

Hien

One of the
RSM team



Bringing you insights
to help you move forward
with confidence

At RSM, we help clients overcome new challenges,
embrace change and adapt to thrive.

By working together, creating deep insights,
combining world-class technology and real-world experience,
we deliver understanding that's unmatched, and confidence that builds.

For a changing world. For the future. For all.

With nearly 40 years of presence in Indonesia,
we have evolved into an integrated professional services firm,
assisting clients with assurance, tax, and consulting.

We are proud to be deemed as the #5 professional services firm in Indonesia.

RSM INDONESIA

40 YEARS OF
EXCELLENCE
& PARTNERSHIP
— 1985 – 2025 —

PROUD TO BE THE RIGHT PARTNER TO OUR STAKEHOLDERS.
THROUGH OUR ASSURANCE, TAX, AND CONSULTING SERVICES,
WE SUPPORT OUR CLIENTS' SUCCESS
WHILE FOSTERING A REWARDING AND ENJOYABLE
PROFESSIONAL CULTURE.

900+ Staff
40+ Partners
2 Offices

RSM

RSM

In support of:

**WOMEN'S
EMPOWERMENT
PRINCIPLES**

Established by UN Women and the
UN Global Compact Office



**Great
Place
To
Work®**

Certified
SEP 2024–SEP 2025
ID

Our Services in Indonesia

ACCOUNTING & REPORTING ADVISORY

Complex Accounting & Reporting | Cost & Management Accounting |
New Accounting Standards & Implementation |

AUDIT

Agreed Upon Procedures | Financial Information Review | General Audit |

BUSINESS & CORPORATE SERVICES

Accounting Services | Business Establishment & Licensing |
Corporate Secretarial | Financial Outsourcing Services | Liquidations | Payroll |

CORPORATE FINANCE & TRANSACTION ADVISORY

Corporate Finance | Corporate Recovery & Insolvency | Restructuring |
Valuation |

GOVERNANCE RISK CONTROL CONSULTING

ESG & Sustainability | Fraud Prevention | Governance | Internal Audit |
Risk Management | Security & Privacy Risk | Technology Risk |

MANAGEMENT CONSULTING

Finance & Performance | Transformation |

TAX

Business Tax | International Tax | Merger & Acquisition | Tax Compliances |
Tax Dispute Resolution | Transfer Pricing |

TECHNOLOGY CONSULTING

Artificial Intelligence & Data Analytics | Digital & Technology Integration |
Enterprise Technology | Technology Infrastructure |

RSM Indonesia Webinar | 11 June 2025

ENHANCING CYBER RESILIENCE WITH NIST CYBER SECURITY FRAMEWORK (CSF) 2.0

Erikman D Pardamean & Dena Sucianandika – Technology Risk Consulting Practice




M&S Reportedly Hacked Using Third-Party Credentials

In April 2025, Marks & Spencer (M&S) experienced a significant cyberattack that disrupted its operations and compromised customer data. The cyberattack was facilitated through compromised credentials from a third-party vendor, Tata Consultancy Services (TCS), which manages M&S's IT helpdesk.



Nature of the Attack

- **Method of Breach:** The attackers employed sophisticated social engineering techniques, notably "vishing" (voice phishing), to deceive IT helpdesk personnel into resetting internal account passwords. This allowed unauthorized access to M&S's systems.
- **Ransomware Deployment:** Once inside, the cybercriminals deployed ransomware, believed to be associated with the "DragonForce" group, encrypting critical systems and disrupting operations across M&S's network. 

Impact on Operations and Finances

- **Operational Disruption:** The attack forced M&S to suspend online orders from April 25, 2025, with disruptions expected to continue into July. This suspension affected the company's ability to process online clothing and homeware sales, leading to significant revenue losses.
- **Financial Losses:** M&S estimated the cyberattack would result in a £300 million (\$400 million) hit to its operating profit for the fiscal year. The company's market value also declined by over £1 billion following the incident.

Data Compromise

- **Customer Data Breach:** The attackers accessed personal customer information, including names, email addresses, home addresses, phone numbers, dates of birth, and online order histories. However, M&S stated that no usable payment card details or account passwords were compromised.

TABLE OF CONTENTS

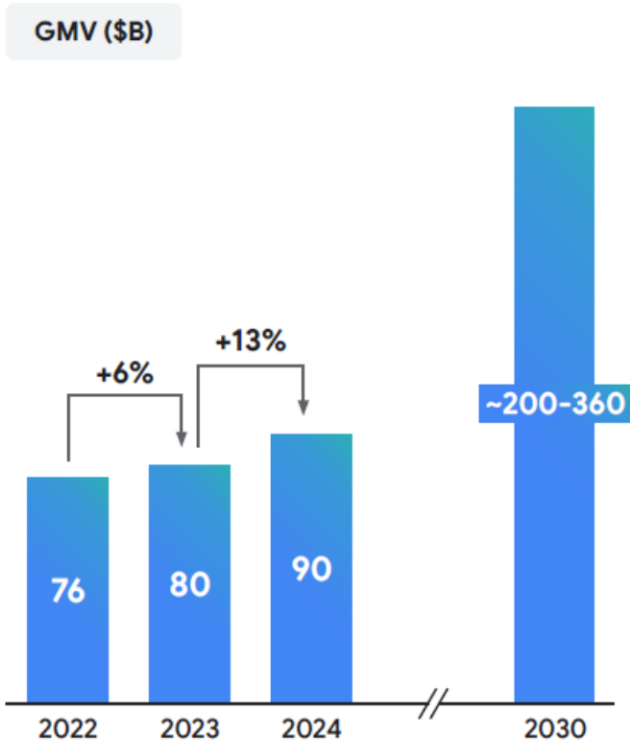
1.	Why It Matters and The Cost of Inaction
2.	Exploring Cybersecurity Standards, Frameworks and Regulations Landscape in Indonesia
3.	How NIST CSF 2.0 Can Helps
4.	Implementing NIST CSF 2.0

WHY IT MATTERS

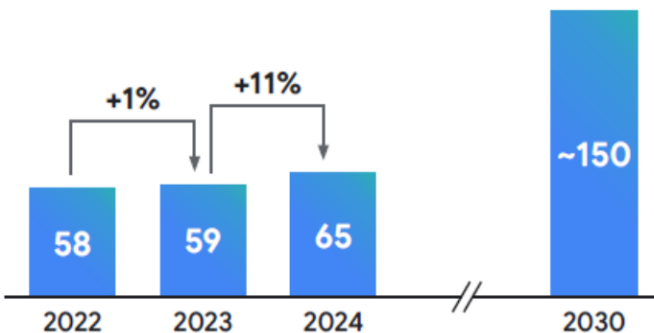
Development of Indonesia's Digital Economy

Growth doubles, bringing GMV to \$90B in 2024

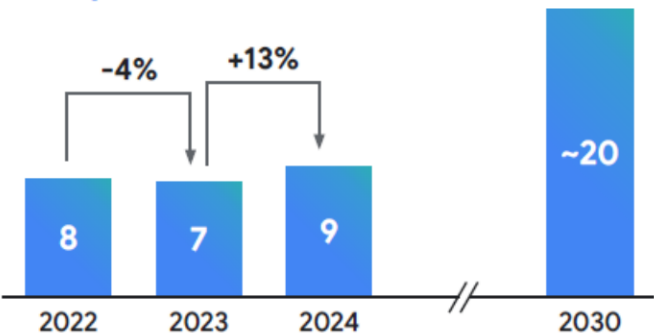
Overall digital economy



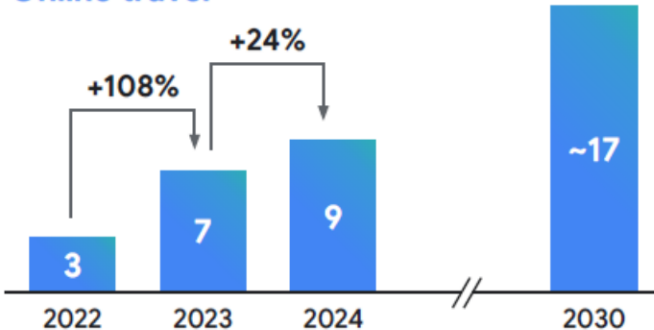
E-commerce



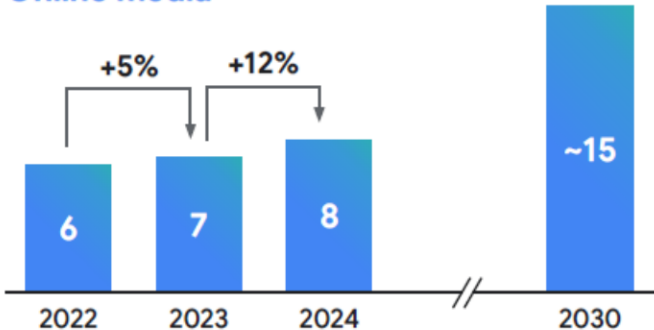
Transport and food



Online travel



Online media



Source: BAIN analysis, e-Conomy SEA 2024



Global Risk Trends

What are the top 5 risks your organization faces?

Last Year's Risk			Current Year's Risk			Risk Expectations in 3 Years		
1.	Cybersecurity	73%	1.	Cybersecurity	73%	1.	Cybersecurity	69%
2.	Human capital	51%	2.	Business continuity	51%	2.	Digital disruption (including AI)	59%
3.	Business continuity	47%	3.	Human capital	49%	3.	Business continuity	47%
4.	Regulatory change	39%	4.	Digital disruption (including AI)	39%	4.	Human capital	42%
5.	Digital disruption (including AI)	34%	5.	Regulatory change	38%	5.	Climate change/environment	39%
6.	Financial liquidity	32%	6.	Market changes/competition	32%	6.	Regulatory change	37%
7.	Market changes/competition	32%	7.	Financial liquidity	31%	7.	Geopolitical uncertainty	31%
8.	Geopolitical uncertainty	30%	8.	Geopolitical uncertainty	30%	8.	Market changes/competition	30%
9.	Governance/corporate reporting	27%	9.	Governance/corporate reporting	25%	9.	Financial liquidity	25%
10.	Supply chain (including third parties)	26%	10.	Organizational culture	24%	10.	Supply chain (including third parties)	24%
11.	Organizational culture	26%	11.	Fraud	24%	11.	Governance/corporate reporting	22%
12.	Fraud	24%	12.	Supply chain (including third parties)	23%	12.	Fraud	21%
13.	Communications/reputation	21%	13.	Climate change/environment	23%	13.	Organizational culture	20%
14.	Climate change/environment	19%	14.	Communications/reputation	20%	14.	Communications/reputation	15%
15.	Health/safety	11%	15.	Health/safety	11%	15.	Health/safety	10%
16.	Mergers/acquisitions	6%	16.	Mergers/acquisitions	6%	16.	Mergers/acquisitions	9%

Source: 2025, Risk in Focus, The IIA

Pengembangan Ekonomi Digital Indonesia 2030

Arah Strategis Pengembangan Ekonomi Digital



Prinsip Utama Pengembangan Ekonomi Digital



Visi

Kejelasan dan keterpaduan visi nasional yang menyeluruh untuk mendukung pengembangan ekonomi digital

Infrastruktur

Kejelasan dan keterpaduan visi nasional yang menyeluruh untuk mendukung pengembangan ekonomi digital

Sumber Daya Manusia

Ketersediaan dan talenta professional tingkat lanjut dengan keterampilan yang dibutuhkan untuk mengakomodasi perkembangan ekonomi digital

Iklim Bisnis dan Keamanan Siber

Keseluruhan penerapan digital lanskap bisnis dan tingkat keamanan siber

Riset Inovasi Pengembangan Bisnis

Akuisisi, pengembangan, dan pemanfaatan keterampilan serta teknologi untuk berinovasi di dalam dan di luar TIK

Pendanaan & Investasi

Kejelasan dan keterpaduan visi nasional yang menyeluruh untuk mendukung pengembangan ekonomi digital

Kebijakan / Regulasi

Kejelasan dan keterpaduan visi nasional yang menyeluruh untuk mendukung pengembangan ekonomi digital

01 Kesetaraan Digital

02 Level Playing Field

03 Winning Edge
(Keunggulan bersaing)

04 Keyakinan dan Kepercayaan Daring

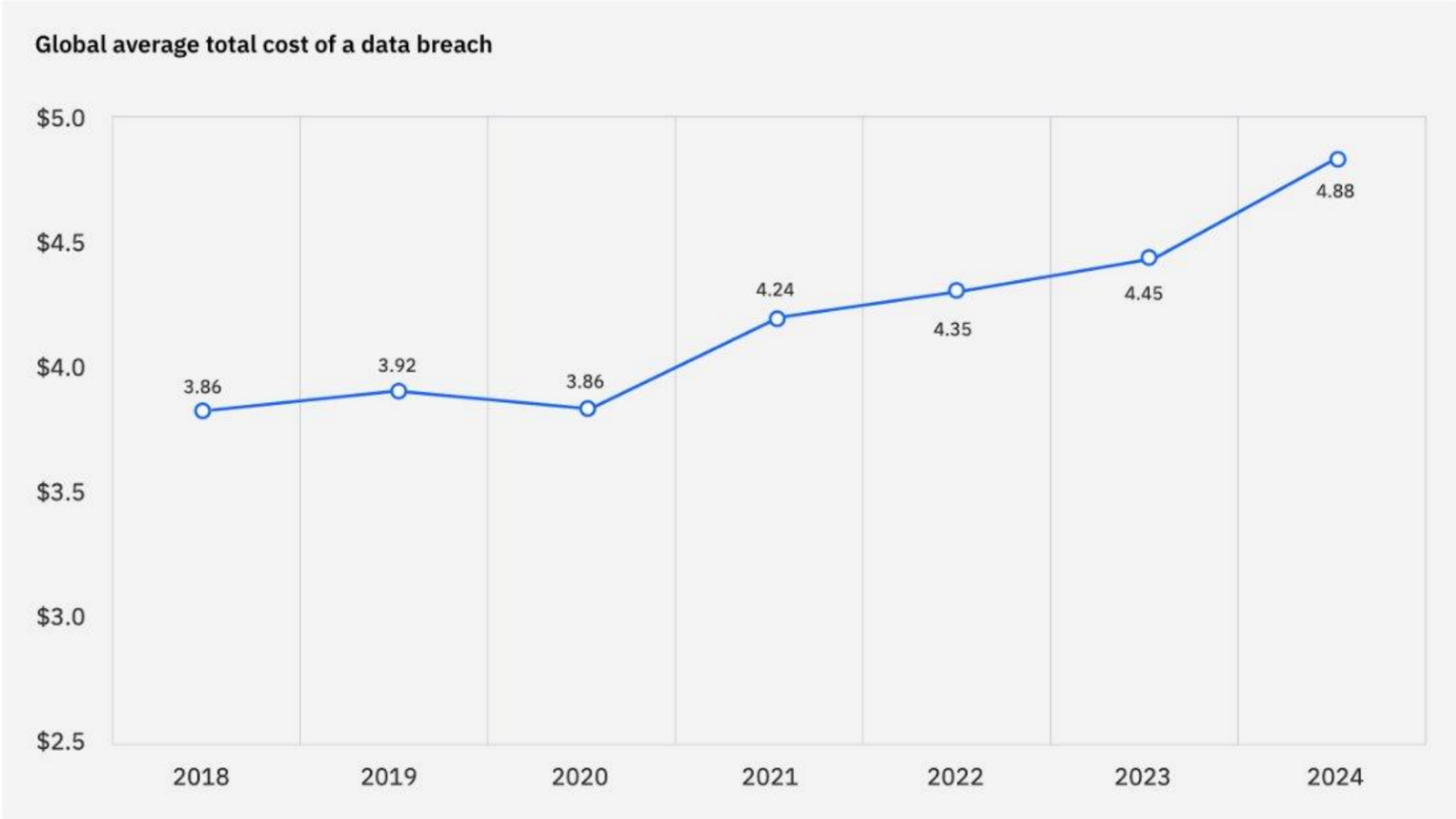
“Aspek pengelolaan data yang transparan, keamanan siber yang kuat, tanggung jawab, dan kepatuhan..”

05 Kolaborasi dan Dampak Kolektif

Pilar	Status Quo Indonesia	Intervensi Utama
Infrastruktur	1 dari 6 Intervensi Kunci	<ol style="list-style-type: none"> Regulasi Infrastructure Sharing Regulasi Right of Way Regulasi Zona Pusat Data Pusat Data / Standar Keamanan Cloud Regulasi Harga Regulasi Kualitas Layanan
Sumber Daya Manusia	0 dari 4 Intervensi Kunci	<ol style="list-style-type: none"> Kurikulum Digital Edukasi Regulasi Teknologi Visa Rencana Aksi Pendidikan Digital Kerangka Keterampilan Digital
Iklim Bisnis dan Keamanan Siber	5 dari 14 Intervensi Kunci	<ol style="list-style-type: none"> Manufaktur: Transfer Teknologi UU Keamanan Siber Agrikultur: Regulasi Taman Teknologi Agrikultur; Regulasi Pertanian Hi-Tech Agrikultur: Regulasi Pelacakan Ternak Data: UU Identitas Digital Tunggal Perdagangan: UU Pasar Digital UU Pelindungan Data Pribadi Keamanan Siber: Pelaporan Insiden Regulasi Startup Listing Perdagangan: Pembayaran Digital Manufaktur: Super Tax Deduction Kerangka Tata Kelola Data Polis Tanda Tangan Digital
Penelitian, Inovasi, dan Pengembangan Bisnis	1 dari 4 Intervensi Kunci	<ol style="list-style-type: none"> Regulasi Teknologi Sandbox Regulasi Kluster Teknologi UU Promosi Industri Software UU Desain Industri
Pendanaan dan Investasi Status Intervensi Keseluruhan	0 dari 4 Intervensi Kunci	<ol style="list-style-type: none"> Berbagai Kredit Pajak Staartup Insentif Pajak untuk R7D Manufaktur Insentif Digitalisasi UMKM Insentif Adopsi Smart Farming

THE COST OF INACTION

The Cost of Data Breach

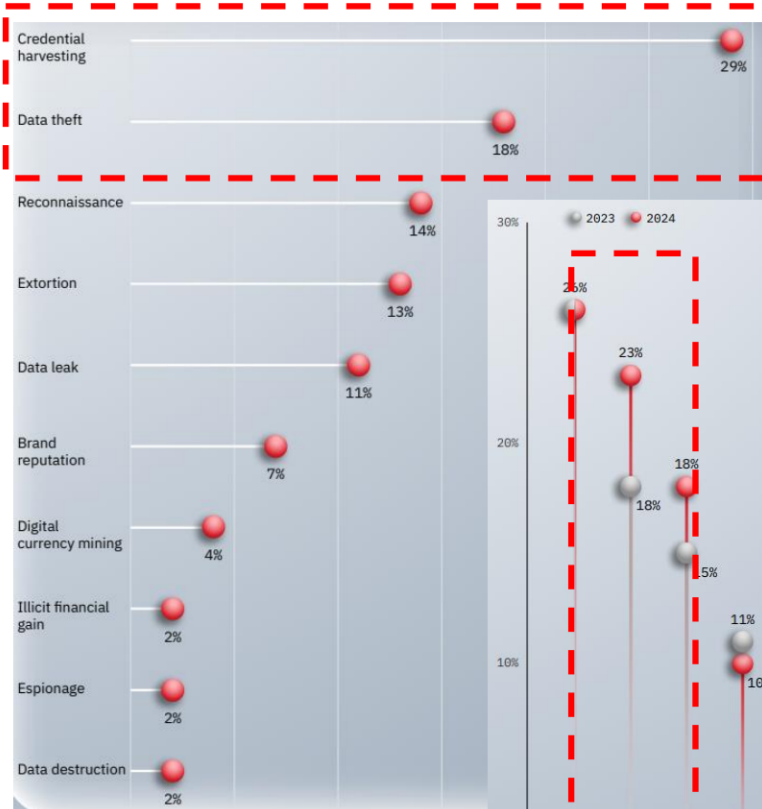


The average cost of a data breach jumped to USD 4.88 million from USD 4.45 million in 2023, a 10% spike and the highest increase since the pandemic.

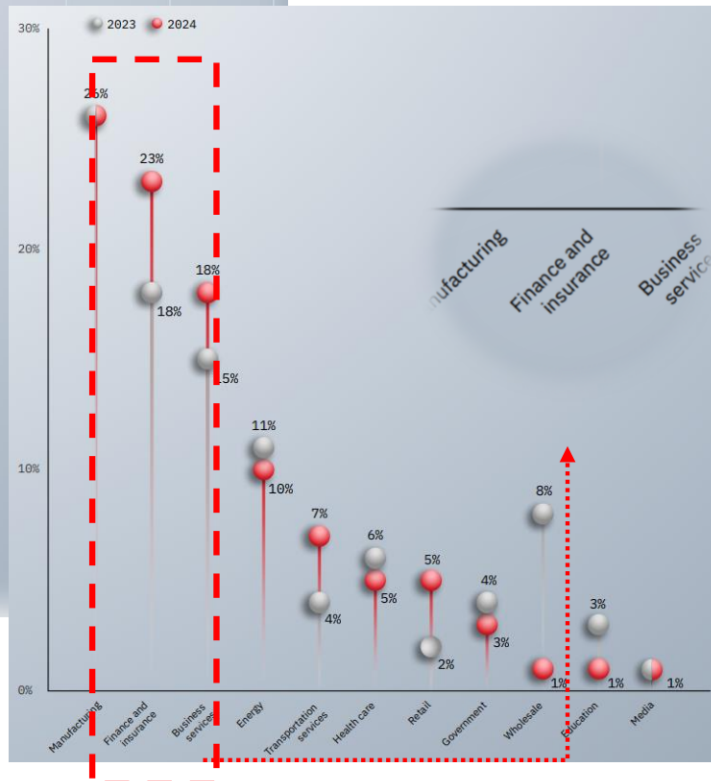
Source: IBM-Cost of a Data Breach Report 2024

The Prime Target of Threat Actors – What We Should Be Concerned

Top impacts observed in incident response engagements (2024)



Share of attacks by industry (2023-2024)



Key Notes

- In 2024, the **top impact experienced** by victim organizations was **credential harvesting**, occurring in 29% of incidents.
- Financial Sector is remain as prime target due to the **high value of financial data and assets**. Attackers primarily breached finance and insurance systems **through phishing / spearfishing attachments (30%)**.
- Espionage, **credential harvesting and data theft (20%)** were equally common, with attackers focusing on **stealing sensitive information** and **compromising account credentials**.

Source: IBM X-Force 2025 Threat Intelligence Index

How Do I Know You Are Not a Deep Fake?

TECH · DEEPFAKES

A deepfake 'CFO' tricked the British design firm behind the Sydney Opera House in \$25 million scam

BY PRARTHANA PRAKASH
May 17, 2024 at 7:32 AM EDT



Arup was attacked by deepfake fraudsters earlier this year.
TERO VESALAINEN—GETTY IMAGES

How AI is threatening elections...



Source: <https://fortune.com/europe/2024/05/17/arup-deepfake-fraud-scam-victim-hong-kong-25-million-cfo/>


DON'T WAIT TO BE ATTACKED
PREVENTION STARTS **NOW >**


TOP TARGETED COUNTRIES

Highest rate of attacks per organization
in the last day.

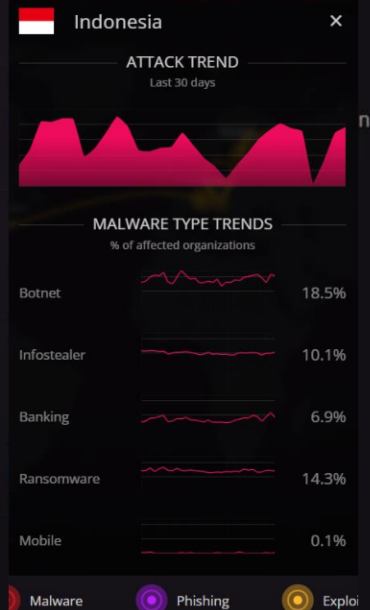
 Ethiopia

 Nepal

 Indonesia

 Mongolia

 Vietnam



LIVE CYBER THREAT MAP

2,488,049 ATTACKS ON THIS DAY

<https://threatmap.checkpoint.com/>







 Malware  Phishing  Exploit



RECENT DAILY ATTACKS



ATTACKS Current rate - 4 +

-  Parsing Error - Cannot Recognize My...
10:58:20 Netherlands → Netherlands
-  Parsing Error - Cannot Recognize My...
10:58:20 Netherlands → Netherlands
-  Mozilla multiple products multiple lo...
10:58:20 NJ, United States → KY, United St...
-  Mozilla multiple products multiple lo...
10:58:20 NJ, United States → KY, United St...
-  Mozilla multiple products multiple lo...
10:58:19 NJ, United States → KY, United St...
-  Parsing Error - Cannot Recognize My...
10:58:19 Netherlands → Netherlands



EXPLORING CYBERSECURITY STANDARDS, FRAMEWORKS AND REGULATIONS IN INDONESIA

Relevant Regulatory for Cybersecurity and Privacy

1

National Cyber and
Crypto Agency



2

Ministry of
Communication
and Information



3

Central Bank
of Indonesia



4

Financial Service
Authority



Relevant Regulatory for Cybersecurity and Privacy

Regulations:

- Peraturan Presiden Republik Indonesia Nomor 47 Tahun 2023 Tentang Strategi Keamanan Siber Nasional Dan Manajemen Krisis Siber
- SE OJK No. 29/SEOJK.03/2022 Tentang Ketahanan Dan Keamanan Siber Bagi Bank Umum
- POJK Republik Indonesia Nomor 11/POJK.03/2022 Tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum
- Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 Tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik.
- Peraturan Bank Indonesia Nomor 2 Tahun 2024 Tentang Keamanan Sistem Informasi Dan Ketahanan Siber Bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang Dan Pasar Valuta Asing, Seperti Pihak Lain Yang Diatur Dan Diawasi Bank Indonesia



Regulations Related to Handling Cyber Incidents



Peraturan BSSN No.10/2020: Tim Tanggap Insiden Siber harus melaporkan penanganan Insiden Siber kepada Tim Tanggap Insiden Siber Nasional.

Perpres 82/2022: mengamanatkan bahwa organisasi yang dikategorikan sebagai Infrastruktur Vital harus:

- membentuk Tim Tanggap Insiden Siber CSIRT.
- melaksanakan kesiapsiagaan terhadap Insiden Siber.
- CSIRT harus melaporkan insiden siber kepada CSIRT sektoral/BSSN paling lambat 1x 24 jam setelah insiden terkonfirmasi.



OJK PTI: Perusahaan wajib memberitahukan kepada subjek data paling lambat 1x24 jam, dan melaporkan kejadian tersebut kepada OJK paling lambat 5 hari kerja sejak dinyatakan sebagai kejadian.

PBI 23/6/PBI/2021: Laporan gangguan dalam pemrosesan transaksi pembayaran wajib disampaikan kepada Bank Indonesia paling lambat 1 (satu) jam setelah kejadian.

PBI No. 2/2024: Penyelenggara mewajibkan IRP & tim CSIRT teruji, membatasi dampak, melakukan forensik, mengirim notifikasi awal ≤ 1 jam dan laporan lengkap ≤ 3 hari kalender ke Bank Indonesia.



UU PDP 27/ 2022:

- Jika terjadi kebocoran data, pemberitahuan kepada subjek data minimal 3x24 jam.
- Perusahaan harus memiliki saluran yang dapat dihubungi oleh subjek data.
- Perusahaan harus memiliki rencana keberlangsungan bisnis, rencana pemulihan bencana, dan/atau kebijakan terkait lainnya.

Perpres 20/2016: Perusahaan wajib melaporkan ke Kemkominfo setelah kejadian dinyatakan sebagai insiden.

Transformation Succeeds Only When Security is Baked Into Every Layer

Transformation succeeds only when culture aligns with innovation and security

NIST



Security architecture consists of **5 domains** with **33 security capabilities**



People

Deploying the right skills to the security team with clear roles & responsibilities



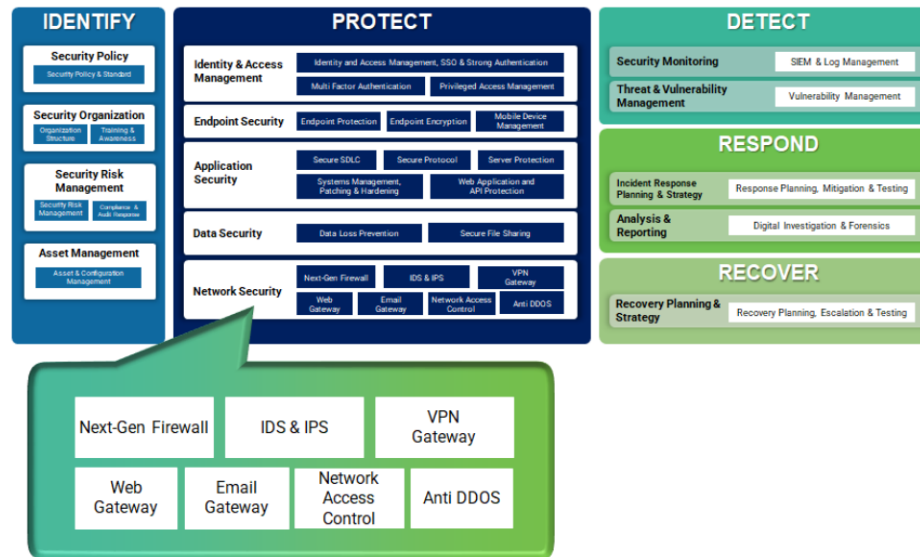
Process

Enforcing the policies & processes to ensure security of information assets

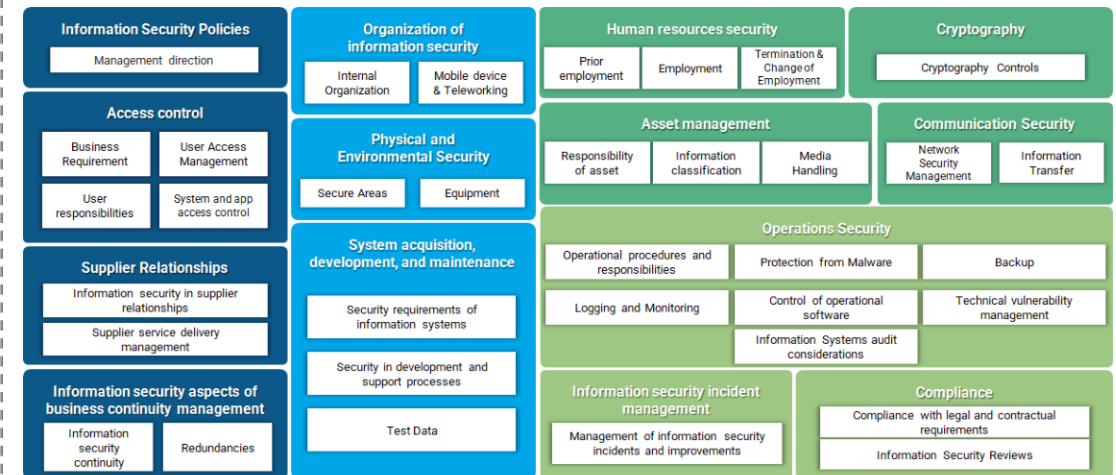


Technology

Developing required security technology to enhance cybersecurity capabilities



ISO 27001:2022



* Companies that already have **ISO 27001:2013 certification** are required to **upgrade their certification to ISO 27001:2022 by October 2025 at the latest.**

Risk Based Approach for Cybersecurity



Risk Identification



Risk Response



Risk Governance & Management



Risk Assessment & Analysis



Risk Monitoring, Reporting and Communication



Objective

Risk

Control

Assurance

“ implementing a structured approach to identifying, assessing, mitigating, and monitoring risks. These objectives aim to protect an organization, individual, or system from potential harm while enabling growth and opportunity. ”

Cyber Security

Data Protection

Maturity Level

Risk Management

Security Operation

Incident Response

Digital Transformation Without Security Is a Risk

Digital transformation without culture is a failure



How



Three line of defense: government, industry, international (cross border)



CIAAN principles: Confidentiality (least privilege), Integrity (password, signature), Availability (authorized), Authenticity (trusted), Non-Repudiation (non denial)



Single point of failure. Understanding umbrella concept: crime, fraud, security. Risk based approach to systems security



What Next



AI Ops for end to end: prevention, detection, investigation, monitoring



AI for fraud detection (continuous monitoring, faster response)



AI for predictive analysis

HOW NIST CSF v2.0 CAN HELP

Quick Overview of NIST Cybersecurity Framework



NIST CSF 2.0 offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts.

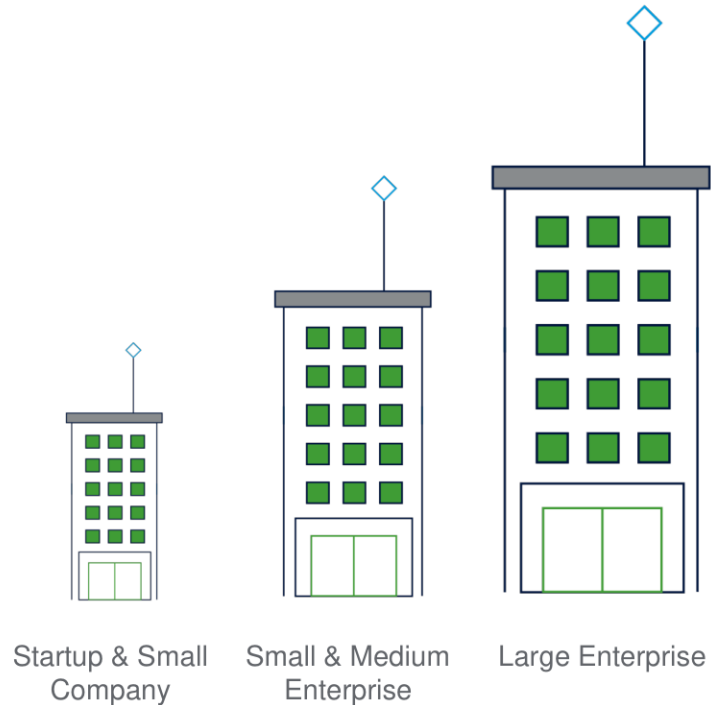
It links to online resources that provide additional guidance on practices and controls that could be used to achieve those outcomes.

NIST CSF 2.0 can help organizations manage and reduce their cybersecurity risks as they start or improve their cybersecurity program

Applicable from all the size of company from all sectors and can speaking for all level in organizations and integrating with broader risk management strategies.

NIST Cybersecurity Framework Can Be Used By Organizations of All Sizes and Sectors

Implementation of **ALL SIZE ORGANIZATION**



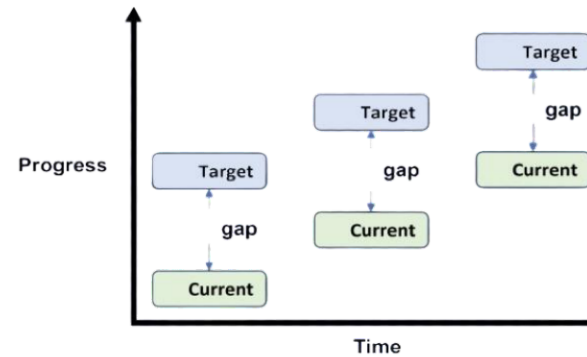
Implementation of **ALL SECTORS**



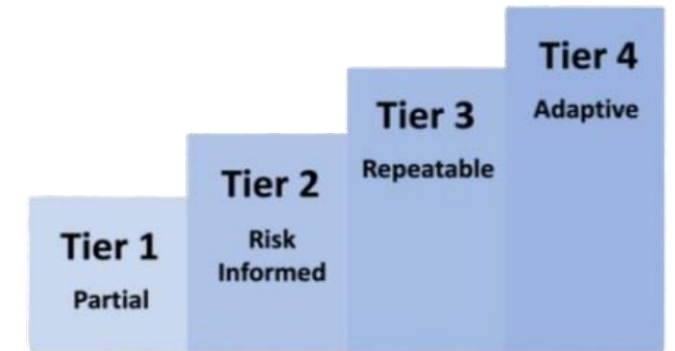
NIST CSF 2.0 Component



CSF Core



CSF Organizational profile



CSF Tiers

Key Highlight Points

- The CSF Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome
- These outcomes can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise
- a mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes
- This can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices. Tiers can also provide context for how an organization views cybersecurity risks and the processes in place to manage those risks.

Benefit of Implementing NIST CSF 2.0



1. Strengthened Cybersecurity Posture and Enhanced Stakeholder Confidence

- helps organizations build a comprehensive defense strategy by covering all aspects of cybersecurity.
- showcases a strong cyber risk management culture to external stakeholders.
- Provides confidence that appropriate controls are in place to protect data and ensure continuity



2. Cybersecurity Maturity Assessment and support Continuous Improvement

- A clear picture of where you are today and what to improve tomorrow.
- understand the maturity of your governance, processes, and integration.
- Current Profile and Target Profile, allowing gap analysis and improvement roadmap



3. Enterprise-Wide Risk Management Alignment, its Customizable and Scalable

- Organizations can define their own "profiles" that reflect unique goals, regulatory needs, and risk environments.
- emphasizes aligning cybersecurity with organizational governance and risk strategy.
- Cybersecurity becomes a board-level priority, not just an IT issue.



4. Prioritization of Investments

- Maturity assessment and profiling help identify critical areas for improvement.
- Avoids wasting resources on low-priority or ineffective solutions.
- Optimized security investment for maximum risk reduction.

And many more.....

Incident Response and Recovery Readiness

Regulatory and Standards Alignment

Improved Communication Across Functions

Better Supply Chain Security

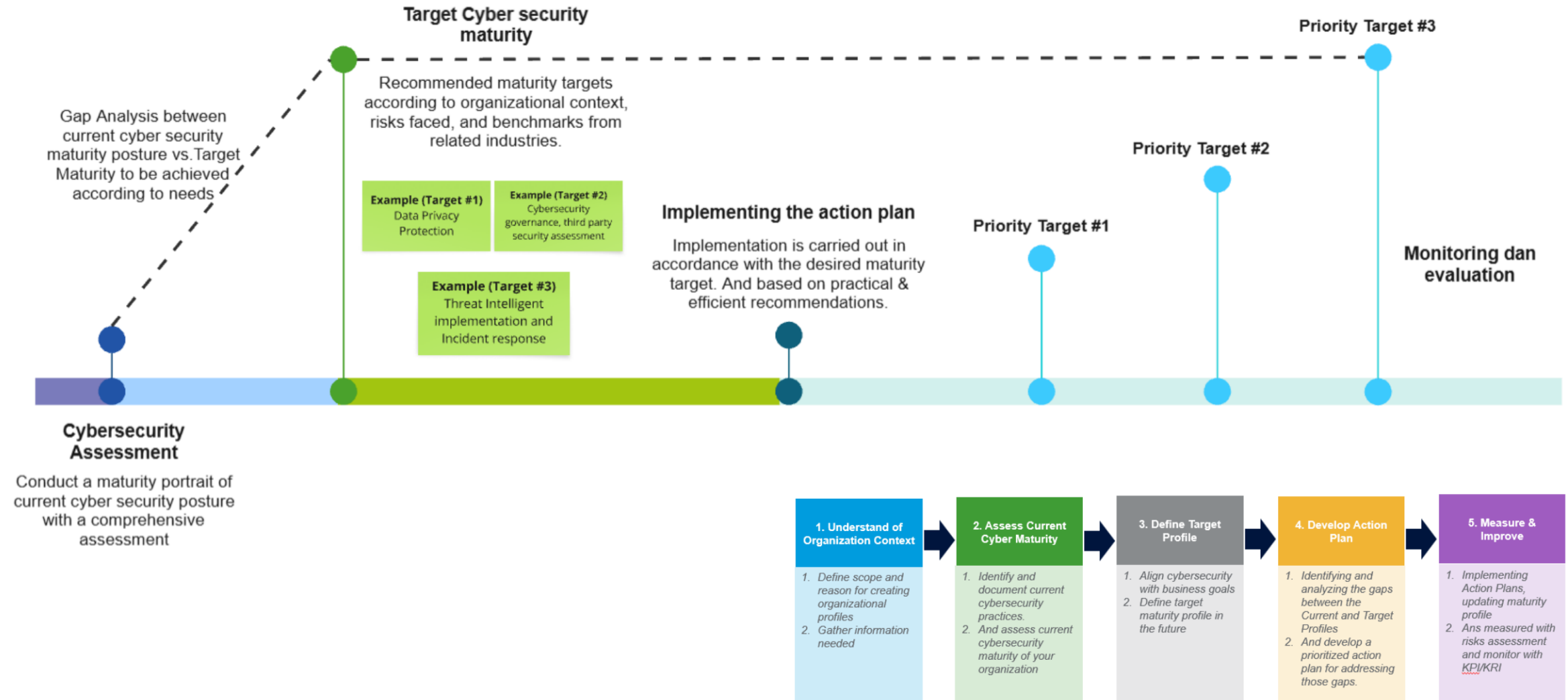
HOW TO IMPLEMENT NIST CSF 2.0 IN YOUR COMPANY

How to Implement NIST CSF 2.0 (1/2)

“Since cybersecurity risks are expanding constantly, managing those risks must be a continuous process”



How to Implement NIST CSF 2.0 (2/2)



Capturing Cybersecurity Current Posture and Targeting Next Maturity and Improvement

CSF Organization Profile



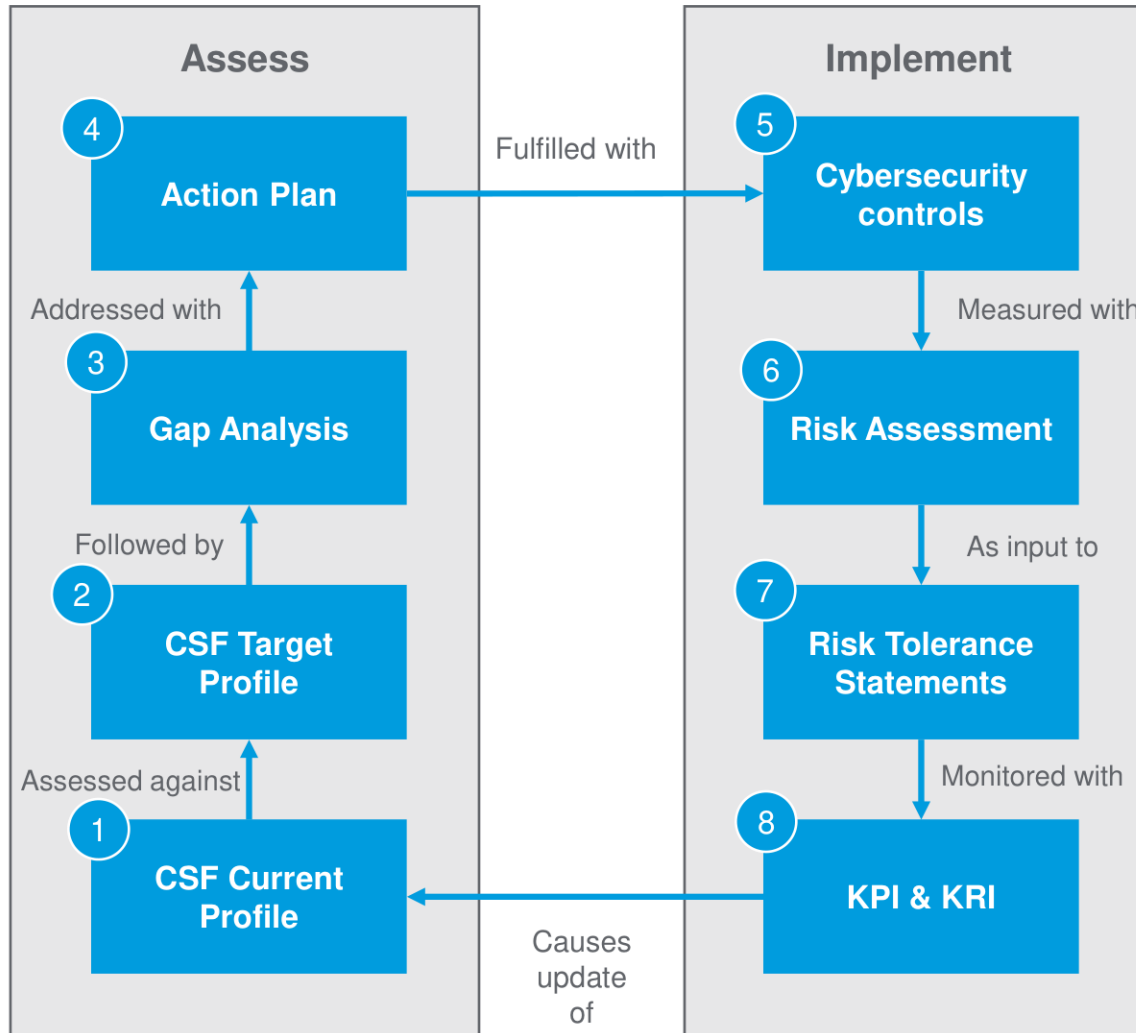
Fig. 3. Steps for creating and using a CSF Organizational Profile

- A **CSF Organizational Profile** describes an organization's current and/or target cybersecurity posture in terms of the Core's outcomes.
- Organizational Profiles are used to understand, tailor, assess, prioritize, and communicate the Core's outcomes by considering an organization's mission objectives, stakeholder expectations, threat landscape, and requirements.
- An organization can then prioritize its actions to achieve specific outcomes and communicate that information to stakeholders.

CSF Tiers for Cybersecurity Governance and Management

Rating	Description
1 Partial	No policy exists for the control, and it has not been implemented on any systems. This maturity rating indicates that several key elements of data security are not in place.
2 Risk Informed	The control has an informal policy, and only parts of the control have been implemented. This maturity rating indicates an ability to sustain some security efforts, though key controls and programs are lacking.
3 Repeatable	The control has been implemented on most systems and has a formalized policy. This maturity rating indicates an ability to define and meet several security objectives. A few key controls may not be implemented effectively.
4 Adaptive	The control has an approved written policy and has been implemented on all systems. This maturity rating indicates a mature security program has been integrated into company culture. The organization has implemented consistent monitoring and analysis of the security program for continual improvement.

Improving Cybersecurity as Iterative Process, Always Update to Stay Relevance



1. All those activity including cybersecurity controls can be references from other NIST family. For instance, NIST SP 800-53, NIST SP 800-37, NIST SP 800-30. Or even from other source such as ISO 27001:2022
2. Risk Assessment can occur at any time and can inform any step.
3. Monitored can be conducted using Key Performance Indicator and Key Risk Indicator which perform periodically or when significant risks change happen
4. The flow is considered as an iterative process since cybersecurity is not a destination, it's about journey.

Pillar	Recommended Score	Current Score
Govern	4.0	2.0
Identify	4.0	2.0
Protect	4.0	2.5
Detect	4.0	1.9
Respond	4.0	1.8

Overview
There are strong environment protections, but weak user training threatens to undermine organizational security.

Strengths
Access control process in place.
Maintenance processes managed by Optimal Networks and in-place.

Opportunities
Information protection strategy should be created and reviewed. End user cybersecurity training should be implemented.

1.9



Tier: Repeatable

Detailed Finding	Risk	Recommendation
<p>#9 – Undefined end user cybersecurity training strategy</p> <p>Despite intermittent trainings held by Optimal Networks, the TS Alliance has not established security and privacy training standards for employees. Users are the key to a strong information security program. Without consistent, effective hands-on training, and phishing and vishing testing, people are the greatest liability to the security of TS Alliance's assets and data. A formal awareness and training program should be established and include role-based information security training on an ongoing basis. Training materials should be updated to reflect changes to the environment. As an augmentation of user training, advanced preparation for access to sensitive data and systems will enable TS Alliance to protect its reputation, as well as client data.</p>	<p>● Moderate</p>	<p>Establish a methodology to provide consistent cybersecurity training and testing of employees. This can be obtained through a Learning Management System (LMS) with applicable material, or through an external vendor to conduct.</p> <ul style="list-style-type: none"> • Training can be in person, or through a subscription to readymade content. • Testing can be through follow up quizzes, phishing, vishing, etc.
<p>#10 – Formal change management procedures and responsibilities have not been defined</p> <p>The TS Alliance relies on supporting vendors to make changes to its IT infrastructure on an as-needed basis. However, this process has not been formally established to consider whether certain level of changes require management's review and approval and/or end-user testing prior to implementing the change. Change testing and approval should be consistently tracked and documented following a standard methodology so the appropriate stakeholders follow the process to completion; safeguarding both the content and the security of the assets.</p>	<p>● Low</p>	<p>Changes to TS Alliance's network should undergo a consistent process before implementation</p> <ul style="list-style-type: none"> • Contract your MSP to formalize the process through which updates and reconfigurations are vetted, tested, approved, and pushed onto TS Alliance systems

● Low Risk
● Moderate Risk
● High Risk

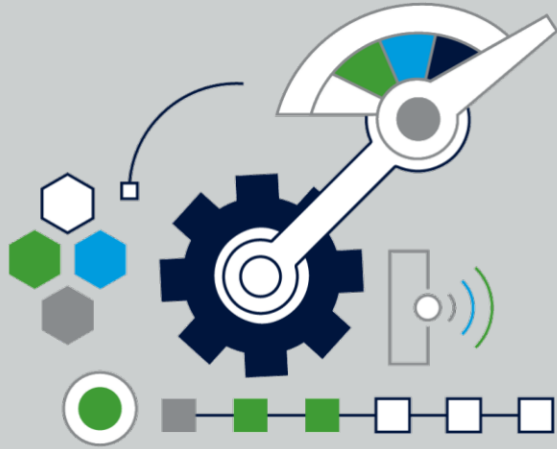
[illegible]

Key Takeaways and Moving Forward

1. **CYBER RISKS ARE BUSINESS RISKS.** THE COST OF INACTION IS RISING- DATA BREACHES, RANSOMWARE, AND REGULATORY FINES CAN SEVERELY IMPACT REPUTATION AND FINANCIAL STABILITY.
2. ORGANIZATIONS **NEED A DYNAMIC, FLEXIBLE FRAMEWORK** TO MANAGE CYBER RISK IN A RAPIDLY CHANGING ENVIRONMENT
3. NIST CSF 2.0 OFFERS A UNIVERSAL, **SCALABLE FRAMEWORK**. DESIGNED TO BE FLEXIBLE FOR **ORGANIZATIONS OF ALL SIZES AND MATURITY LEVELS**.
4. **IMPLEMENTATION IS A JOURNEY, NOT A ONE-TIME PROJECT.** START WITH A CURRENT PROFILE → DEFINE A TARGET PROFILE → CREATE AN ACTION PLAN AND FOCUS ON CONTINUOUS IMPROVEMENT.



Ready for Cybersecurity Transformation?



**Free Cybersecurity Self
Assessment Tools For Your
Exercise**



**Getting Expert Consultation &
Strategic Discussion – Anytime, at
No Cost for your Organization**

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM Indonesia

Plaza ASIA Level 10,
Jl. Jend. Sudirman Kav.59
Jakarta 12190
Indonesia
T +62 21 5140 1340
E inquiry@rsm.id
rsm.id

RSM in Indonesia is represented by KAP Amir Abadi Jusuf, Aryanto, Mawar & Rekan, PT RSM Indonesia Konsultan, PT RSM Indonesia Mitradaya, PT RSM Indonesia Mitradana, PT RSM Indonesia Advisori, member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm which practices in its own right. The RSM network is not itself a separate legal entity in any jurisdiction.

The network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

© RSM International Association, 2025