



Security and Resilience Assessment Workshop (SaRA)

Prepared for Customer

Why perform a Security & Resilience Assessment?

Improve your cyber security and cyber resilience by:

- Understanding how to **mitigate the growing cyber threat**
- **Ensure business continuity and recovery** after an incident
- Match technology capabilities against **regulatory requirements**
- foster your teams' **awareness to cyber attacks**

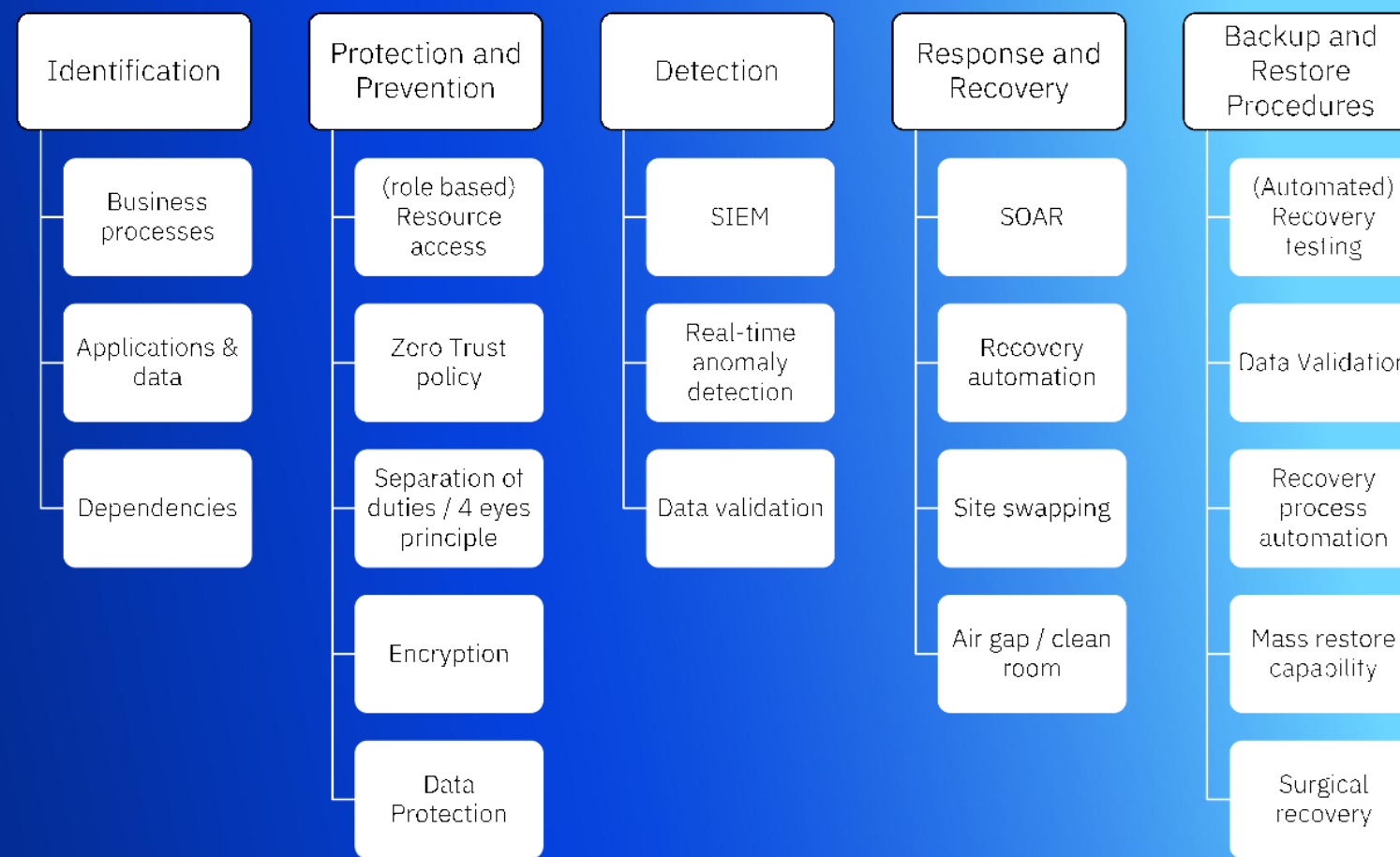
It helps to:

- Identify **blind spots** and recommended areas for improvement
- Develop a customized **Cyber Resilience** or **Operational Resilience strategy** fitting your vision & mission
- Identify **gaps, strengths, and weaknesses**

The assessment is based on

- **best practices**
- **NIST Cyber Security Framework V2**
- **EU DORA**

It is vendor agnostic and non-intrusive



Start with a Short Assessment:

- Answer a few questions in max. 10 minutes
- Your individual Report can be downloaded immediately
- You can request the full assessment from here



Identify & Protect

How exposed to risk do you think you are?

Not at all

Somewhat

I don't know

Quite

Very

Detect & Respond

How often do you run vulnerability scans and penetration testing?

Never

Rarely

I don't know

Often

Regularly

Recover

In the event of a cyberattack do you know how long it would take to make your company operational again?

Definitely Not

Probably Not

I don't know

Probably

Definitely

Compliance

Are your solutions compliant with relevant industry security standards?

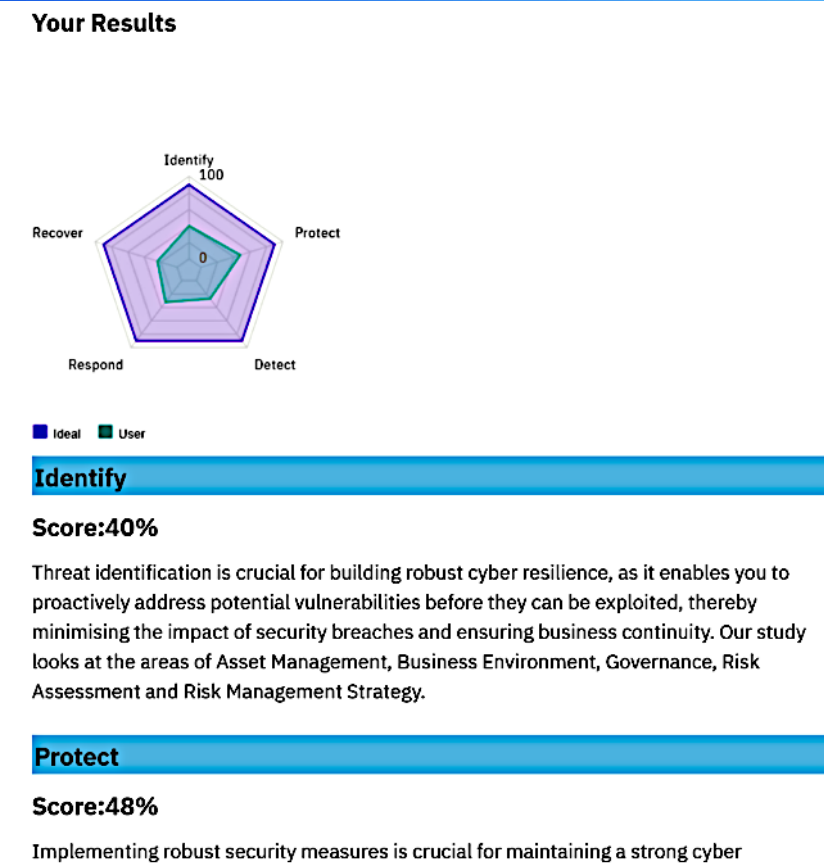
Definitely Not

Probably Not

I don't know

Probably

Definitely



What does the SaRA assessment deliver?

It delivers:

01

A technology agnostic maturity assessment

02

A view on the organisation, processes, and strategies regarding operational and cyber resilience

03

A better cross team understanding of security and resilience requirements

04

A list of prioritized recommendations to improve your overall resilience

It is NOT:

- A compliance assessment
- A technology check or product assessment
- A penetration testing or infrastructure hardening exercise

It requires

- Collaboration
- Being open to discuss sensitive topics



Security & Resilience Assessment Workshop

Sample

The Security & Resilience Assessment covers ~100 controls within 6 categories (Identification / Protection & Prevention / Detection / Response & Recover / Backup & Restore / Learning & Evolving)

Security & Resilience Assessment

Identify

Category:
Risk Assessment

Objective:

- The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Risk Assessment Controls

ID.RA-1	Backups are stored on separate devices from production
ID.RA-2	Backup data and traffic are separated and use physically or logically isolated networks (e.g., VLAN)
ID.RA-3	Data to be backed up is assessed and determined, and periodically revalidated
ID.RA-4	Data from Cloud based applications (e.g. SaaS workloads) is being protected / backed up
ID.RA-5	Data Classification and identification is performed and managed by Security to identify sensitive data sets (PII, PHI, client data etc) and is communicated to the appropriate teams



Sample Recommendations

The Security & Resilience Assessment covers ~100 controls within 6 categories
(Identification / Protection & Prevention / Detection / Response & Recover / Backup & Restore / Learning & Evolving)

Governance	2	Conduct periodic management reviews to ensure that those given cybersecurity risk management responsibilities have the necessary authority
Identify	4	Quantify cost of system outage per system
	4	Quantify cost of application outage per application
Protect	2	Separate duties for management of data project mechanisms and policy management (separation of admins per data center)
	5	Consider implementing self-service policies (efficiency)
Detect	2	Leverage Anomaly / Data corruption detection for active threats on storage snapshots and or backups
Respond	3	Perform Analysis of Competing Hypothesis
	4	Perform Cones of Plausibility
Recover	2	Establish a periodic process to identify valid copies or for latent threat detection
	2	Set up an isolated recovery environment ("Clean Room") for data validation, workload recovery, or surgical repair
	3	Define and implement a process to identify and protect "Good copy" of backup images
	3	Define and implement a process to ensure recovery points are validated before recovery
	5	Determine, assess, and manage granularity of restore for surgical recovery, e.g. of MVC

IBM Security & Resilience Assessment



Which teams should participate in the workshop?

- Sponsor (e.g. CISO, CSO, CIO)
- Storage Administrator / Storage Team
- Security Administrator / Security Team
- Enterprise Business Continuity Management
- IT Disaster Recovery

Optional:

- IT Operations (Problem, Change, Configuration Management) / Technology/IT / Corporate Crisis Management / Corporate Communications / Procurement/Supply Chain / Business Partners focal