CYBERSECURITY IN DE PRAKTIJK

Hoe vertaal je Complexiteit naar een Geïntegreerde Aanpak?

Techlink
Linking technicians

wpp
warmtepomp platform

PV-Vlaanderen
fotovoltaïsche zonne-energie

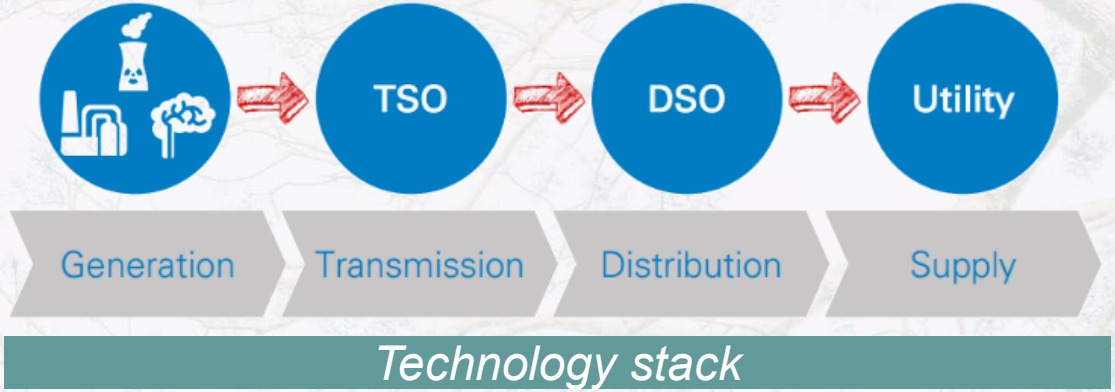
TOREON

Cyber security in practice
From complexity to unity

#whoami

- 10y+ Cyber security
- 10y+ Energy

SCAN ME



What is ”Secure”?

Source: Fort Knox -Travis Good.

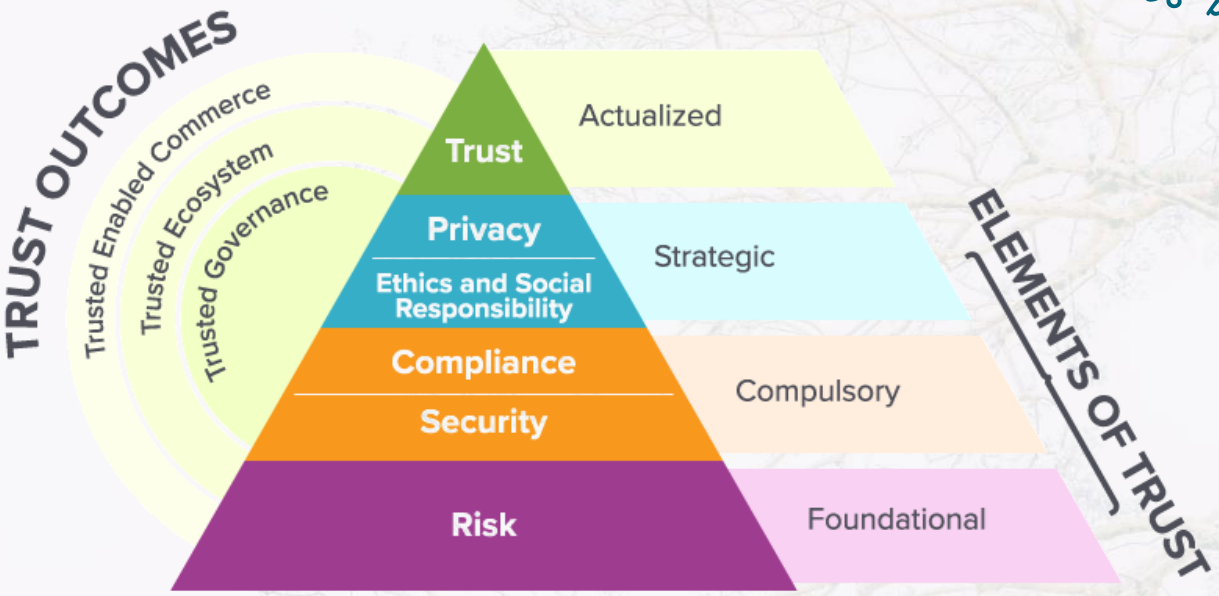
vs.

Source: https://giphy.com/

Security = Resilience

Security = Trust

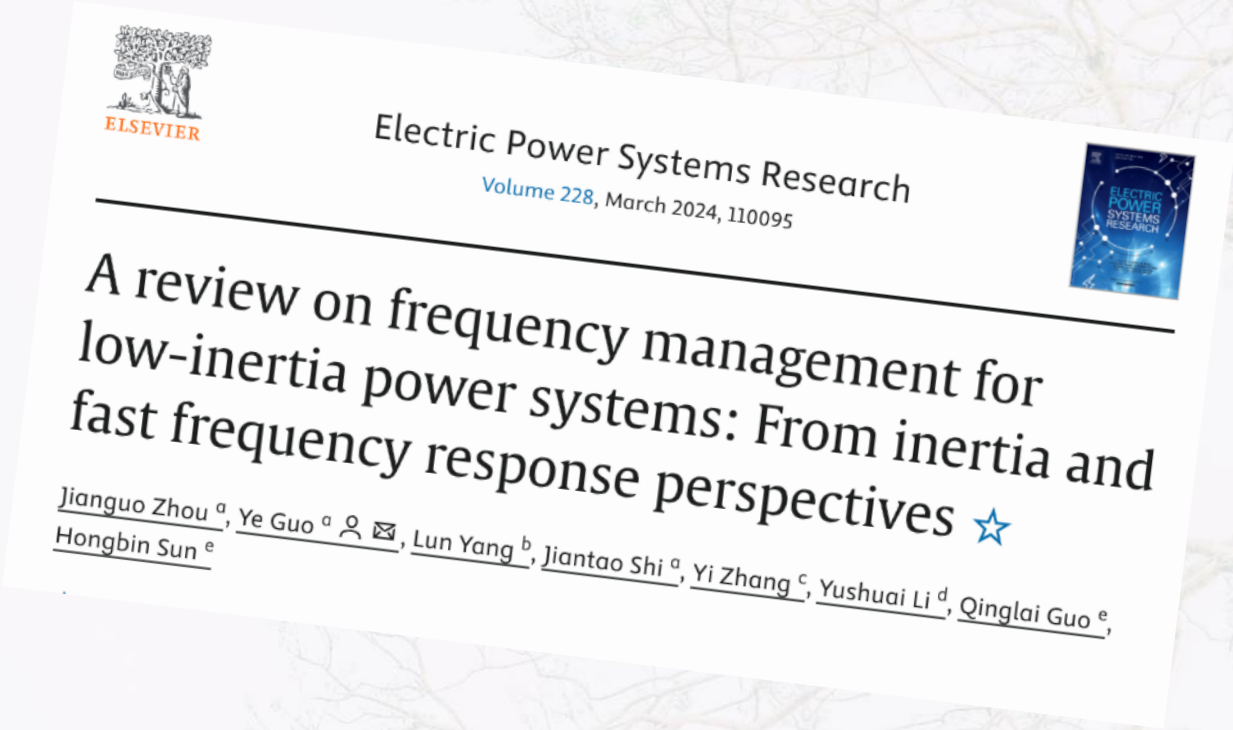
"Security drives trust, trust drives business"



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


l je vraag
vrt nws
Dossier Zonnepanelen
LEVEN | MENINGEN | POLITIEK
DeMorgen.
Achtergrond Black-out
POWER OUTAGE
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
Energy resilience requires all options to be on the table.

Balancing grid with renewables: challenge



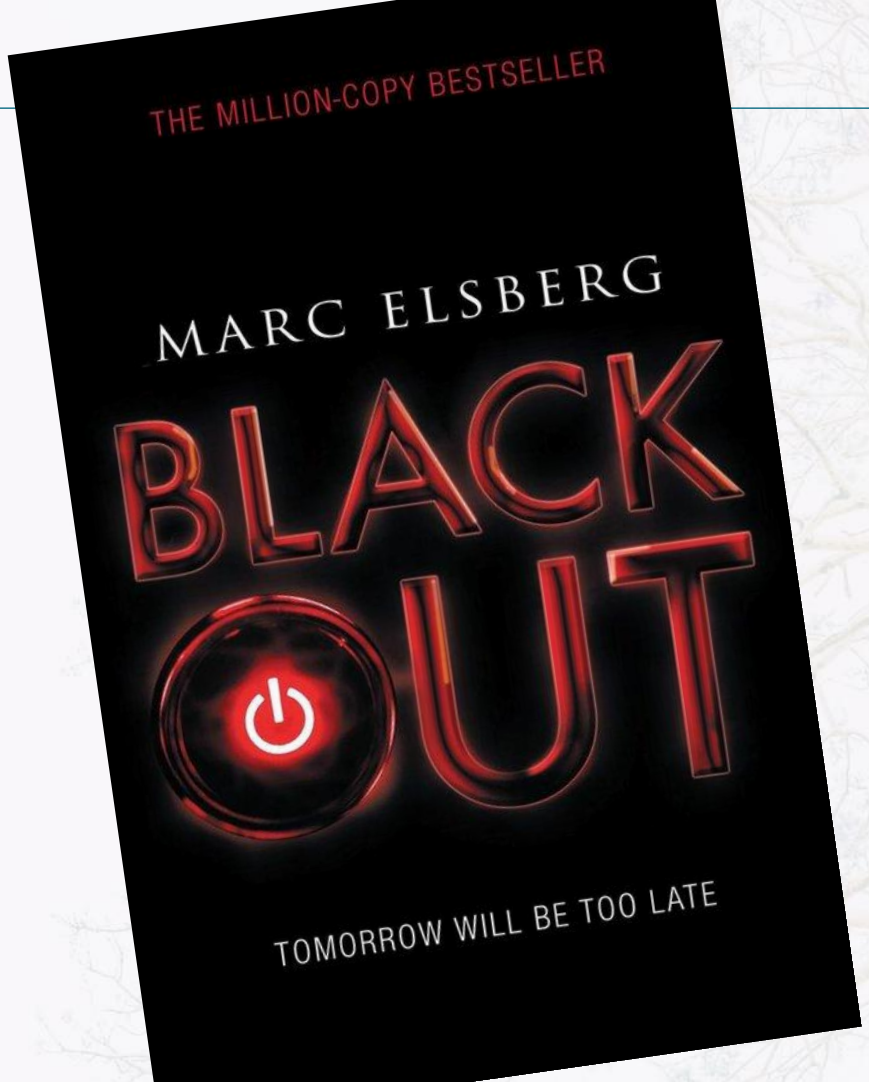
ELSEVIER

Electric Power Systems Research

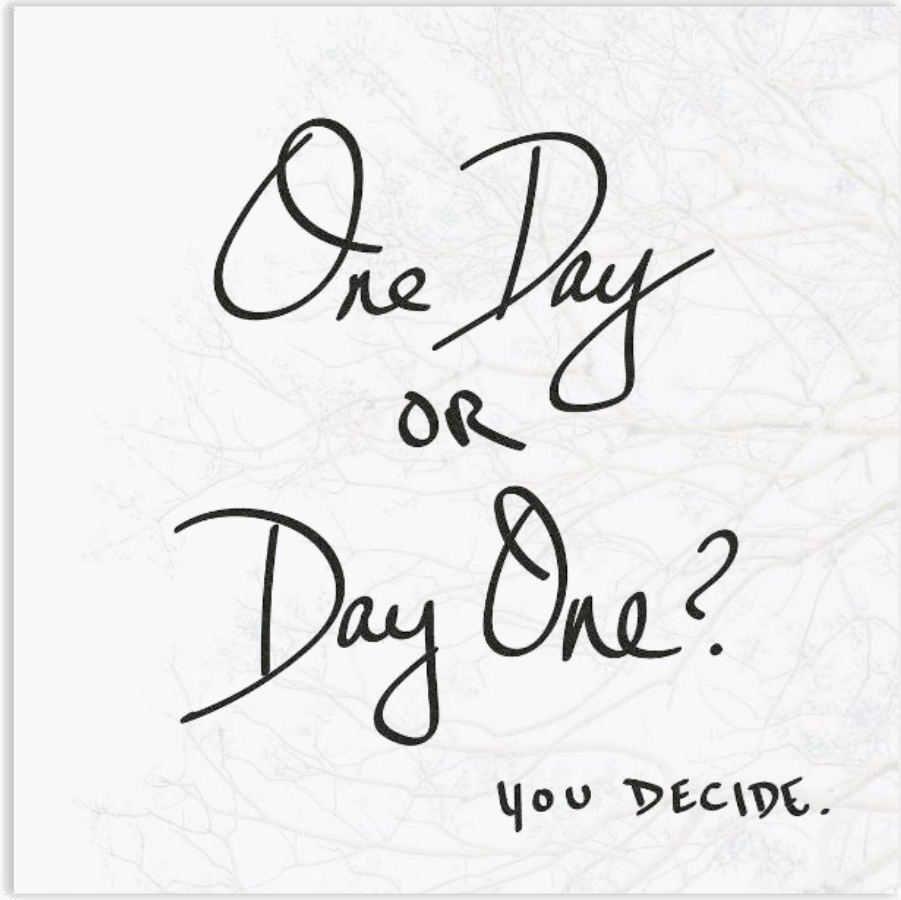
Volume 228, March 2024, 110095

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]


THE MILLION-COPY BESTSELLER
MARC ELSBERG
BLACK OUT
TOMORROW WILL BE TOO LATE

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

Risk = Likelihood * Impact

How bad it will be

Risk mgmt.

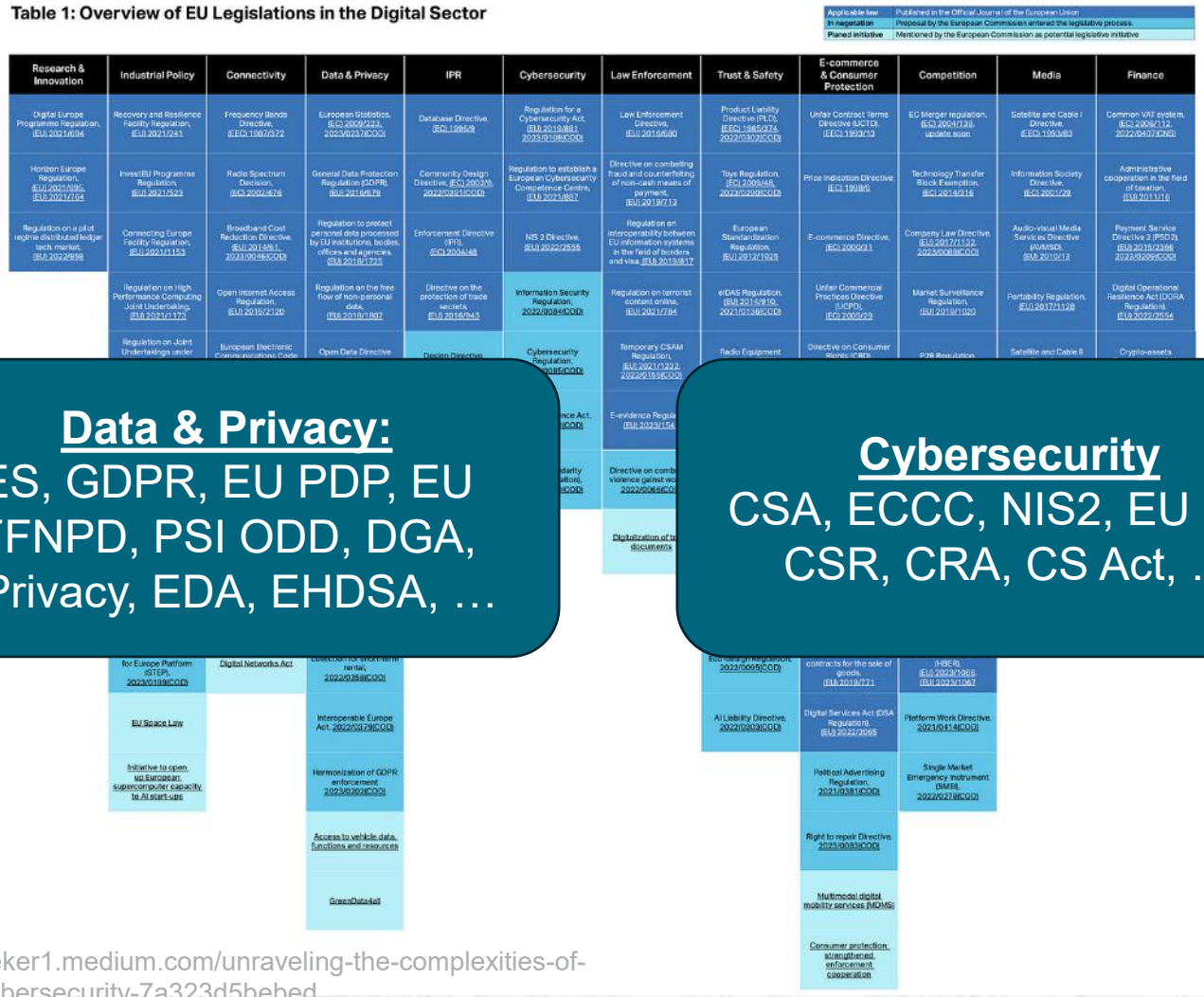
What it actually is

How it feels like

Source/Copyright: Disney

Law & Order

"Rules for thee but not for me"



Source: https://ensarseker1.medium.com/unraveling-the-complexities-of-eu-legislation-part-1-cybersecurity-7a323d5bebed

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

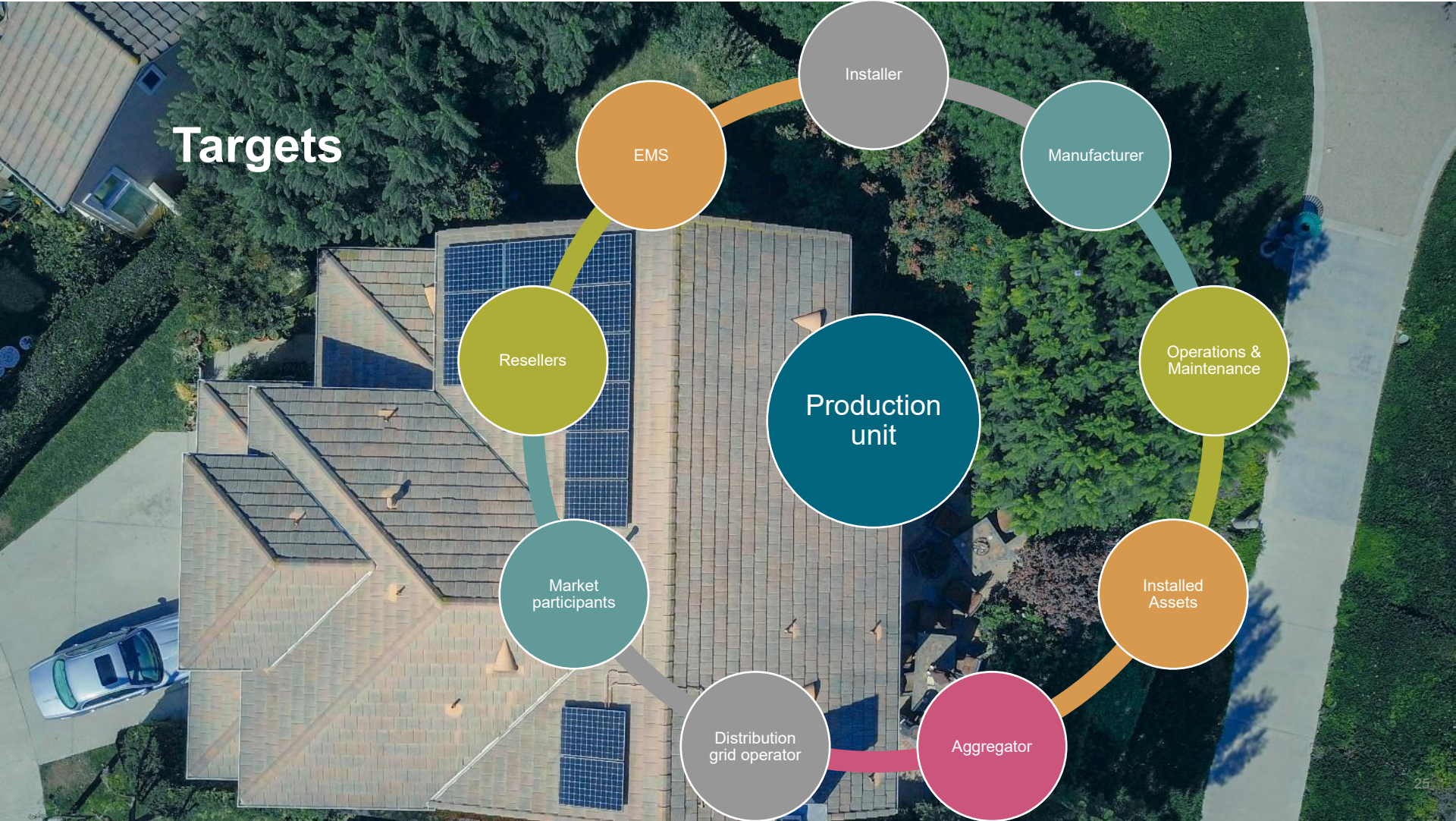
Differences in companies within sectors

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

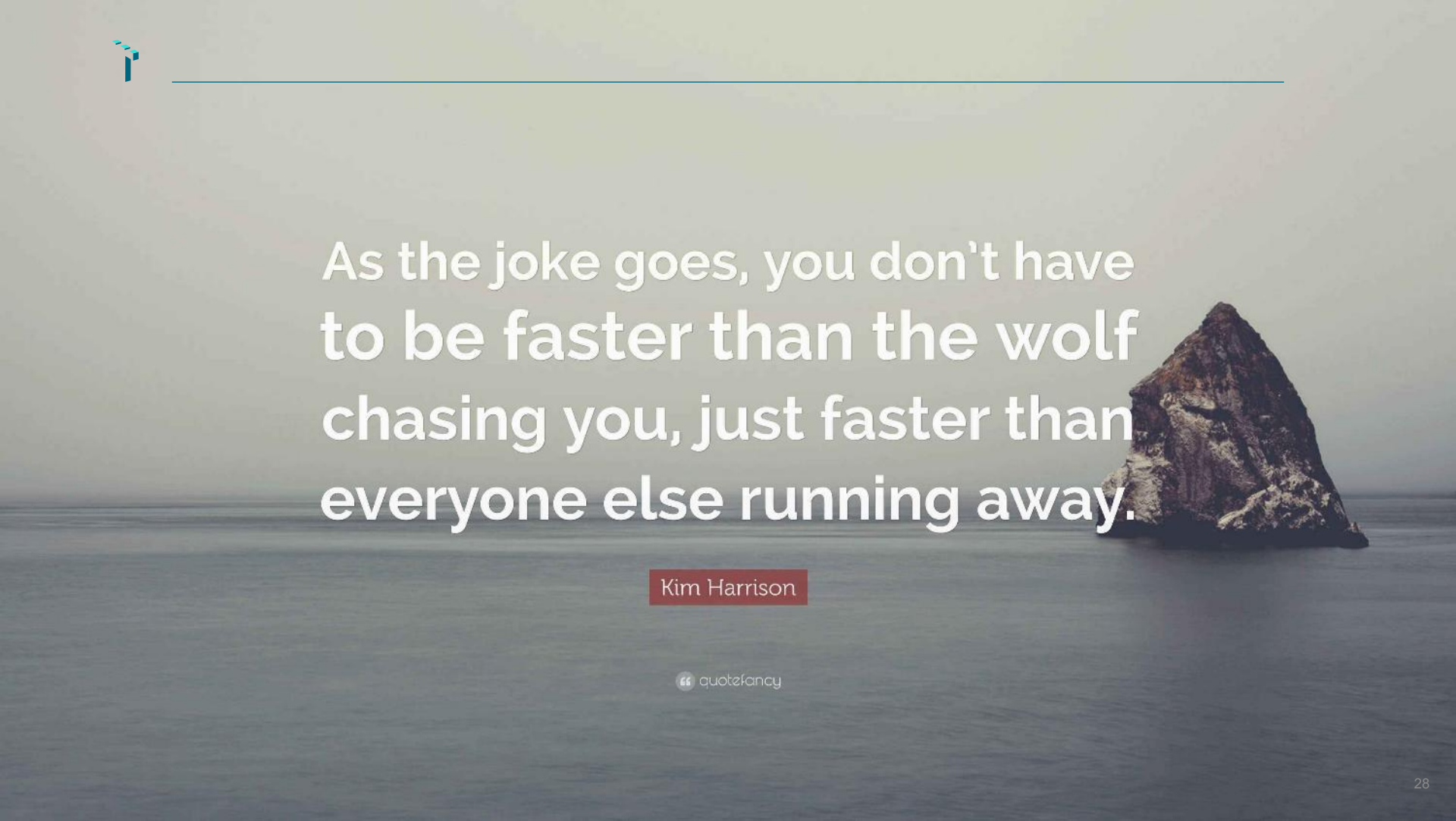

Installer
Manufacturer
Operations & Maintenance
Installed Assets
Aggregator
Distribution grid operator
Market participants
Resellers
EMS
Production unit


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
quotefancy

port:102 country:BE

Overview | Facet

// TOTAL RESULTS

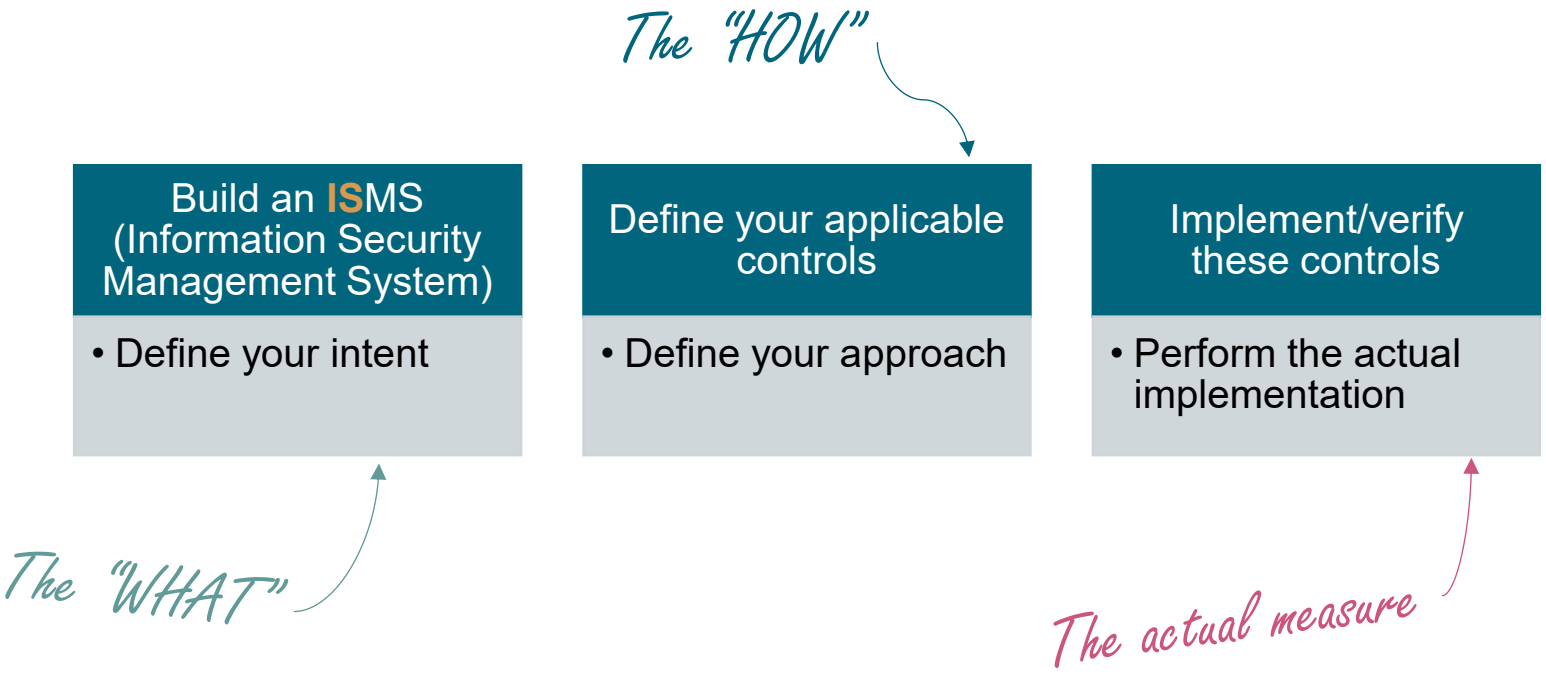
24 MONTHS AGO	12 MONTHS AGO	6 MONTHS AGO	3 MONTHS AGO	1 MONTH AGO	NOV 2025
345	446	290	366	237	336
↓ 2.68%	↓ 32.74%	↑ 15.86%	↓ 8.93%	↑ 41.77%	

TOREON

How to start?


CYBERSECURITY
TIPS TO KEEP YOU & YO COMPANY SAFE
PATCH YOUR
USE PA
Cyber Security
Tips for Employees
Keep software up to date
Create strong passwords
Know how to identify phishing attempts
CAMBRIDGE SUPPORT
IT Security & Cloud Specialists
Cyber Security
Essential Tips for Businesses
Get Antivirus Software
Educate Staff
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
CURITY TIPS
LE VPN

Plan


The "HOW"
Build an ISMS (Information Security Management System)
• Define your intent
Define your applicable controls
• Define your approach
Implement/verify these controls
• Perform the actual implementation
The "WHAT"
The actual measure

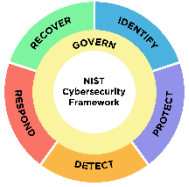
Working with frameworks

Governance framework	Control framework	Implementation framework
• Defining all the rules and their intent	• Defining all the measures you will take	• Structure to ensure successful implementation

ISO 27001

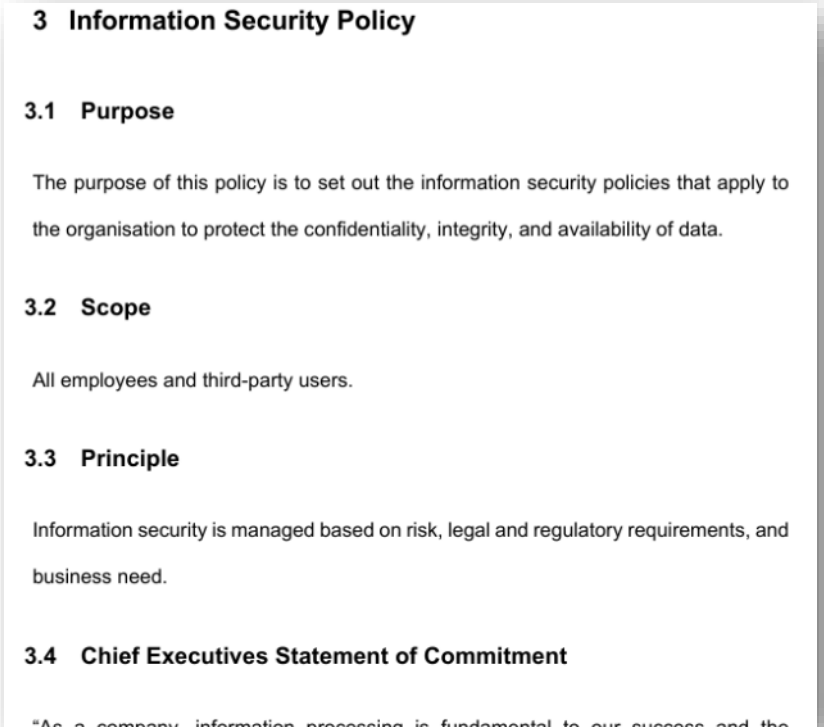
ISO 27002

CyFun®



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

Source: Hightable.io

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

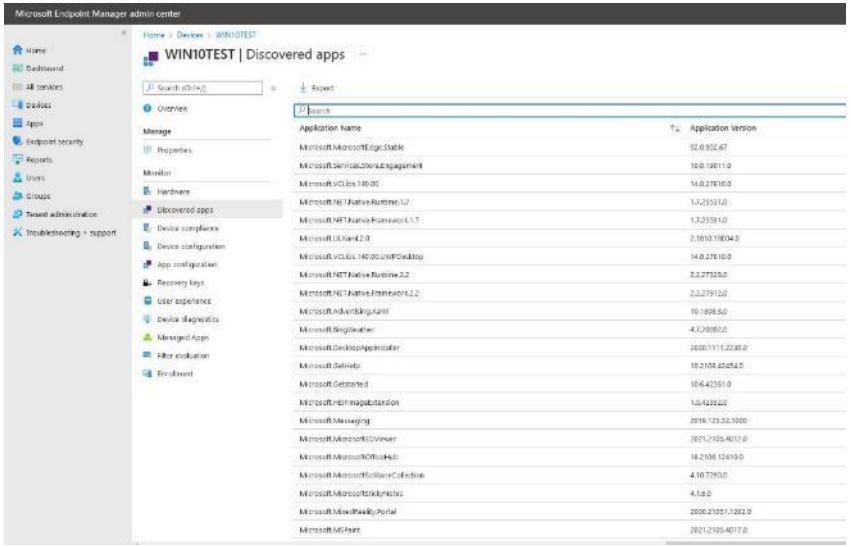
The goal of this control is to ensure that asset inventories support operational transparency, enable responsible ownership, and adapt to changes in the organisation's structure, technology, and risk landscape.

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

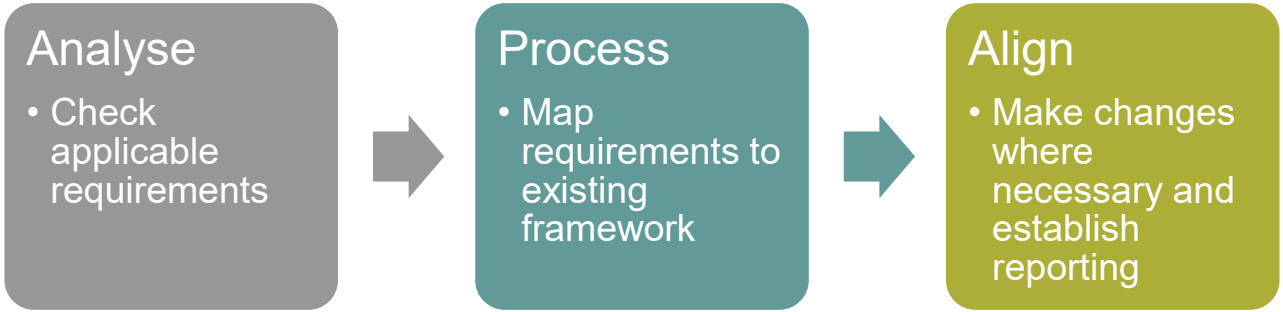
vs.



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
quotefancy


LITTLE BOBBY
by Robert M. Lee and Jeff Haas
HERE'S THE NEW STANDARDS FRAMEWORK.
WHO DESIGNED THIS?
A COMMITTEE.
OF EXPERTS ON THIS TOPIC?
OF PEOPLE AVAILABLE.
DOES IT LOOK BETTER THAN OTHERS?
MEH-- IT'S AVAILABLE.
HAAS


BLACK
FRIDAY
SALE


30%
OFF


PARAMECIUM

Thank you!