
CYBERSECURITY IN DE PRAKTIJK

Hoe vertaal je Complexiteit naar een Geïntegreerde Aanpak?





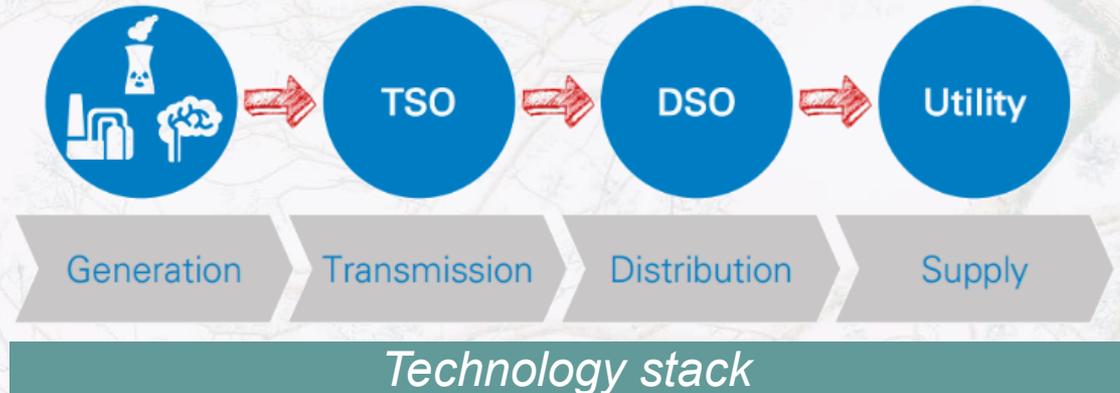
Cyber security in practice

From complexity to unity



#whoami

- 10y+ Cyber security
- 10y+ Energy







What is "Secure"?



Source: Fort Knox - Travis Good.

VS.



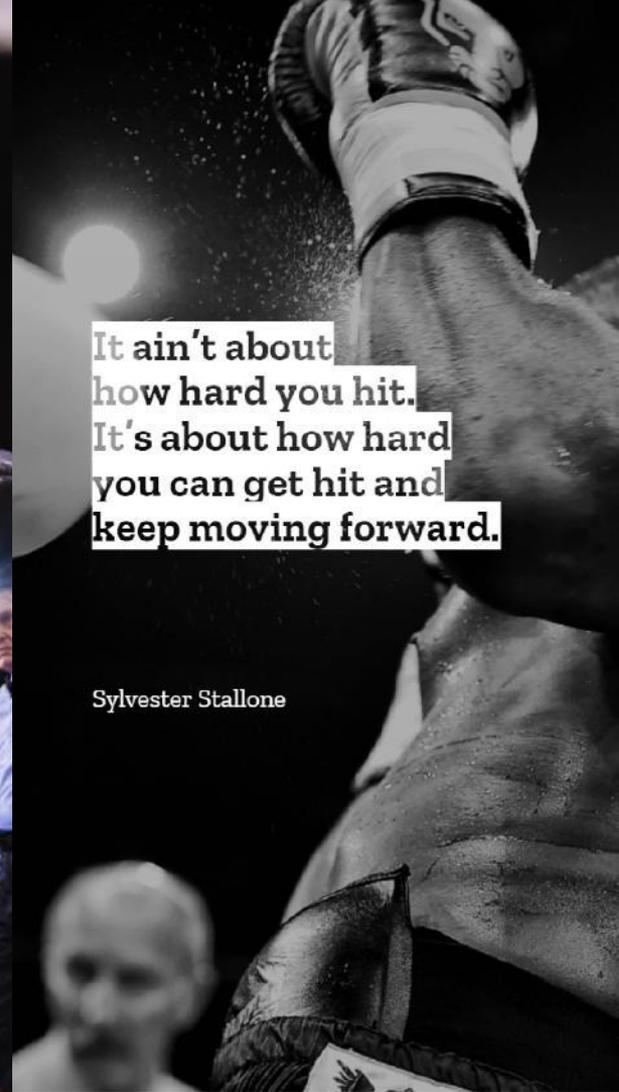
Source: <https://giphy.com/>

Security = Resilience



It ain't about
how hard you hit.
It's about how hard
you can get hit and
keep moving forward.

Sylvester Stallone





Security = Trust

*"Security drives trust,
trust drives business"*



Source: <https://blogs.idc.com/2020/04/22/the-five-elements-of-the-future-of-trust/>



al je vraag

vrtnws

Dossier Zonnepanelen

85 p

LEVEN | MENINGEN

DeMorgen.

POLITIEK

Achtergrond Black-out

IUR | TECHNIEK

POWER OUTAGE
AFTER

EURACTIV

Ukraine Defence The Capitals Politics Economy | Newsletters Videos Events Jobs Advocacy Lab Public Projects
Energy, Environment & Transport

Advocacy Lab Content

EU's energy transition resilience needs action, gas infrastructure funding

Europe needs low-carbon hydrogen, but there's also a push to develop renewable gases and to incentivise the infrastructure. Energy resilience requires all options to be on the table.



Balancing grid with renewables: challenge

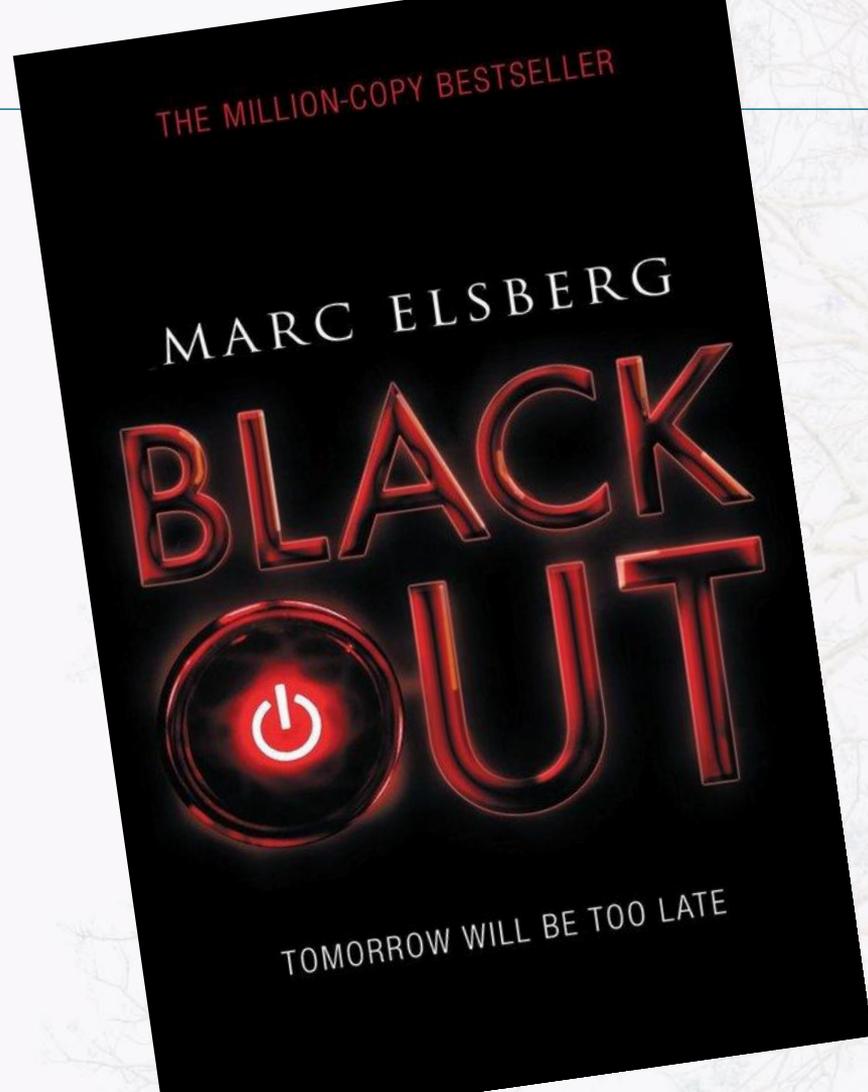


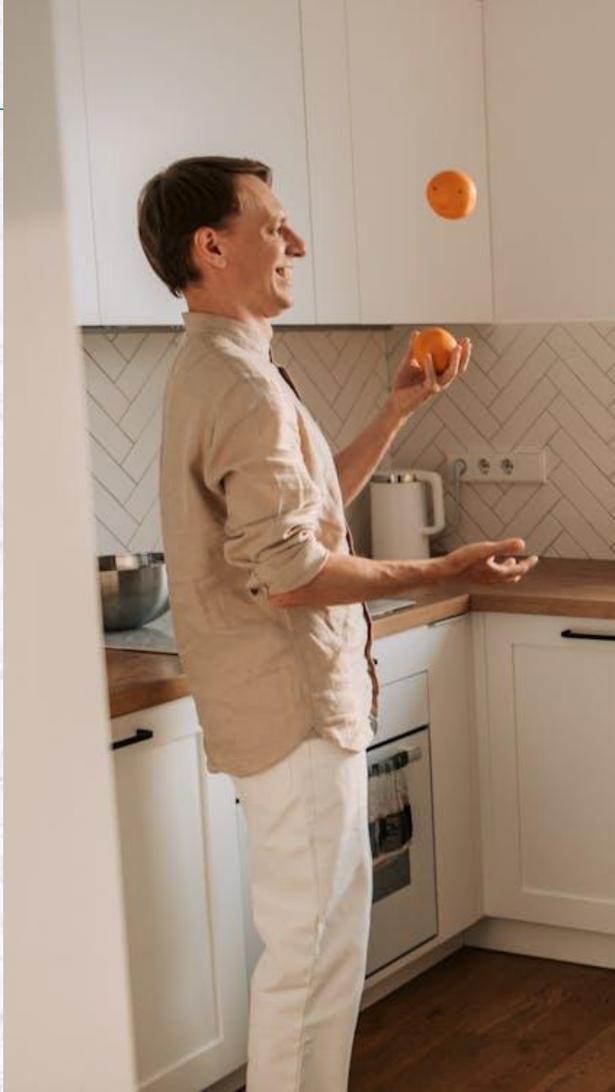
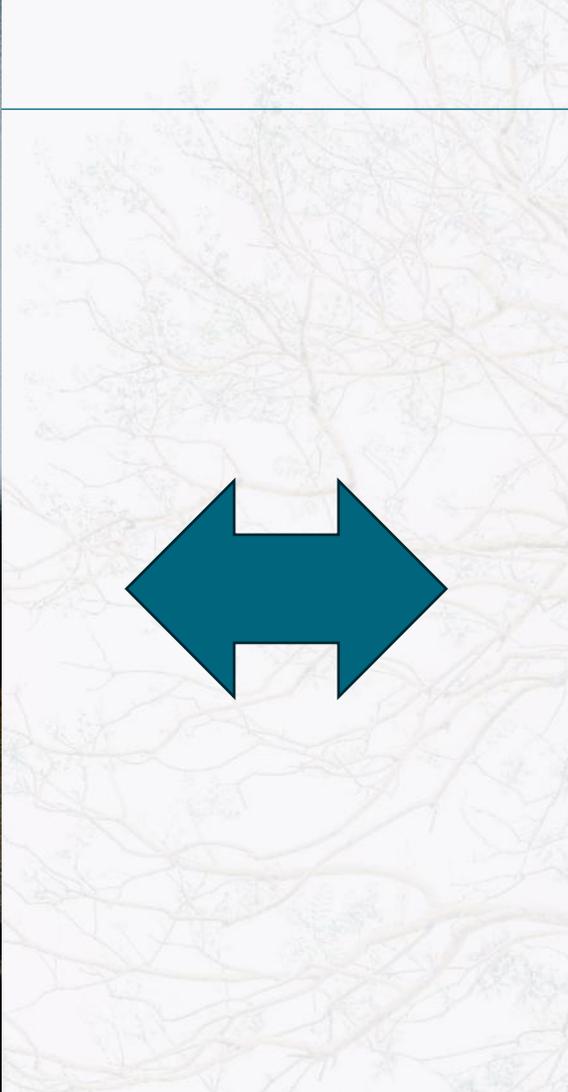
Electric Power Systems Research
Volume 228, March 2024, 110095



A review on frequency management for
low-inertia power systems: From inertia and
fast frequency response perspectives ☆

Jianguo Zhou^a, Ye Guo^a ✉, Lun Yang^b, Jiantao Shi^a, Yi Zhang^c, Yushuai Li^d, Qinglai Guo^e,
Hongbin Sun^e







Source: Tenor



One Day
OR
Day One?

YOU DECIDE.



**Successful investing is about
managing risk, not avoiding it.**

Benjamin Graham

 quotefancy





Odds that something happens

$$\mathbf{Risk} = \mathbf{Likelihood} * \mathbf{Impact}$$

How bad it will be





Risk mgmt.

What it
actually is



How it feels
like



Source/Copyright: Disney

Law & Order

"Rules for thee but not for me"

Cyber Resilience Act

The Cyber Resilience Act enhances cybersecurity standards of a key component, requiring manufacturers and retailers to secure their products.

NIS2 Directive: new rules on cybersecurity of network and information systems

Table 1: Overview of EU Legislations in the Digital Sector

Applicable law

Proposed by the European Commission as potential legislative initiative

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance
Digital Europe Programme Regulation, (EU) 2021/694	Recovery and Resilience Facility Regulation, (EU) 2021/241	Frequency Bands Directive, (EU) 1997/72	European Statistics, (EC) 2009/222, 2022/0227(COD)	Databases Directive, (EC) 1996/9	Regulation for a Cybersecurity Act, (EU) 2019/831, 2022/0198(COD)	Law Enforcement Directive, (EU) 2016/680	Product Liability Directive (PLD), (EU) 1985/274, 2022/0302(COD)	Unfair Contract Terms Directive (UCTD), (EC) 1993/93	EC Merger regulation, (EC) 2002/726, (update soon)	Satellite and Cable I Directive, (EU) 1993/68	Common VAT system, (EC) 2006/112, 2022/0407(CNS)
Horizon Europe Regulation, (EU) 2021/546, (EU) 2021/754	Innov8EU Programme Regulation, (EU) 2021/1592	Radio Spectrum Decision, (EU) 2017/826	General Data Protection Regulation (GDPR), (EU) 2016/679	Community Design Directive, (EU) 2009/24	Regulation to establish a European Cybersecurity Cooperation Centre, (EU) 2021/867	Directive on countering fraud and counterfeiting of non-cash means of payment, (EU) 2019/713	Toys Regulation, (EU) 2009/48, 2022/0209(COD)	Price Indication Directive, (EC) 1993/93	Technology Transfer Block Exemption, (EU) 2015/118	Information Society Directive, (EC) 2002/22	Administrative cooperation in the field of taxation, (EU) 2011/116
Regulation on a pilot regime for distributed ledger tech. markets, (EU) 2022/958	Connecting Europe Facility Regulation, (EU) 2013/1653	Broadband Cost Reduction Directive, (EU) 2011/651, 2022/0938(COD)	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Enforcement Directive (FR), (EC) 2006/46	NIS 2 Directive, (EU) 2022/2526	Regulation on an interoperability between EU information systems in the field of border and visa, (EU) 2019/817	European Standardisation Regulation, (EU) 2017/1003	E-commerce Directive, (EC) 2000/31	Company Law Directive, (EU) 2017/1322, 2022/0038(COD)	Audio-visual Media Services Directive (AVMSD), (EU) 2010/13	Payment Service Directive 2 (PSD2), (EU) 2015/2366, 2022/0205(COD)
Regulation on High Performance Computing Joint Undertaking, (EU) 2017/1172	Open Interest Access Regulation, (EU) 2018/2730	Open Interest Access Regulation, (EU) 2018/2730	Regulation on the free flow of non-personal data, (EU) 2018/1807	Directive on the protection of trace secrets, (EU) 2016/683	Information Security Regulation, 2022/0904(COD)	Regulation on terrorist content online, (EU) 2021/7784	eIDAS Regulation, (EU) 2015/1810, 2022/0213(COD)	Unfair Commercial Practices Directive (UCPD), (EC) 2005/29	Market Surveillance Regulation, (EU) 2017/1100	Portability Regulation, (EU) 2017/1128	Digital Operational Resilience Act (DORA) Regulation, (EU) 2022/2534
Regulation on Joint Undertakings under	European Electronic Communications Code	Open Data Directive	Open Data Directive	Design Directive	Cybersecurity Regulation, 2022/0904(COD)	Temporary CSAM Regulation, (EU) 2021/1222, 2022/0193(COD)	Radio Equipment	Directive on Consumer Remedies, (EU) 2022/0154	FRB Regulation	Satellite and Cable II	Crypto-assets

Data & Privacy:
 ES, GDPR, EU PDP, EU
 FFNPD, PSI ODD, DGA,
 ePrivacy, EDA, EHDSA, ...

Cybersecurity
 CSA, ECC, NIS2, EU ISR,
 CSR, CRA, CS Act, ...

for Europe Platform
 (ETEP),
 2022/0194(COD)

Digital Networks Act,
 2022/0235(COD)

Directive on a framework
 for artificial intelligence,
 2022/0254(COD)

Interoperable Europe
 Act, 2022/0279(COD)

Harmonization of GDPR
 enforcement,
 2023/0020(COD)

Access to vehicle data,
 functions and resources

Open Data Act

Directive on the sale of
 goods,
 (EU) 2019/721

(RBE N),
 (EU) 2023/0918,
 (EU) 2023/1067

AI Liability Directive,
 2022/0039(COD)

Digital Services Act (DSA)
 Regulation, (EU) 2022/2065

Platform Work Directive,
 2021/0641(COD)

Political Advertising
 Regulation,
 2023/0381(COD)

Single Market
 Emergency instrument
 (SMEL),
 2022/0278(COD)

Right to repair Directive,
 2022/0033(COD)

Multimodal digital
 mobility services (MDMS)

Consumer protection,
 strengthened
 enforcement
 cooperation



Why so many rules and regulations?

1. EU wants to heighten the **resilience** of the EU society
2. EU wants its residents to be better protected, within EU and outside of it
3. But we can't impose the same rules for everyone

Some sectors need a bigger nudge or are more critical, hence the differences in DORA, NIS2, CER, ...

Some topics need different enforcement mechanisms

Each discipline is implemented differently in member states



Differences in companies within sectors

PV Inverter
manufacturer

Main risks are in production of insecure/vulnerable product and potential insecure remote monitoring, potential Intellectual property theft

O&M service
provider

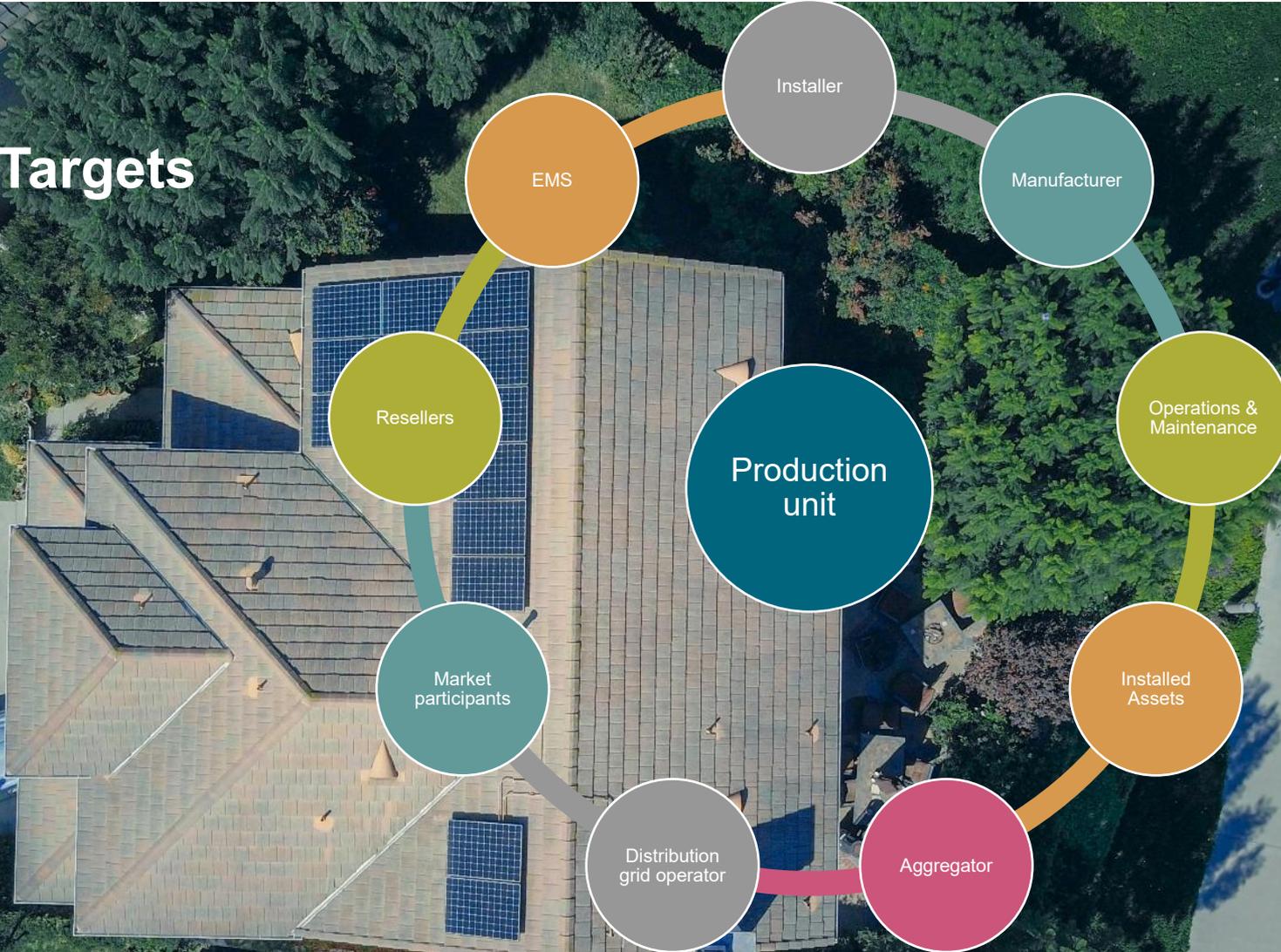
Main risks are in unlawful plant control and potential insecure remote monitoring/control + customer data

What should I consider?

“THE SCOPE”



Targets



VS.





Defenders vs attackers (*Blue vs Red team*)



Source: Twentieth Century Fox



Source: LPGA



As the joke goes, you don't have to be faster than the wolf chasing you, just faster than everyone else running away.

Kim Harrison

“ quote fancy

port:102 country:BE

Overview ▾ Facet

// TOTAL RESULTS

24 MONTHS AGO

345

↓ 2.68%

12 MONTHS AGO

446

↓ 32.74%

6 MONTHS AGO

290

↑ 15.86%

3 MONTHS AGO

366

↓ 8.93%

1 MONTH AGO

237

↑ 41.77%

NOV 2025

336





How to start?

CYBERSECURITY

TIPS TO KEEP YOU & YOUR COMPANY SAFE

PATCH YOUR

Making sure all your systems can be updated is one of the most important things you can do. According to Verizon, only 42% of companies have implemented 42% of the opportunity that we give...

USE PA

Use a 12+ char password with symbols, numbers & the easiest to remember. Password generators are available to help you create a strong password.

Cyber Security Tips for Employees

- Keep software up to date
- Create strong passwords
- Know how to identify phishing attempts
- Check for authentication

TOP 10 NETWORK SECURITY TIPS

- 1 Be aware of phishing attacks
- 2 Biometric identifications
- 3 Password security
- 4 Safeguard your data
- 5 Mobile savviness
- 6 Manage risks with the Internet of Things
- 7 Keep the operating system updated
- 8 Stay informed of current cyber-attacks events & follow precaution measures
- 9 PsyOps
- 10 Smart Shopping

Cyber Security

Essential Tips for Businesses

- 1 Get Antivirus Software
Install antivirus software on all work computers and any mobile devices.
- 2 Educate Staff
Train your employees on how to spot phishing emails and how to react in such times, regularly.
- 3

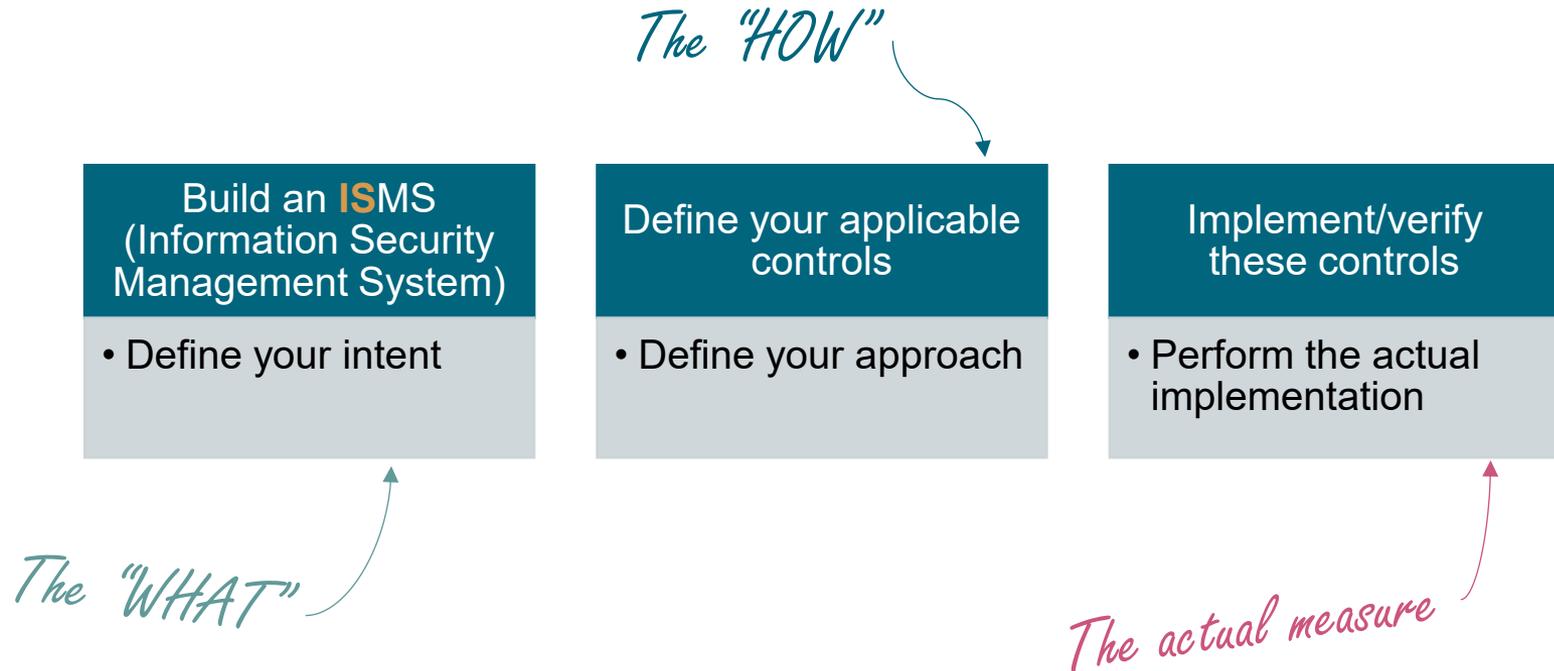
SECURITY TIPS

LE VPN
INTERNET BY YOUR OWN RULES





Plan







Working with frameworks

Governance framework

- Defining all the rules and their intent

Control framework

- Defining all the measures you will take

Implementation framework

- Structure to ensure successful implementation





Governance framework – Example

Information Security Policy

3 Information Security Policy

3.1 Purpose

The purpose of this policy is to set out the information security policies that apply to the organisation to protect the confidentiality, integrity, and availability of data.

3.2 Scope

All employees and third-party users.

3.3 Principle

Information security is managed based on risk, legal and regulatory requirements, and business need.

3.4 Chief Executives Statement of Commitment

"As a company, information processing is fundamental to our success and the



Implementation example

- “We want to be the best-in class regarding the privacy of our customers”
- Our employees are customer-first minded and take utmost care of our customers data.



Control Frameworks – CSF/CyFun



Source: NIST CSF v2 / CCB Cyber Fundamentals 2025



Controls: Example – CyFun

Asset inventory

ID.AM-01.2 The inventory of enterprise assets associated with information and information processing facilities shall reflect changes in the organisation's context and include all information necessary for effective accountability.

Implementation guidance

The goal of this control is to ensure that asset inventories support operational transparency, enable responsible ownership, and adapt to changes in the organisation's structure, technology, and risk landscape.

To achieve this goal:

- **Include Essential Asset Details**
Inventories should capture key specifications such as manufacturer, device type, model, serial number, machine name, network address, and physical location. OT assets should be included where applicable.
- **Support Accountability**
Asset records should enable traceability of actions and decisions, ensuring that responsible parties can be identified and held answerable for outcomes.
- **Reflect Organisational Changes**
Inventories should be updated to reflect changes such as asset relocation, upgrades, or decommissioning.



Implementation: Example



VS.

Microsoft Endpoint Manager admin center

Home > Devices > WIN10TEST

WIN10TEST | Discovered apps

Search (0/10)

Report

Application Name	Application Version
Microsoft.MicrosoftEdge.Stable	92.0.902.67
Microsoft.Services.DesktopEngagement	10.0.19011.0
Microsoft.Windows.Common-Infrastructure	14.0.27610.0
Microsoft.NET.Native.Runtime.1.7	1.7.25531.0
Microsoft.NET.Native.Framework.1.7	1.7.25531.0
Microsoft.LLNL.L2.8	2.1810.21804.0
Microsoft.VCLibs.140.00.UWPDesktop	14.0.27610.0
Microsoft.NET.Native.Runtime.2.0	2.2.27550.0
Microsoft.NET.Native.Framework.2.2	2.2.27510.0
Microsoft.Windows.Common-Infrastructure	10.1008.50
Microsoft.BingWeather	4.2.200622
Microsoft.DesktopAppInstaller	2020.1111.20200.0
Microsoft.DetachApp	10.2108.02050.0
Microsoft.Getstarted	10.6.42361.0
Microsoft.HiFiManager	1.0.42320.0
Microsoft.Messaging	2019.123.0.10000
Microsoft.MicrosofTViewer	2021.2102.4010.0
Microsoft.MicrosoftOfficeHub	18.2106.12410.0
Microsoft.MicrosoftSoftwareCollection	4.10.7740.0
Microsoft.MicrosoftStickyNotes	4.1.0.0
Microsoft.MixedRealityPortal	2020.2102.11.2021.0
Microsoft.MSPaint	2021.2102.4017.0

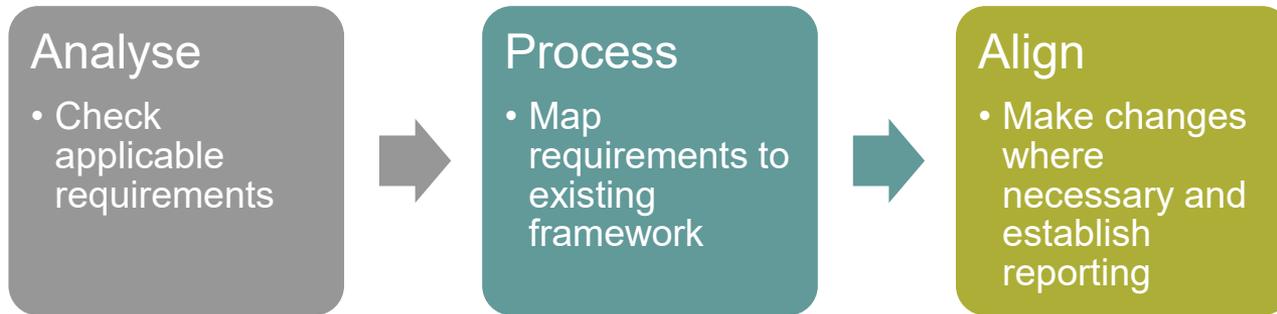
VS.

...



How to process changes

- E.g. NIS2





NIS 2

- Analyse:
 - What are the requirements? *E.g. Mandatory incident reporting*
- Process
 - Map requirements to own governance/control framework *E.g.*
 - *RS.CO-02: Internal and external stakeholders are notified of incidents*
 - *RC.CO-04 Public updates on incident recovery are shared using approved methods and messaging*
- Align
 - Update policies, controls and implementation where needed *E.g. add "send short initial warning to Belgian CSIRT within 24h"*



Source: HLN

It is not that hard
to get started



Use a framework
to keep
structure/overview



Work risk-based!



How easy is it?



where i can download motivation?



The best way of learning
about anything is by doing.

Richard Branson



LITTLE BOBBY



by Robert M. Lee and Jeff Haas





**BLACK
FRIDAY
SALE**







Thank you!

