Ensuring Financial Resilience Dell POV to DORA

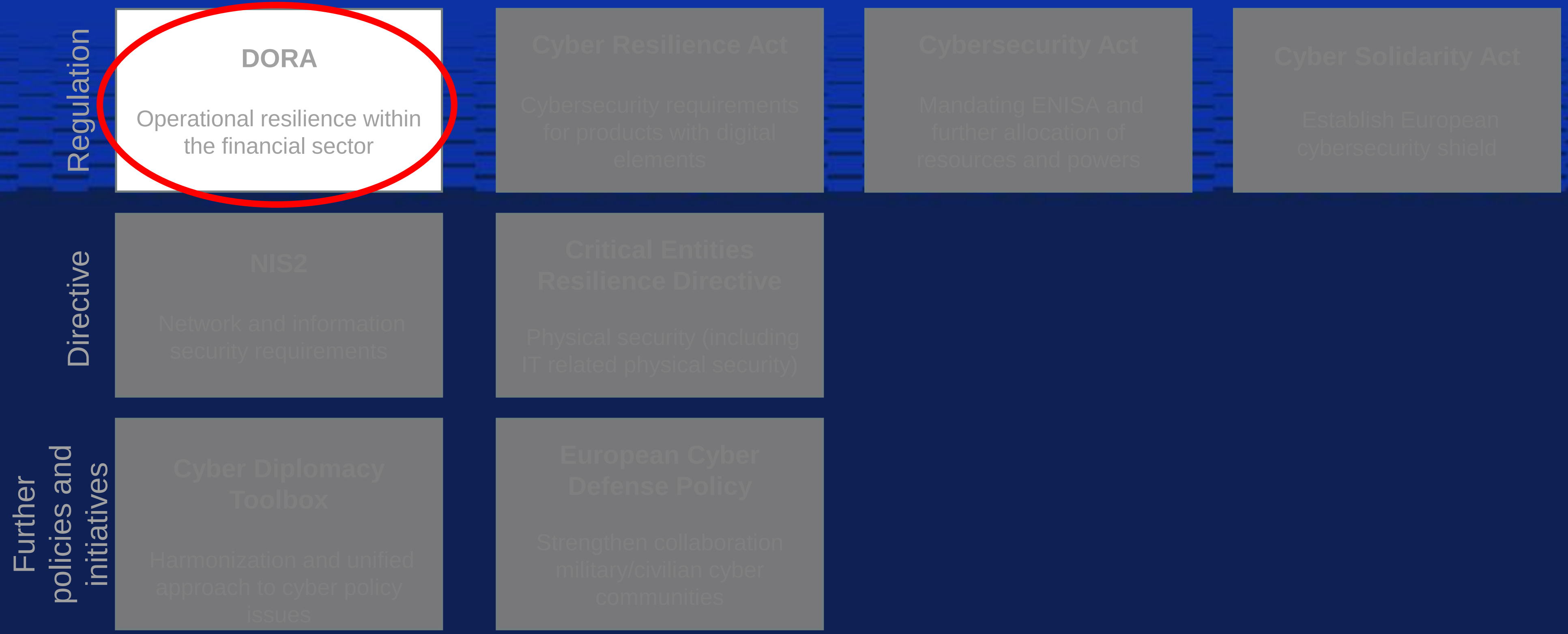
Itay Mesholam

Field CTO of EMEA Cybersecurity Services

The EU regulatory outlook

European cyber strategy

- Protecting Europe from cyber attacks
- Integrated approach with all stakeholders
- Creation of European cyber security center
- Stimulation of research and development
- International cooperation and common standards and guidelines
- Integration of cybersecurity into all aspects of business
- Enforcement of regulatory frameworks and laws.



Regulation

DORA

Operational resilience within the financial sector

Cyber Resilience Act

Cybersecurity requirements for products with digital elements

Cybersecurity Act

Mandating ENISA and further allocation of resources and powers

Cyber Solidarity Act

Establish European cybersecurity shield

Directive

NIS2

Network and information security requirements

Critical Entities Resilience Directive

Physical security (including IT related physical security)

Further policies and initiatives

Cyber Diplomacy Toolbox

Harmonization and unified approach to cyber policy issues

European Cyber Defense Policy

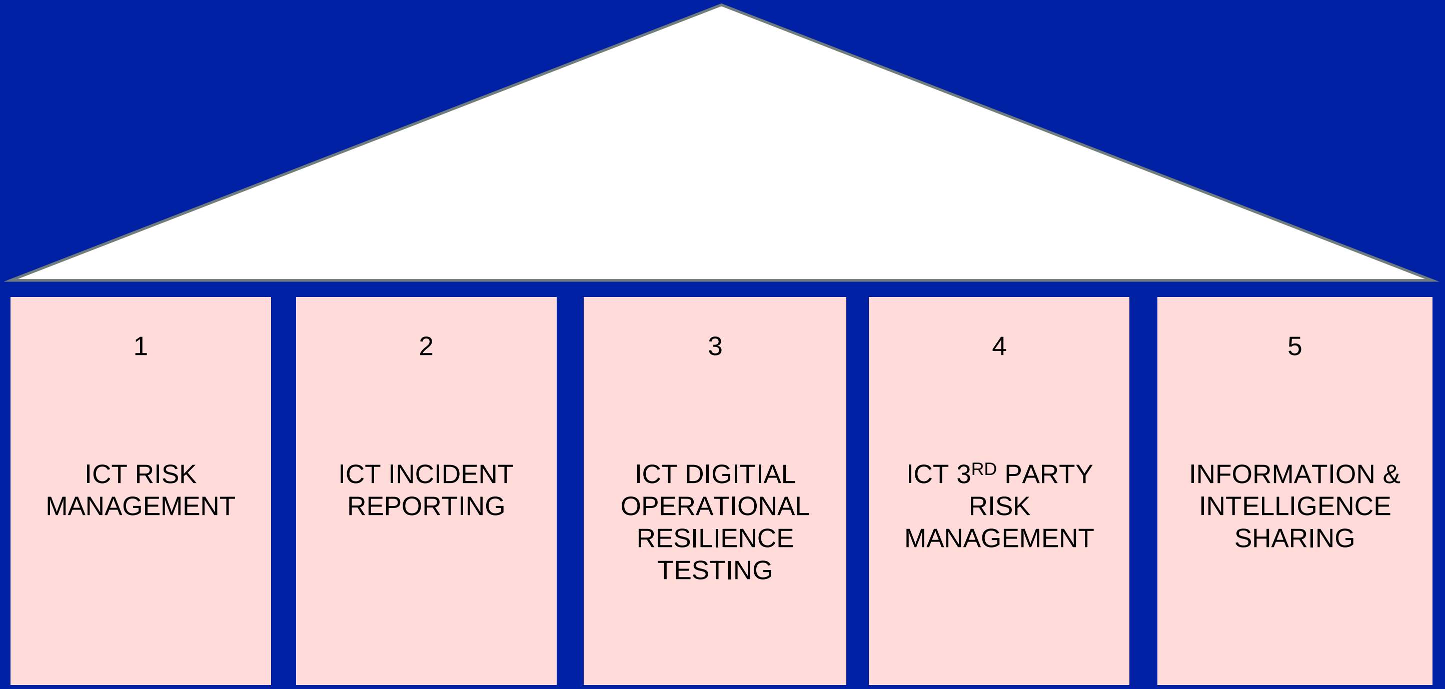
Strengthen collaboration military/civilian cyber communities

Digital Operational Resilience Act

On 17 January 2025, it comes into force

DORA

5 Pillars:



1

ICT RISK MANAGEMENT

2

ICT INCIDENT REPORTING

3

ICT DIGITIAL OPERATIONAL RESILIENCE TESTING

4

ICT 3RD PARTY RISK MANAGEMENT

5

INFORMATION & INTELLIGENCE SHARING

Procedures, processes, monitoring, reviewing & reporting

What is DORA?

What are the DORA pillars?

What's the schedule?

WHY?

The problem with modern cyberattacks and ransomware events is that all your previously held assumptions about your current environment and the challenges you will face as you restore or rebuild are probably **wrong**.

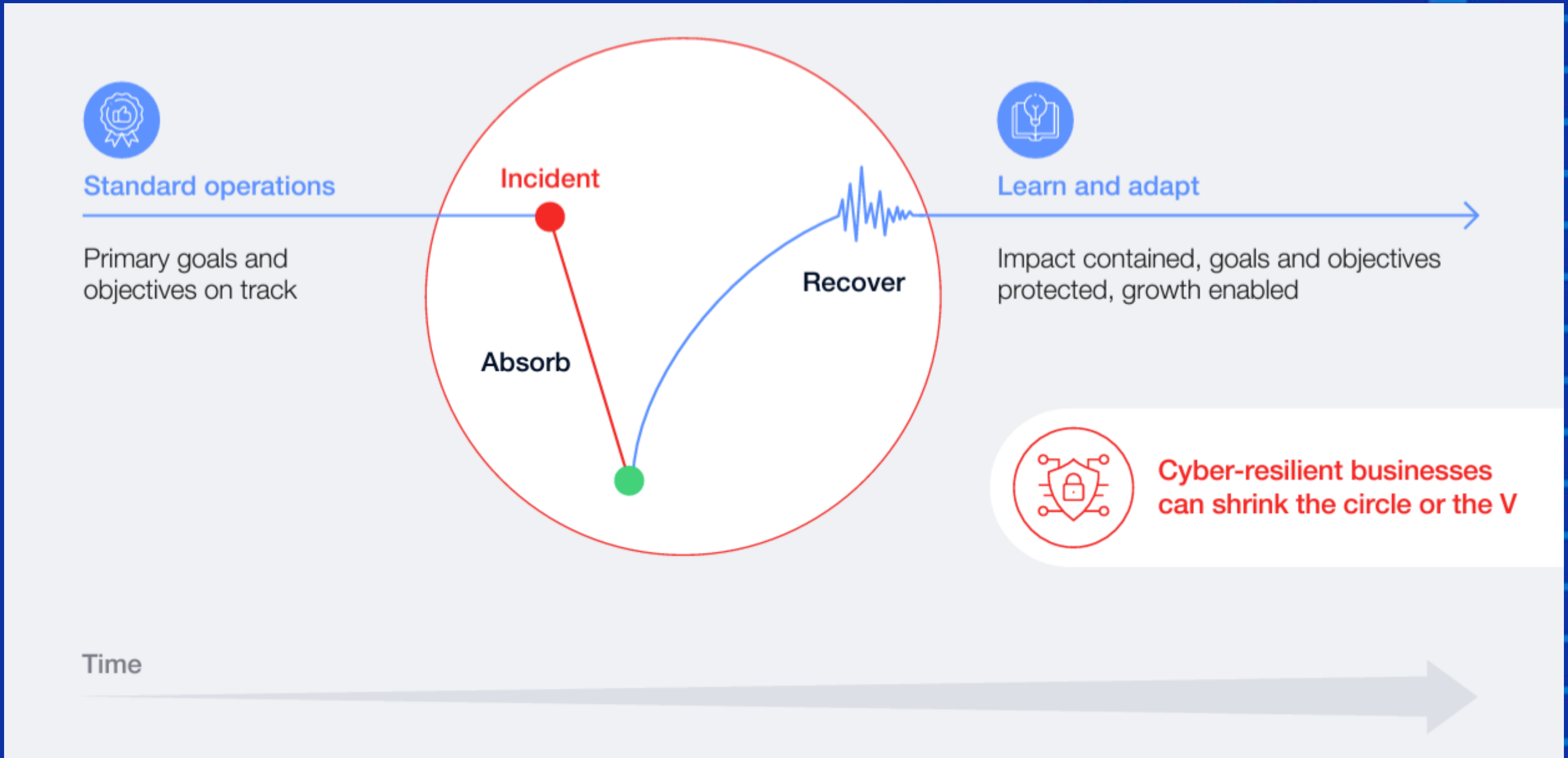
Everything will take longer. ***Everything*** that should be easy and straight forward will not be. All of your technical and architectural debt will likely come back to haunt you.

"Everybody has a plan until they get punched in the face.“

Mike Tyson

Dell Technologies

Resilience - Shrink the circle or the V



Standard operations

Primary goals and objectives on track

Incident

Absorb

Recover

Learn and adapt

Impact contained, goals and objectives protected, growth enabled

Cyber-resilient businesses can shrink the circle or the V

Time

Source: Adapted by the World Economic Forum and the University of Oxford from Linkov, I., & Trump, B.D. (2019). *The science and practice of resilience: Risk, systems and decisions*, Chapter 6. Springer. https://doi.org/10.1007/978-3-030-04565-4_6

Ransomware and the Impact to Business

BUSINESS DOWNTIME

24 days

Average downtime after a Ransomware attack[2]

NO MALWARE TO FIND

75%

Attacks that did not deploy malware - relying instead on identity, trust relationships and vulnerabilities[1]

BACKUPS UNDER ATTACK

94%

Ransomware attacks including attempts to compromise the backup (57% success rate)[3]

Recovery Objectives

Identify primary business services

Identify a viable recovery source

Identify a viable recovery target

Validate recovered items are free from compromise

Identify primary business services

Identify primary business services (aligned with article 11)

LLOYD'S

Business Recovery

Start by identifying business processes and relationships with applications and infrastructure

Business Mapping

Business Processes

Identify business processes critical to day-to-day operations

Map business activities and dependencies associated to those processes

Build a recovery strategy focused on recovering the most critical parts of the business first

IT Mapping

Applications and Infrastructure

Chart out applications and infrastructure related to identified business processes

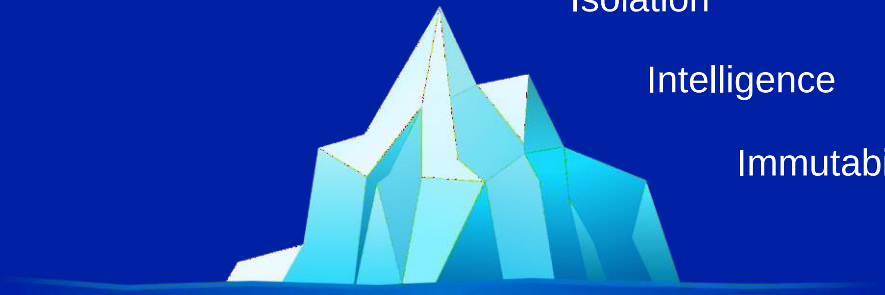
Document IT recovery needs to align with business needs

Focus efforts on applications and infrastructure restoration based on prioritization

Recovery Source

(aligned with article 11)

Defining Cyber Recovery with DORA



Isolation

Intelligence

Immutability

Multiple reports following real world events have indicated that *technology alone is simply not enough.*

Isolation

Intelligence

Immutability

End-to-end Services

Incident Response Plan

Secure Supply Chain

Recovery Focused

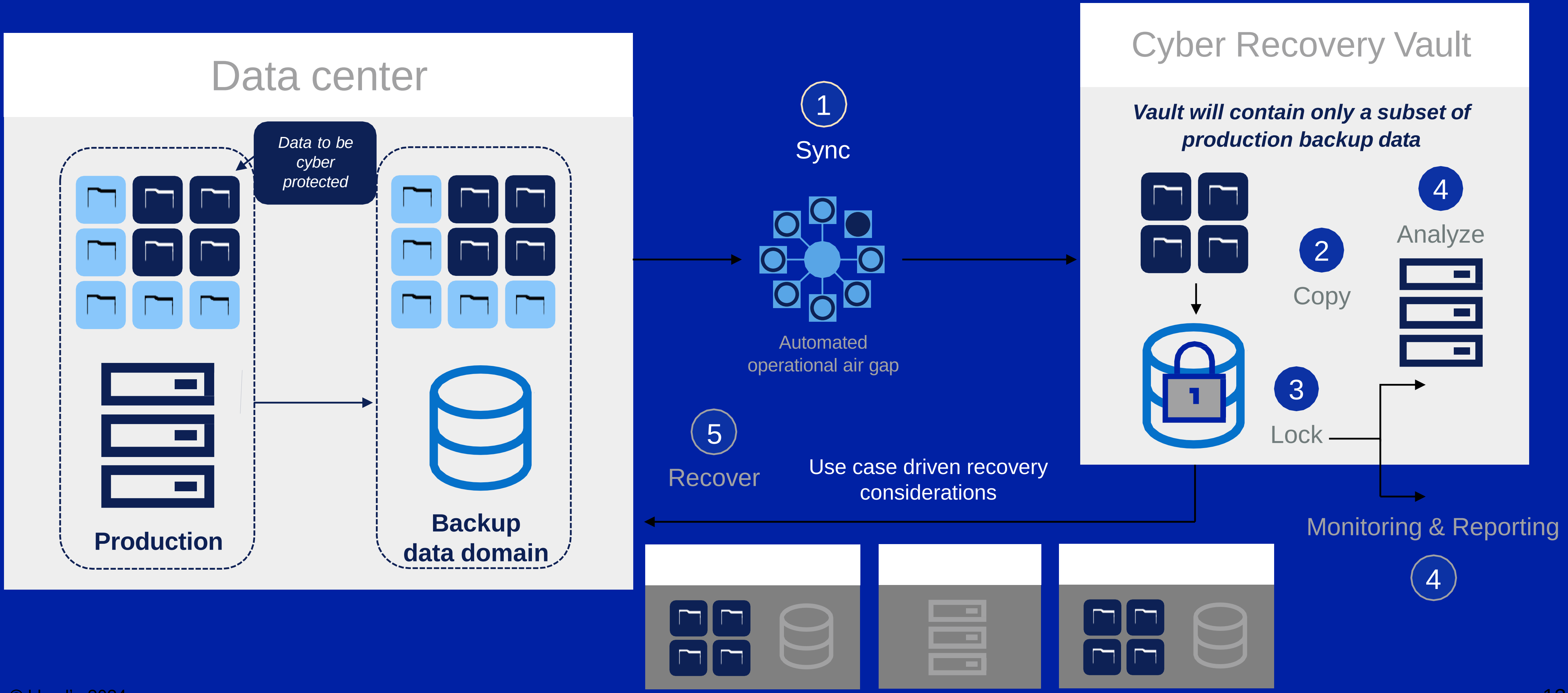
Cleanroom technology

No external access

LLOYD'S

PowerProtect Cyber Recovery

Automate data vaulting and recovery path


Data center
Data to be cyber protected
Production
Backup data domain
1
Sync
Automated operational air gap
Cyber Recovery Vault
Vault will contain only a subset of production backup data
4
Analyze
2
Copy
3
Lock
5
Recover
Use case driven recovery considerations
Monitoring & Reporting
4

© Lloyd's 2024

DELL Technologies

Classification: Confidential

Validate Recovery Source

(aligned with article 11-12)

Gather recovery requirements

What

Critical Rebuild Materials

Business Processes

OS Images

Applications

How

Restore

Restore data from known Point in Time

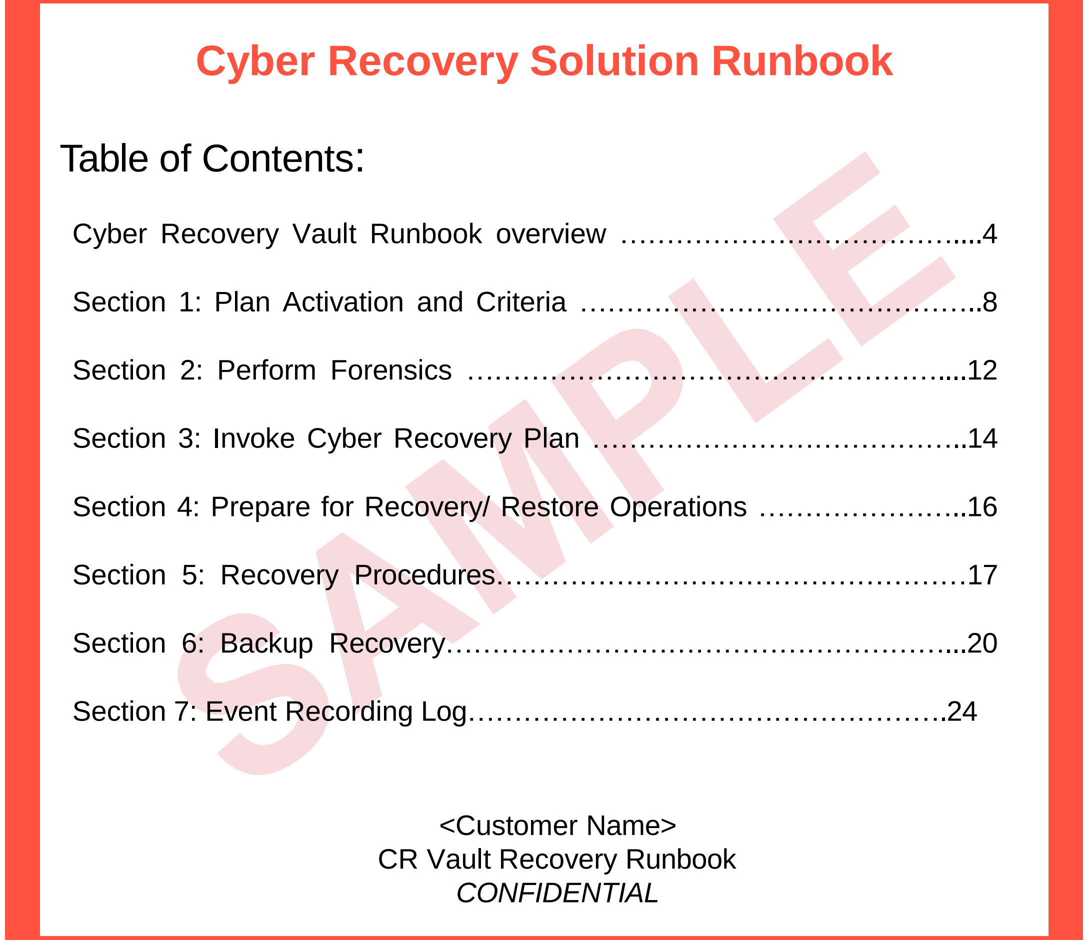
Repair

Restore data and apply known fixes

Rebuild

Assume nothing, rebuild new environment, restore transactional configs and data

Create tailored documentation



Cyber Recovery Solution Runbook

Table of Contents:

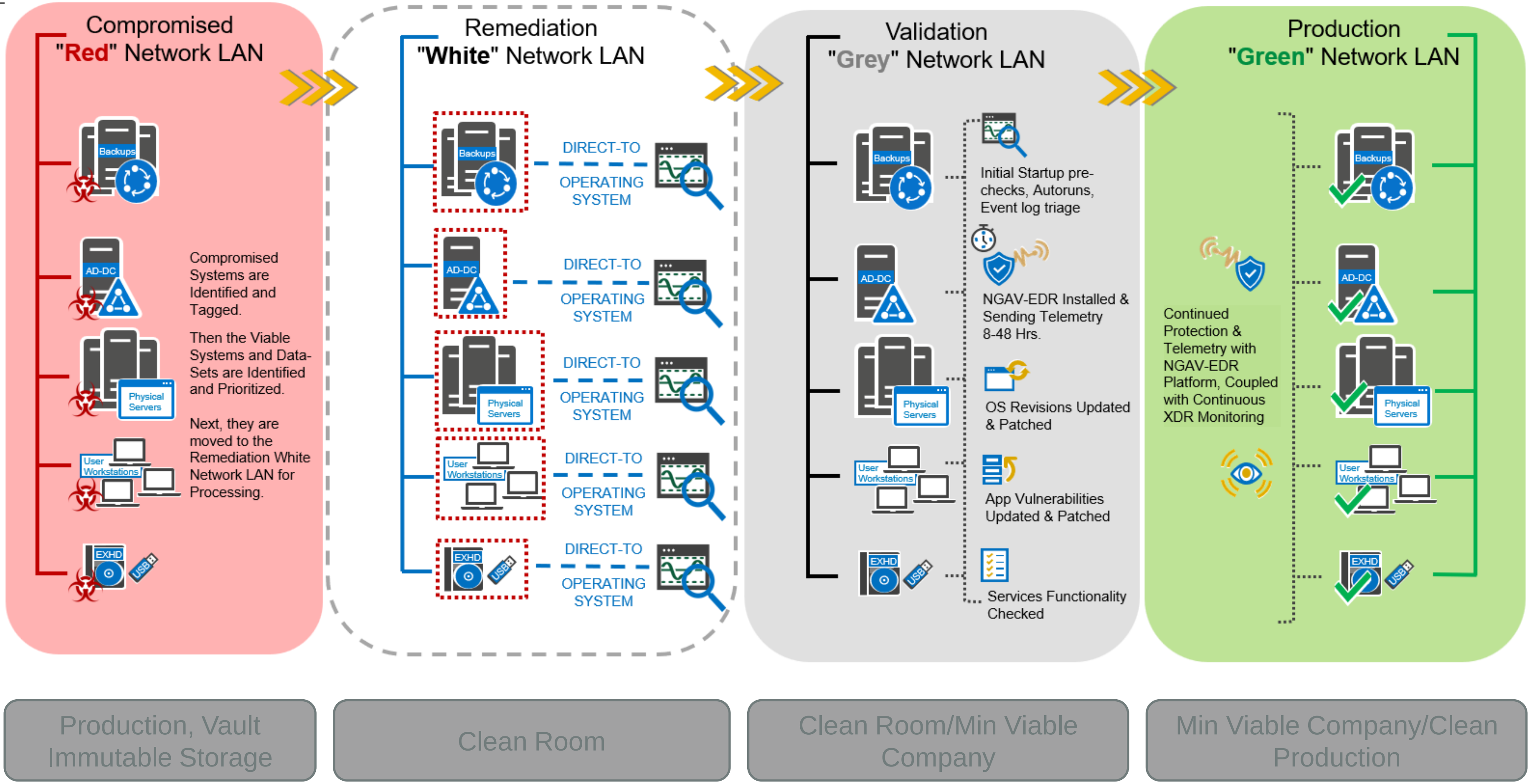
<Customer Name>
CR Vault Recovery Runbook
CONFIDENTIAL

LLOYD'S

Data Free from Compromise
(aligned with article 11-12)

DELL Technologies

Data Restoration and Recovery process used by IRR



Compromised Systems are Identified and Tagged.

Then the Viable Systems and Data-Sets are Identified and Prioritized.

Next, they are moved to the Remediation White Network LAN for Processing.

Initial Startup pre-checks, Autoruns, Event log triage

NGAV-EDR Installed & Sending Telemetry 8-48 Hrs.

OS Revisions Updated & Patched

App Vulnerabilities Updated & Patched

Services Functionality Checked

Continued Protection & Telemetry with NGAV-EDR Platform, Coupled with Continuous XDR Monitoring

LLOYD'S

Connected Partner Ecosystem

Easing security operations burdens…

DELL Technologies

Professional services

Managed services

Integration & implementation

by connecting organizations with…

industry leading technologies, reference architectures and tools…

VERSA NETWORKS

INDEX ENGINES Power Over Information

CROWDSTRIKE

MAINTEGRITY

Microsoft Security

NETSCOUT

Rocket software

superna

BEYONDEDGE

Cymulate

vmware by Broadcom

ABSOLUTE

Fast Lane

okta

tenable

Progress Flowmon

metalsoft

netskope

Secureworks

zscaler

through an automated, integrated and optimized customer experience.

Dell Security and Resiliency Services

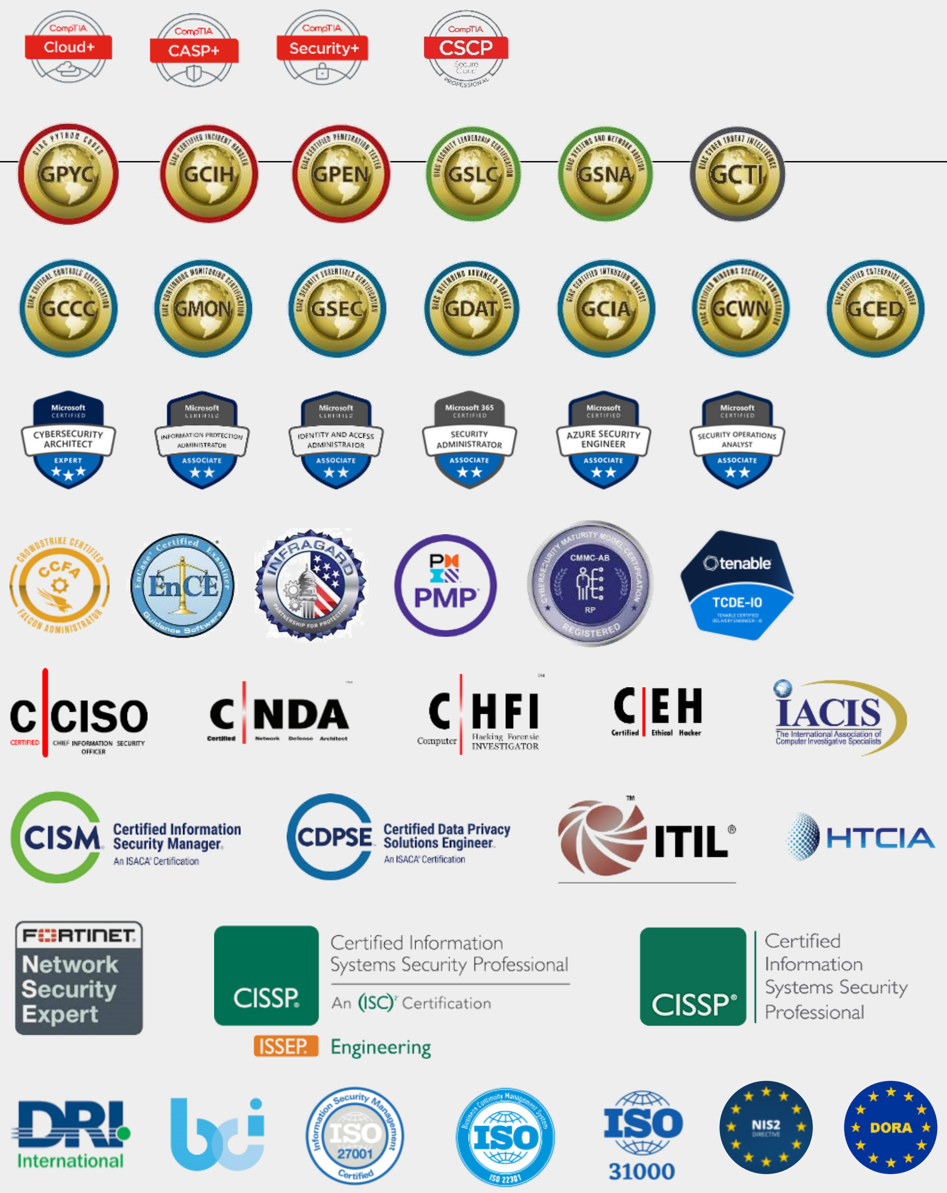
Certifications attained by team members

Where to begin …

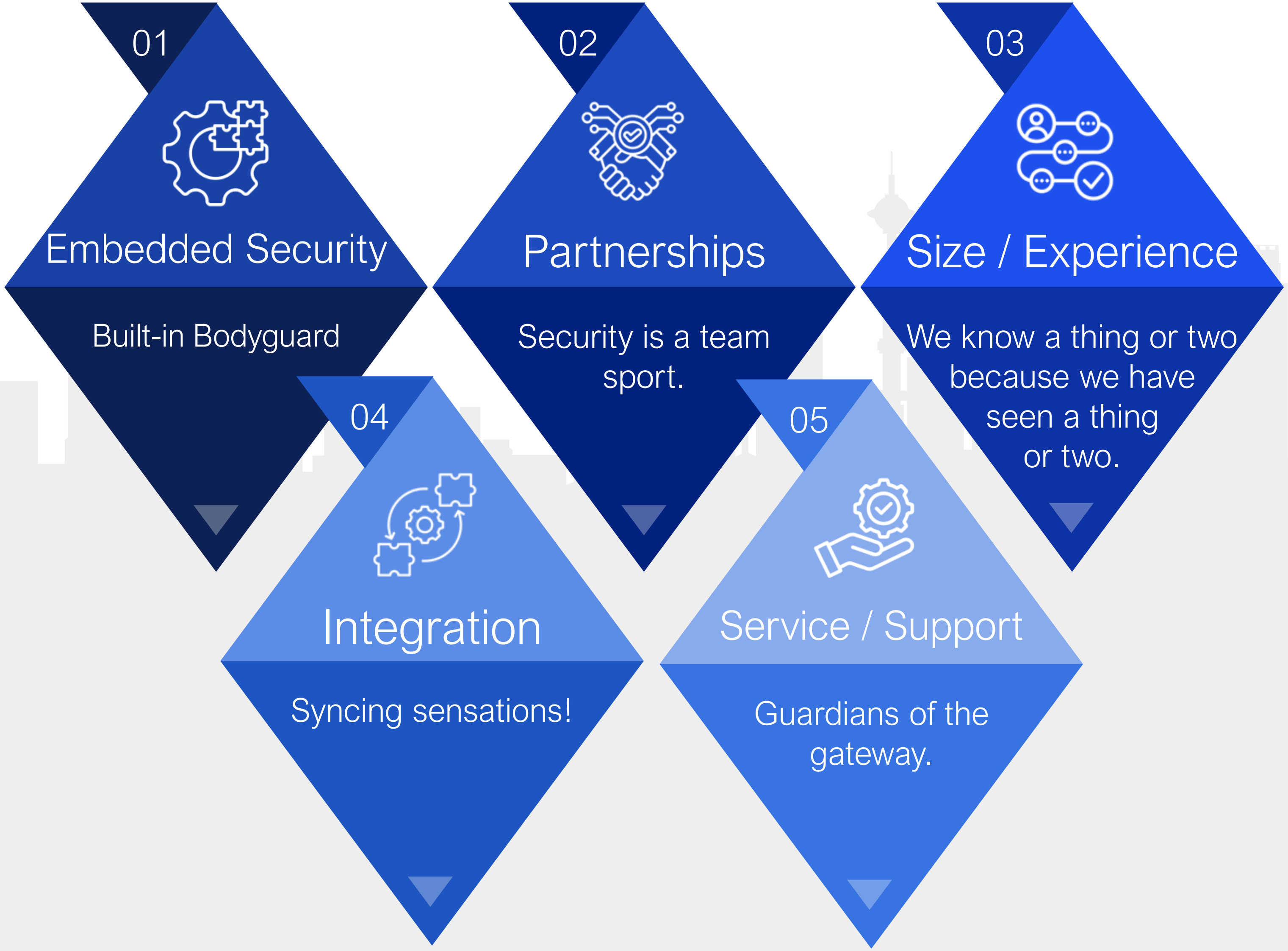
Focus on unifying key components and ensuring gaps are identified and filled continuously

- **Product Agnostic**
- **Framework-Driven Methodology**
- **Expertise of a collective**
- **Focus on security and resilience**

Security and Resilience Certifications


CompTIA Cloud+
CompTIA CASP+
CompTIA Security+
CompTIA CSCP
GPYC
GCIH
GPEN
GSLC
GSNA
GCTI
GCCC
GMON
GSEC
GDAT
GCIA
GCWN
GCED
Microsoft Certified Cybersecurity Architect Expert
Microsoft Certified Information Protection Administrator Associate
Microsoft Certified Identity and Access Administrator Associate
Microsoft 365 Certified Security Administrator Associate
Microsoft Certified Azure Security Engineer Associate
Microsoft Certified Security Operations Analyst Associate
CrowdStrike Certified CCFA Falcon Administrator
EnCE
InfraGard
PMP
CMMC-AB RP Registered
tenable TCDE-IO
C|CISO Certified Chief Information Security Officer
C|NDA Certified Network Defense Architect
C|HFI Computer Hacking Forensic Investigator
C|EH Certified Ethical Hacker
IACIS The International Association of Computer Investigative Specialists
CISM Certified Information Security Manager An ISACA Certification
CDPSE Certified Data Privacy Solutions Engineer An ISACA Certification
ITIL
HTCIA
FORTINET Network Security Expert
CISSP Certified Information Systems Security Professional An (ISC)² Certification
ISSEP Engineering
CISSP Certified Information Systems Security Professional
DRI International
bci
ISO 27001
ISO 22301
ISO 31000
NIS2
DORA

Why Dell for Cybersecurity?



01

Embedded Security

Built-in Bodyguard

02

Partnerships

Security is a team sport.

03

Size / Experience

We know a thing or two because we have seen a thing or two.

04

Integration

Syncing sensations!

05

Service / Support

Guardians of the gateway.

Thank you