor/review regularly
- Involve stakeholders in risk strategy and assessments

Asset, Change and Configuration Management

- Adopt CIS configuration baselines for servers and infrastructure
- Classify critical assets supporting key business functions
- Document asset management, change and configuration policies
- Include security stakeholders in change processes
- Verify security compliance during asset lifecycle events

Identity and Access Management

- Set access revocation timescales for leavers
- Expand privileged account monitoring
- Document access management policies and procedures

Threat and Vulnerability Management

- Verify external provider is delivering actionable threat intelligence
- Analyse relevant threats and adjust controls/monitoring
- Update risk register based on new threat information
- Perform regular internal vulnerability scans
- Document TVM policies and procedures

Situational Awareness

- Identify all log sources required for monitoring
- Define service requirements for external provider
- Establish reporting requirements and formats
- Define security event severity thresholds
- Verify staff understand roles in incident response

Information Sharing and Communication

- Address Cybersecurity in business continuity plans
- Document information sharing processes
- Define requirements for sharing threat data

Event and Incident Response, Continuity of Operations

- Classify Cybersecurity events/incidents
- Log and track security incidents
- Identify and train incident response personnel
- Develop and test cyber incident response plans
- Include Cybersecurity in business continuity plans
- Set RTOs and RPOs for prioritised assets

Supply Chain and External Dependencies Management

- Map suppliers/partners and identify risks
- Assess supplier Cybersecurity posture
- Document supply chain risk processes
- Include supply chain risks in register

Workforce Management

- Define and document Cybersecurity roles
- Deliver training for personnel in key roles
- Provide Cybersecurity awareness training
- Set hiring criteria for roles with security duties
- Create workforce Cybersecurity policies

Cybersecurity Program Management

- Gain executive support and sponsorship
- Develop a Cybersecurity architecture
- Establish metrics based on industry frameworks
- Document a roadmap for capability improvement

CRITICAL SECURITY CONTROLS IMPLEMENTATION

Alongside maturity improvements, Stack recommends adopting the Center for Internet Security (CIS) Critical Security Controls (CSC) as a prioritised set of technical security measures.
The controls provide a proven, high-impact starting point based on real-world attack data that is maintained by a global community of experts.

Stack has mapped the controls to the Cybersecurity Framework (CSF) to derive a set of controls tailored to [Client's] needs and maturity level. We recommend focusing initially on basic hygiene measures in the first 5 control groups:

- CSC 1: Inventory of Authorised and Unauthorised Devices
- CSC 2: Inventory of Authorised and Unauthorised Software
- CSC 3: Secure Configurations for Hardware and Software
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges

Stack will provide guidance and tools to implement these controls, then measure effectiveness using agreed metrics based on industry standards. As maturity increases, additional controls can be added incrementally.

REPORTING AND PROGRESS TRACKING

To monitor progress, Stack will conduct recurring maturity assessments every 6 months using C2M2 and provide formal reports to [Client] leadership. We will also generate metrics tied to the CIS Controls.

This provides continuous visibility into capability improvements, control effectiveness, residual risk, and overall cyber resilience. It enables data-driven decisions on security priorities and investments.

REFERENCES

To monitor progress, Stack will conduct recurring maturity assessments every 6 months using C2M2 and provide formal reports to [Client] leadership. We will also generate metrics tied to the CIS Controls.

This provides continuous visibility into capability improvements, control effectiveness, residual risk, and overall cyber resilience. It enables data-driven decisions on security priorities and investments.

Find out Your Cybersecurity Maturity Level Now and Shield Your Business from Online Threats!

Don't Wait Any Longer -

Schedule Your Cybersecurity Maturity Assessment Today!

2nd Floor, 30 Churchill Place,
Canary Wharf, London, E14
5RE

www.gostack.co.uk