Current State Cyber Security Assessment

Sample Findings Report

Iridium

Contents

Introduction

This sample report is based on a genuine current state cyber security assessment that Iridium carried out for a major UK organisation in early 2020, with all sensitive and confidential information removed or edited. This provides an insight into the level of detail we assess, analyse and report on, whilst demonstrating exactly what each client can expect when they choose to work with us.

In order to create your bespoke current state cyber security assessment, we will undertake a complimentary, half-day, pre-assessment scoping session. The final assesment will also include an executive summary and a detailed remediation report, which will outline the steps Iridium would take to resolve issues identified within the assesment.

If you have any questions or would like to discuss a current state assessment for your business, please contact Ben.Dainton@ir77.co.uk

Executive Summary and Remediation Plan

An executive summary, consumable at CxO level, as well as a detailed remediation plan of how Iridium can help to reduce risks and increase maturity, accompanies all of our current state cyber security assessment reports.

As part of the executive summary, we will visualise how people, process and technology remediation recommendations will actively improve your cyber security posture.

1 Background

The free initial half-day scoping session will be undertaken by Iridium cyber security specialists and business analysts. The objective of this is to determine the breadth of work, timeframe and to create a detailed, bespoke proposal. This would be followed by a comprehensive health check of the business's information security maturity and posture, carried out by Iridium in conjunction with the client.

Assessments are undertaken in accordance with the relevant controls of the NIST-CSF framework, outlined in detail in section 2, and are performed in the three phases described.

Current state cyber security assessments can be conducted over the full three phases, or the first two phases; Preparation & Health Check.

This sample report comprises the first two phases of a current state cyber security assessment. The resulting maturity ratings are, therefore, a representation of each control's design effectiveness (e.g. how well people believe the controls are defined), as opposed to their operational effectiveness (e.g. sample testing of how the controls are applied in practice), which would be covered in the Audit phase.

Appendices available at the end of this report include the schedule of interviews and full risk table.

A current state assessment is conducted in three phases:

Assessment Phases	Brief Description	Status
Preparation Phase	Pre-work required to undertake assessment (e.g. assessment work-book production, meeting arrangements etc.).	This section would be tailored to the specific client.
Health Check Phase	Conduct stakeholder interviews and assess any supporting documentation against each aspect of the NIST-CSF assessment workbook. Establish initial view of current state maturity and key gaps / risks.	
Audit Phase	Deep dive assessment of the functions that score between 3-5 on the maturity scale, in order to provide a deeper understanding of operational effectiveness.	

2 Assessment Framework

Reports are compiled against the NIST-CSF framework detailed below. This framework is a set of best practices, standards and recommendations that help an organisation improve its cyber security measures.

Categories (Pillars):

	Identify	Protect	Detect	Respond	Recover	Other
Functions	Identify potential cyber security risks to your information assets.	Protect yourself against these risks by developing and implementing safeguards.	Detect any irregular activity to determine if breaches have occurred.	Respond to any detected breaches to contain their impact.	Recover from these breaches by restoring any undermined assets.	Additional control areas, over and above those in NIST-CSF.
Categories	Asset Management	Access Control	Anomalies & Events	Response Planning	Recovery Planning	Mobile Data
	Business Environment	Awareness Training	Security Continuous Monitoring	Communications	Improvements	Secure by Design
	Governance	Data Security	Data Processes	Analysis	Communications	Proactive Event Discovery
	Risk Management	Info Protection & Procedures		Mitigation		Cloud Security Controls
	Risk Management Strategy	Maintenance		Improvements		
	Supply Chain Risk Management	Protective Technology				

Maturity Rating:

Each Category is given a maturity rating in accordance with the below NIST-CSF standards.

Level 0 – Non-existent	Level 1 – Initial	Level 2 – Ad-hoc	Level 3 – Defined	Level 4 – Managed	Level 5 – Optimised
No policies, standards or procedures in place.	Policies or standards drafted but not formally communicated.	Policies or standards approved but not formally adopted across the organisation.	Policies or standards approved but evidence of significant non-adherence / exceptions.	Policies or standards approved and adopted with non-adherence / exceptions c.5%.	Policies or standards approved and adopted with non-adherence / exceptions less than .5%.

3 Overall Maturity Summary

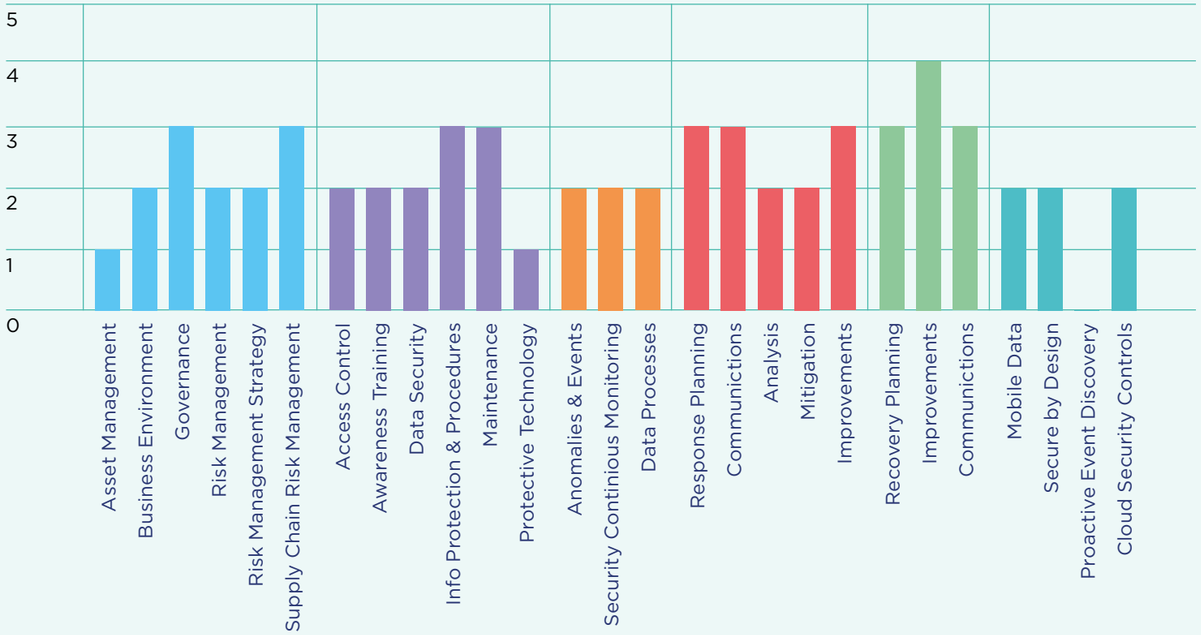
3.1 Maturity Assessment Ratings

A maturity assessment rating is provided for each of the 6 main NIST-CSF categories detailed below. The rating is derived from the mean average of the total number of sub-categories.

- Identify
- Protect
- Detect
- Respond
- Recover
- Other

The following chart outlines the average maturity score assigned to each sub-category of the above.

Current State Maturity Assessment
— Average maturity per function / category



3.2 Key Findings

A summary of the key findings of the security maturity assessment includes key strengths, weaknesses and recommendations.

In this section, we provide an overall maturity rating for the organisation, details of what this actually demonstrates and potential implications for a client's business.

The detailed findings, risks and remediation activities can be found in section 4 of this report, with further detail in the assessment workbook.

3.2.1 Key Strengths

Where there is a visibly high degree of people/process/technology in place, it will be noted here.

3.2.2 Key Weaknesses

The key weaknesses identified will be noted here, and these will link directly to the highest risk, along with the lower maturity scores

Note: - A deeper-dive assessment into the true operational effectiveness of the identified risks in this section would be required in order to fully understand and quantify the impact of these risks.

3.2.3 Recommendations

A clearly defined set of remediation activities (short and longer term) for each of the 6 NIST-CSF categories will be recommended. These will be linked to the findings and identified risks.

At this stage, Iridium will establish a remediation plan and implimentation roadmap to enable clients to consider steps needed to improve their security posture and reduce risks:

1) Remediate maturity rating 0-2 using a risk-based approach. Each of the key risks that have been identified are prioritised based upon their probability of occurance and potential impact, in order to deliver maximum benefit.

2) Audit maturity rating 3-5 in order to validate existing scores. Testing the operational effectiveness of the policies that are in place would provide the business with the confidence necessary for widespread adoption and enforced adherence. It is worth noting that if adoption was then sponsored at an executive level, this would act as a catalyst for wider cultural change. This is the key to achieving advanced (4 & 5) maturity scores.

Note: The Audit phase will often be outside of scope as part of the initial health check assessment.

3.3 Key Risk Matrix

The 16-box risk model below highlights the highest-rated risks identified as part of the maturity assessment.

They are categorised against probability versus impact, with a score of 16 being the highest, and 1 being the lowest.

3.4 Summary Table of Highest Rated Risks

The highest-rated risks will be detailed in the table below along with a reference to the specific NIST-CSF control(s). A full table will be included in the appendices at the back of this report.

Risk Assessment Methodology

Probability (of a threat occurring):
1 = Rare
2 = Unlikely
3 = Possible
4 = Probable

Impact (should a threat materialise)
1 = Low
2 = Medium
3 = High
4 = Very High

Risk ID	Risk Title	Business Risk	Probability	Impact	Risk Rating
RA–1	Specific to client				Very High
RA–2	Specific to client				Very High
RA–3	Specific to client				Very High

Risk ID	Volume of Associated Controls					
	Identify	Protect	Detect	Respond	Recover	Other
RA–1						
RA–2						
RA–3						

4 Detailed Findings

This section would be divided into six functions, one per each category of the NIST- CSF framework (as below):

Identify — 27 categories / subcategories assessed

Identify is aimed at establishing the organisational understanding to successfully manage information security across assets – including data, systems, hardware and processes.

Protect — 37 categories / subcategories assessed

Protect addresses the need to develop and implement controls to ensure continued delivery of core business services.

Detect — 17 categories / subcategories assessed

Detect is concerned with ensuring the right controls are in place to identify an information security event.

Respond — 16 categories / subcategories assessed

Respond ensures that the correct controls and approach are in place to react to an identified information security event.

Recover — 6 categories / subcategories assessed

Recover ensures that following a robust response to an information security incident, the correct approach is in place to restore impacted services and review procedures to learn from the events that occurred.

Other Controls — 19 categories / subcategories assessed

This section covers additional control areas, over and above those in NIST-CSF, that Iridium may beleive should be included in the current state assessment (e.g. cloud related controls).

Each of the above six functions will be reported on following the structure overpage.

4.1 Associated risks

For each function, a graph such as the example below, will provide a view of the maturity rating of each category/sub-category assessed, with the specific category codes expanded beneath each graph*.

4.2 Key Findings

An in-depth and detailed summary will be provided in this section against the key categories assessed.

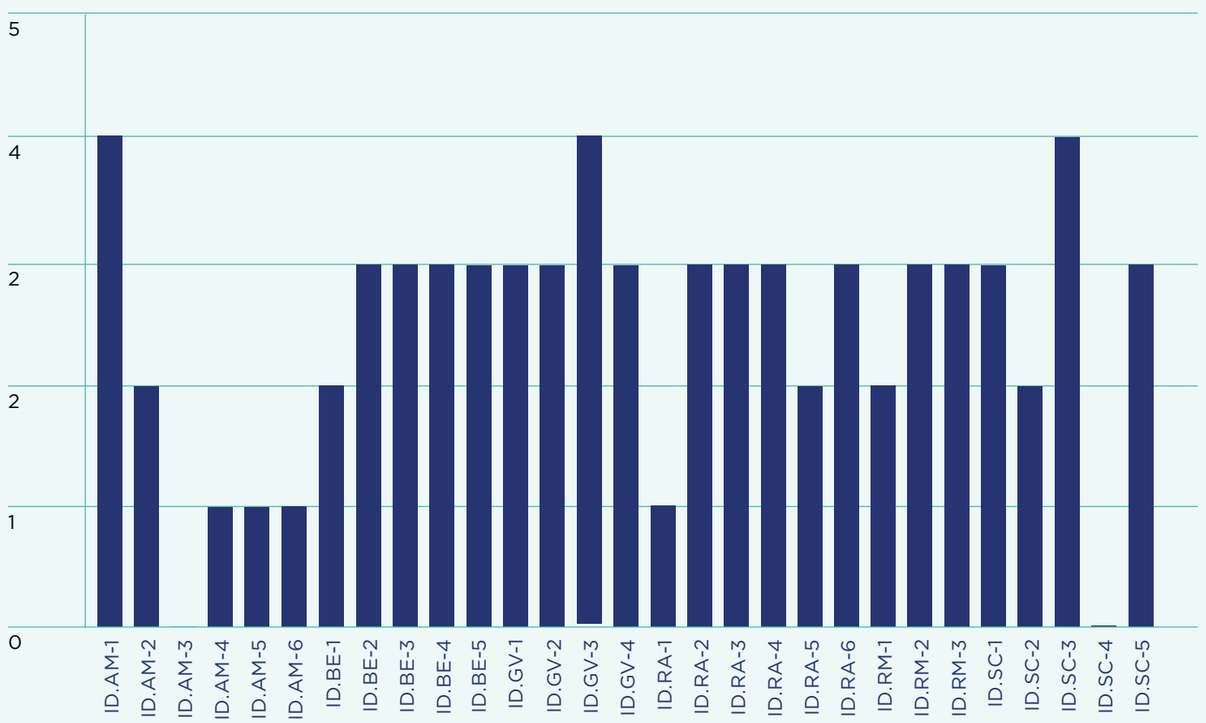
4.3 Associated Risks

The risks highlighted will link directly to the key findings.

4.4 Remediation

Our short-term (<12 months) and long term (>12 months) remediation activities will be detailed in this section.

Identify — Maturity per function — category / sub-category



*In order to help provide traceability to the underlying Assessment Workbook, each key finding has been linked to the applicable function > category > sub-category of the workbook which is coded as follows: [ID.AM-n].

5 Appendices

5.1 Schedule of stakeholder interviews

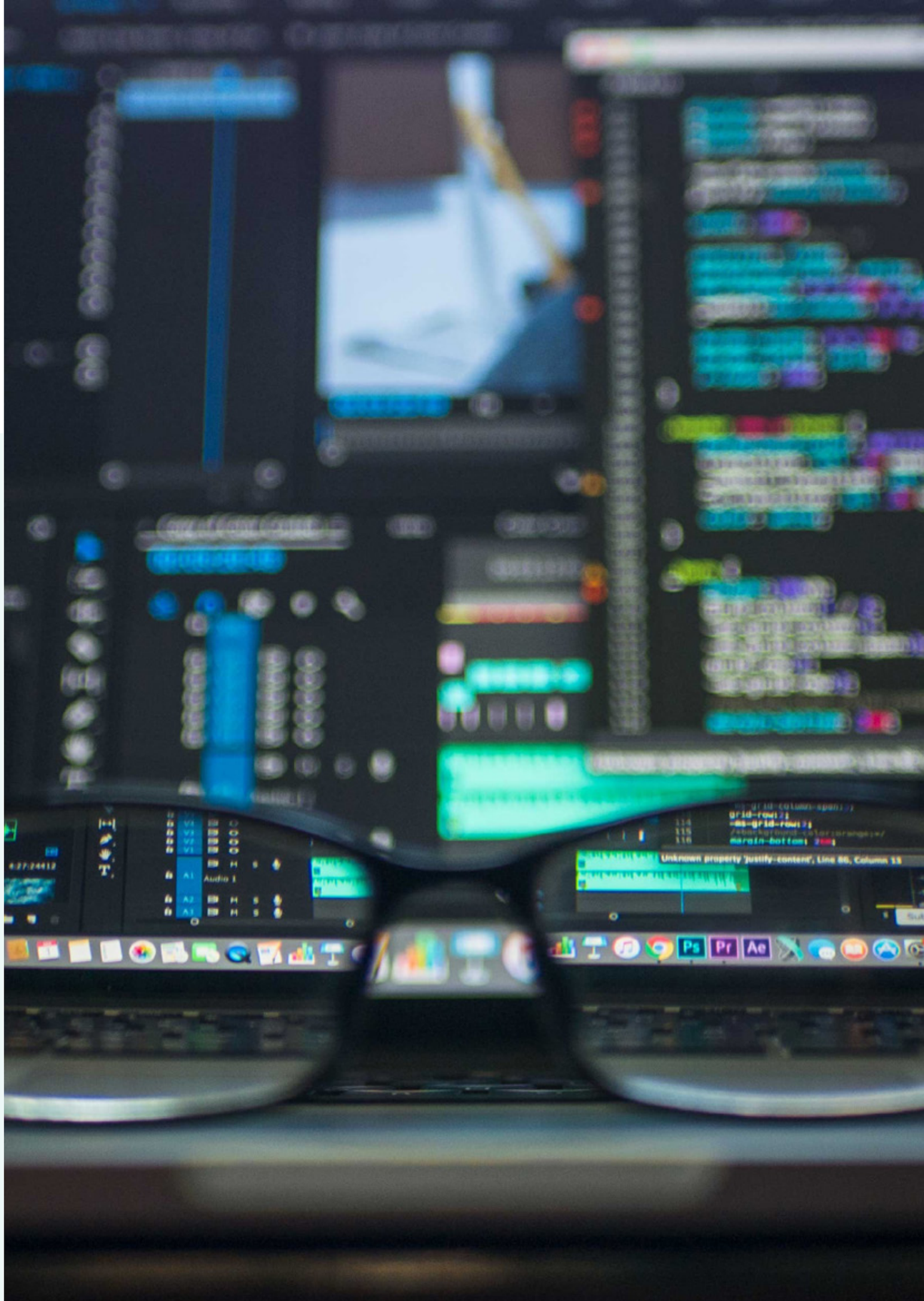
The following table details the various sessions held during the Health Check phase:

5.2 Key Risks Table

Client Attendees	Date	Topics Discussed	Status

Risk ID	Risk Title	Business Risk	Probability	Impact	Risk Rating
RA–1	Specific to client				
RA–2	Specific to client				
RA–3	Specific to client				

Risk ID	Volume of Associated Controls					
	Identify	Protect	Detect	Respond	Recover	Other
RA–1						
RA–2						
RA–3						



Iridium

Avenue HQ
10-12 East Parade
Leeds, West Yorkshire
LS1 2BH

enquiries@ir77.co.uk
0800 1931677

Follow us
iridium-consulting-ir77-limited

77
Ir