System Auditing – Helping or disrupting?

KENNETH WAABEN NIELSEN

Disclaimer!

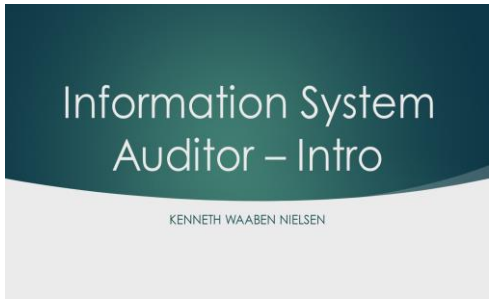
The opinions expressed in this presentation and on the following slides are solely those of the presenter

This presentation is for educational purposes only (Fair use)

whoami

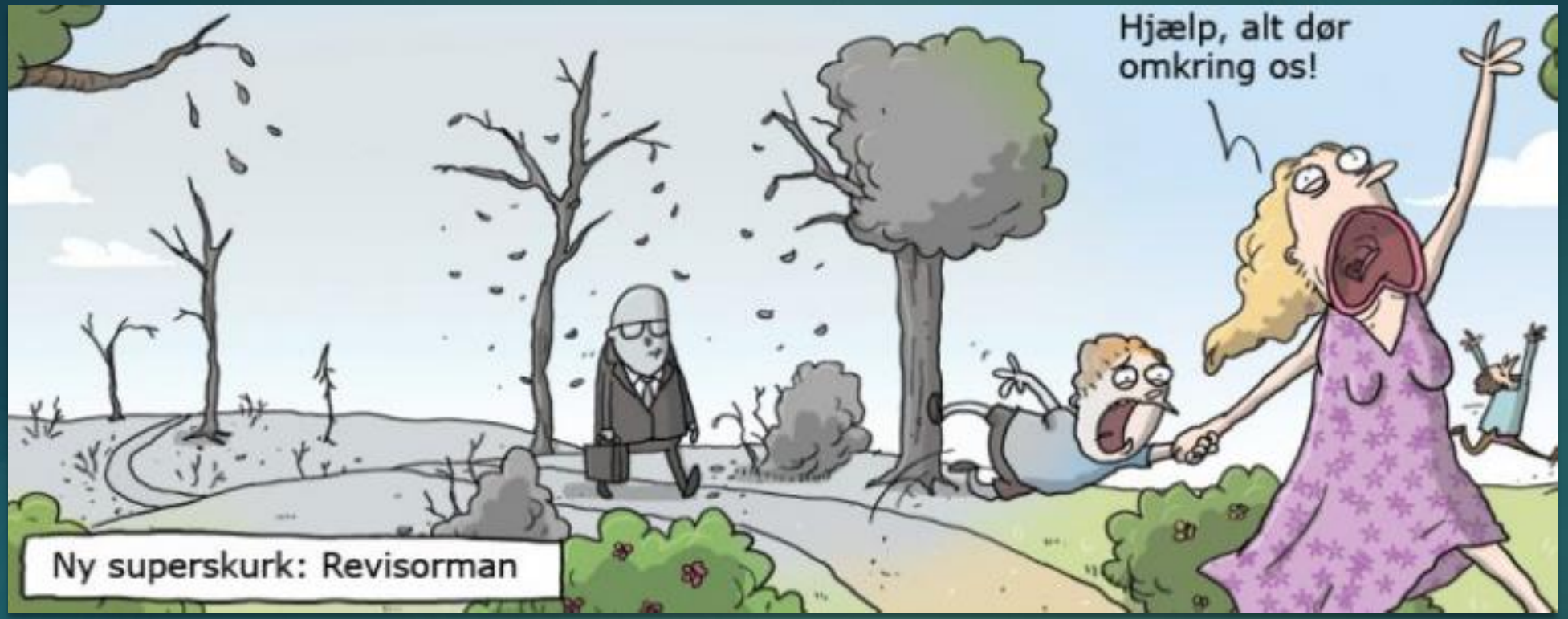
- Kenneth Waaben Nielsen
- 41 years
- Married + 2 kids
- +13 years as system auditor
- +8 years in JN Data
  - Technical Lead Auditor
- Certs: Security+, CISA, CISSP
- Like to learn stuff

Why this talk?



LinkedIn

OWASP
Open Web Application Security Project



Prejudices

INFOSEC

…

…

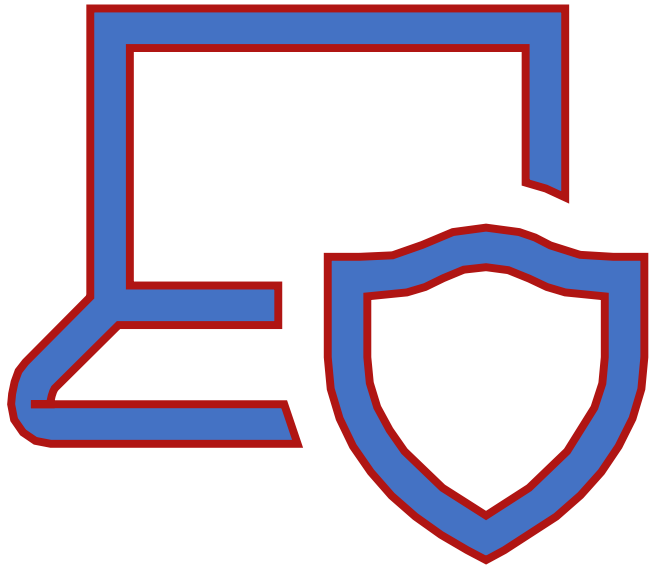
Compliance

System Audit

Control

…

…



Types of System Audits

Information System Audit (Financial)

Information System Audit (Security)

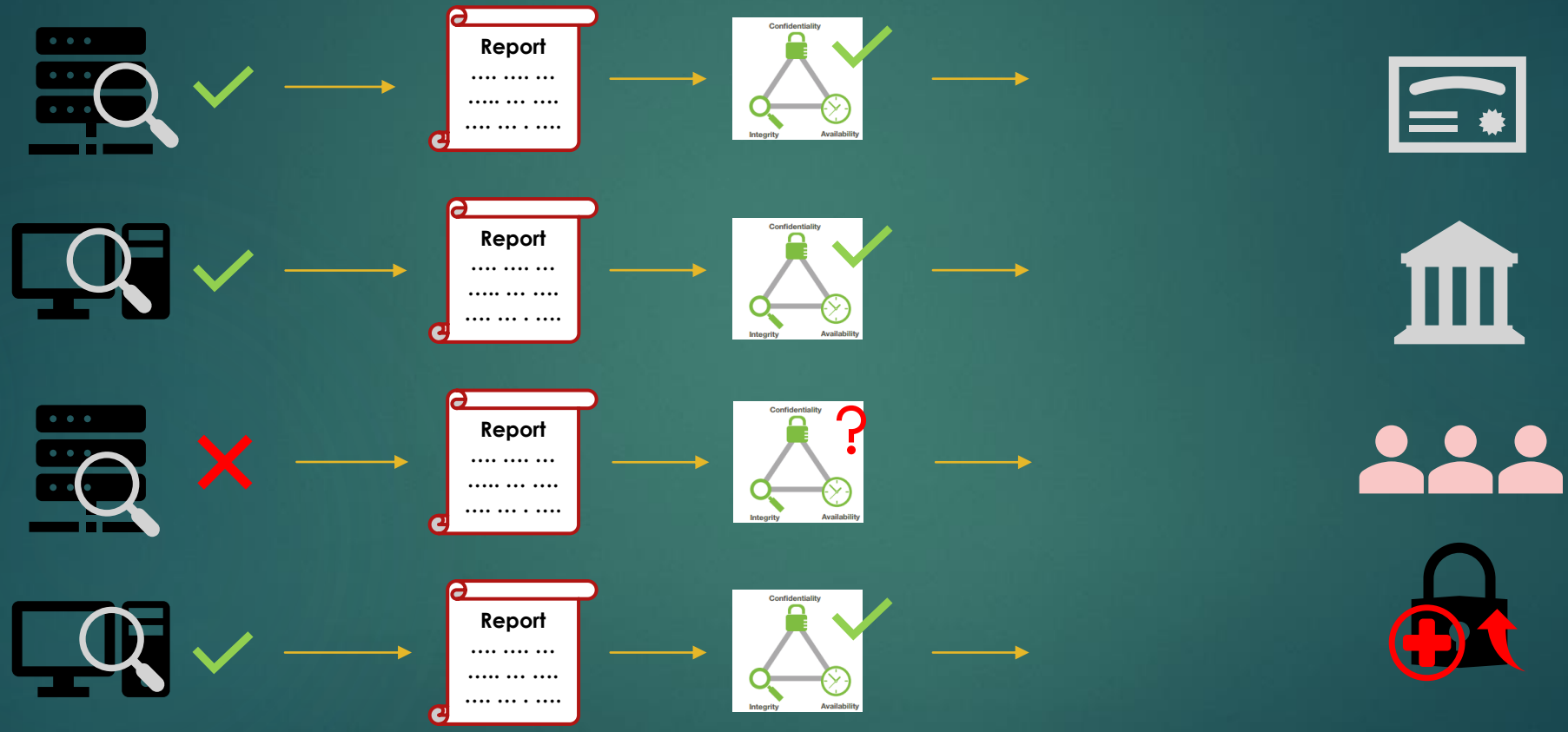
External Auditor

Internal Auditor

Self-Auditing

Information System Audit (Financial)

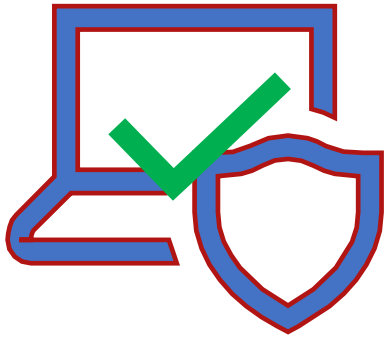
Information System Audit (Security)

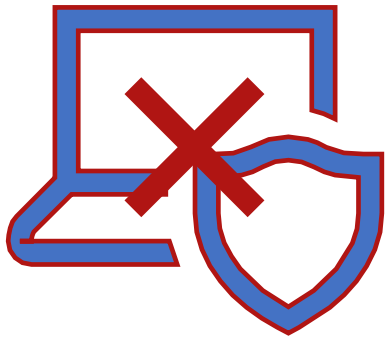


Audit & Audit statements

- Audit statements is an easy way to ensure customers about the security level
- External/Internal Auditors are independent
- Audits might set focus on things that would otherwise have a low priority
- ”Another pair of eyes”

The 3 Lines of Defense

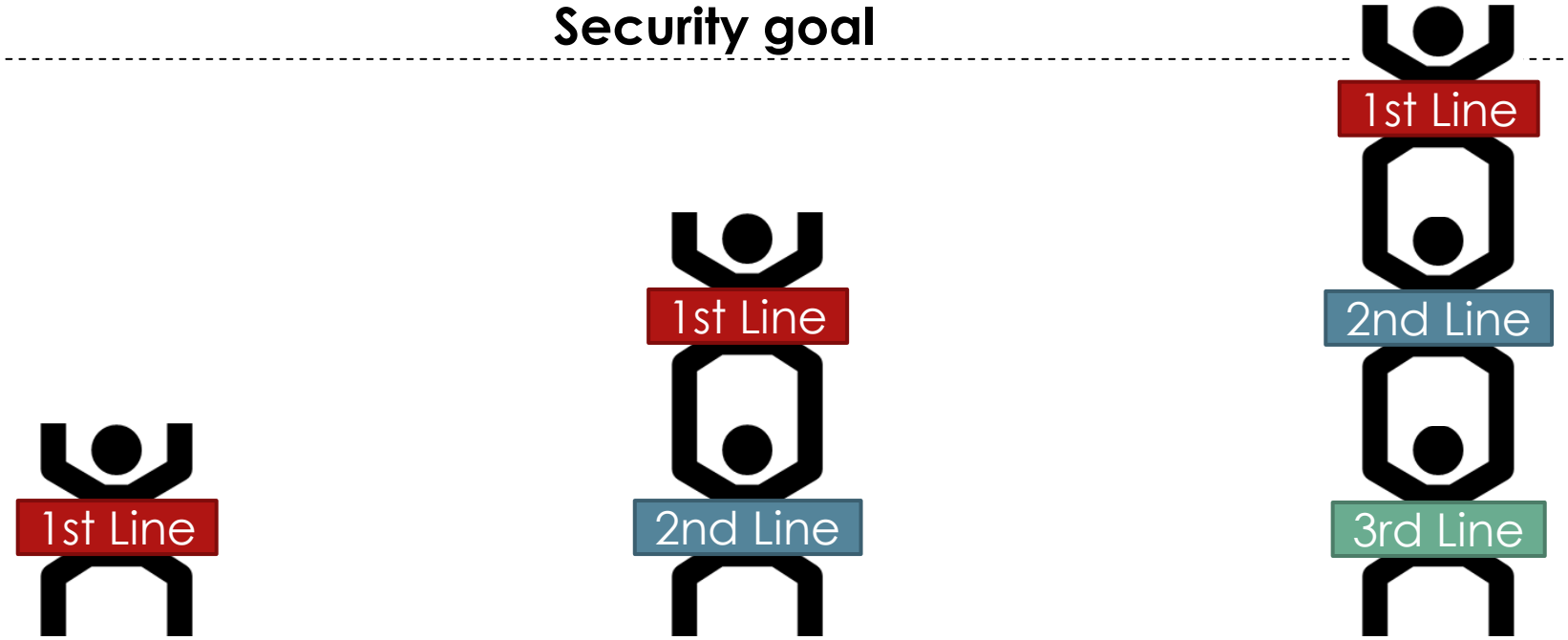




Source: IIA

3 Lines of Defense

Security goal



1 Line of Defense

2 Lines of Defense

3 Lines of Defense

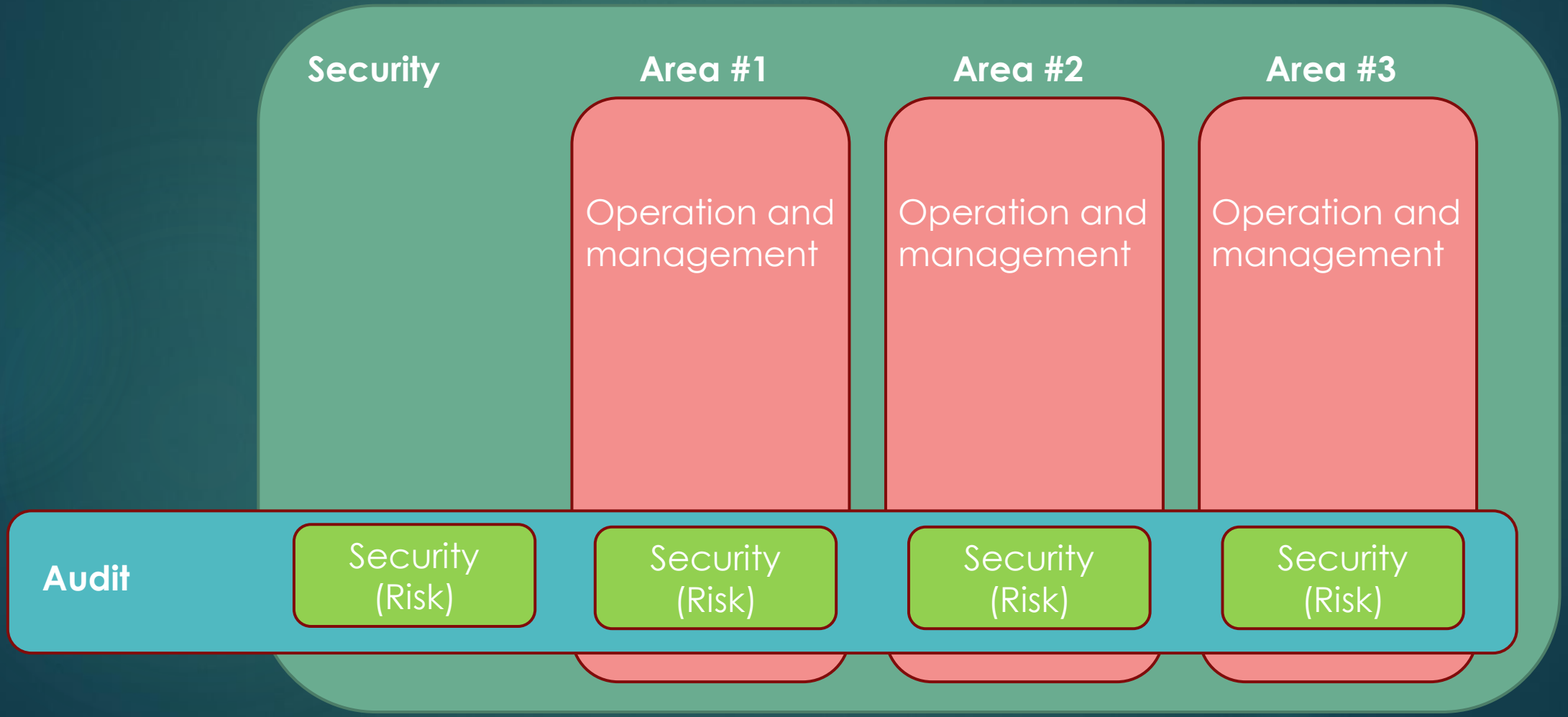
System audit as a Task (Self-audit)

A part of management

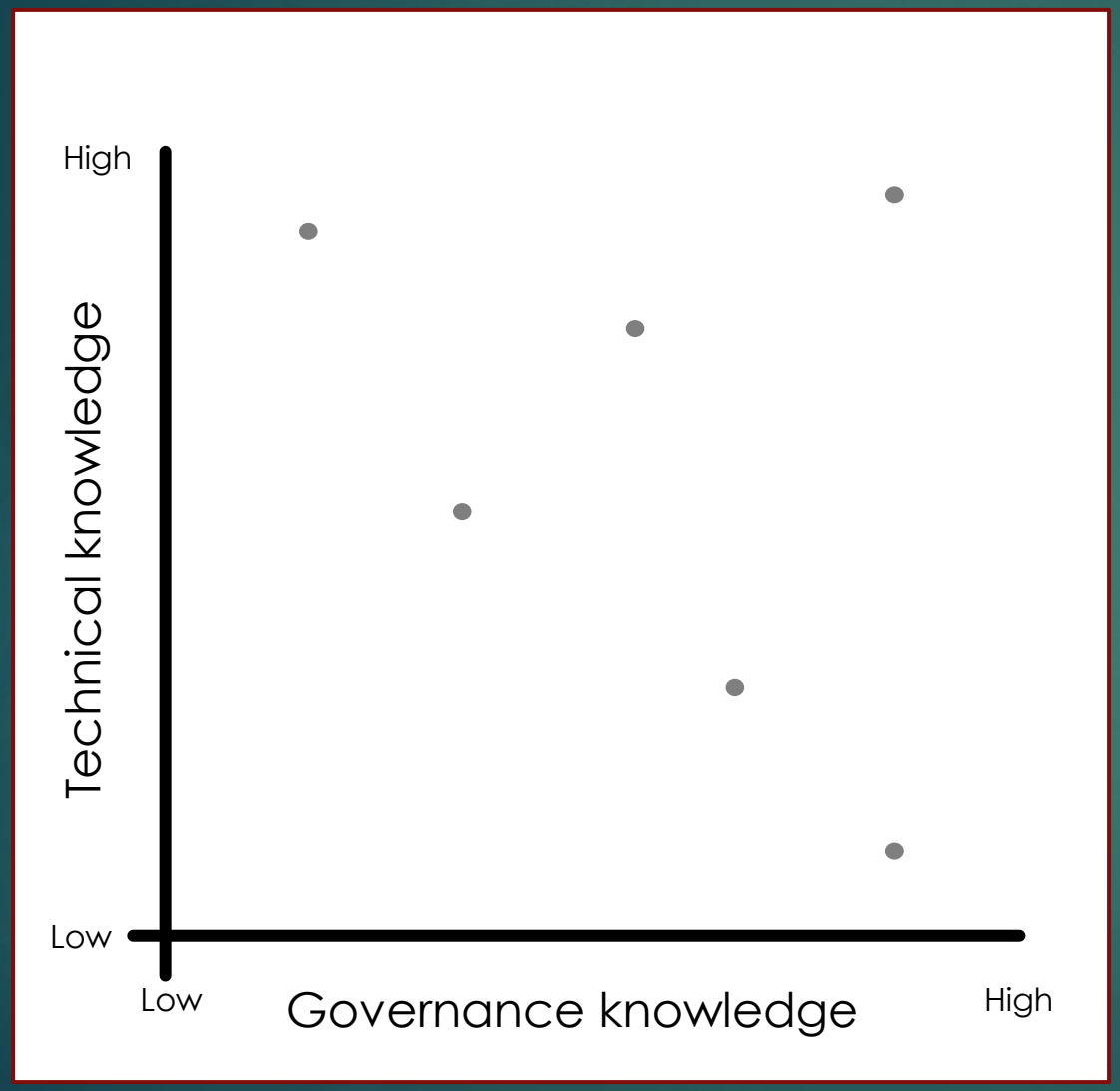
Baseline scans

Best practices

Extra focus on security!



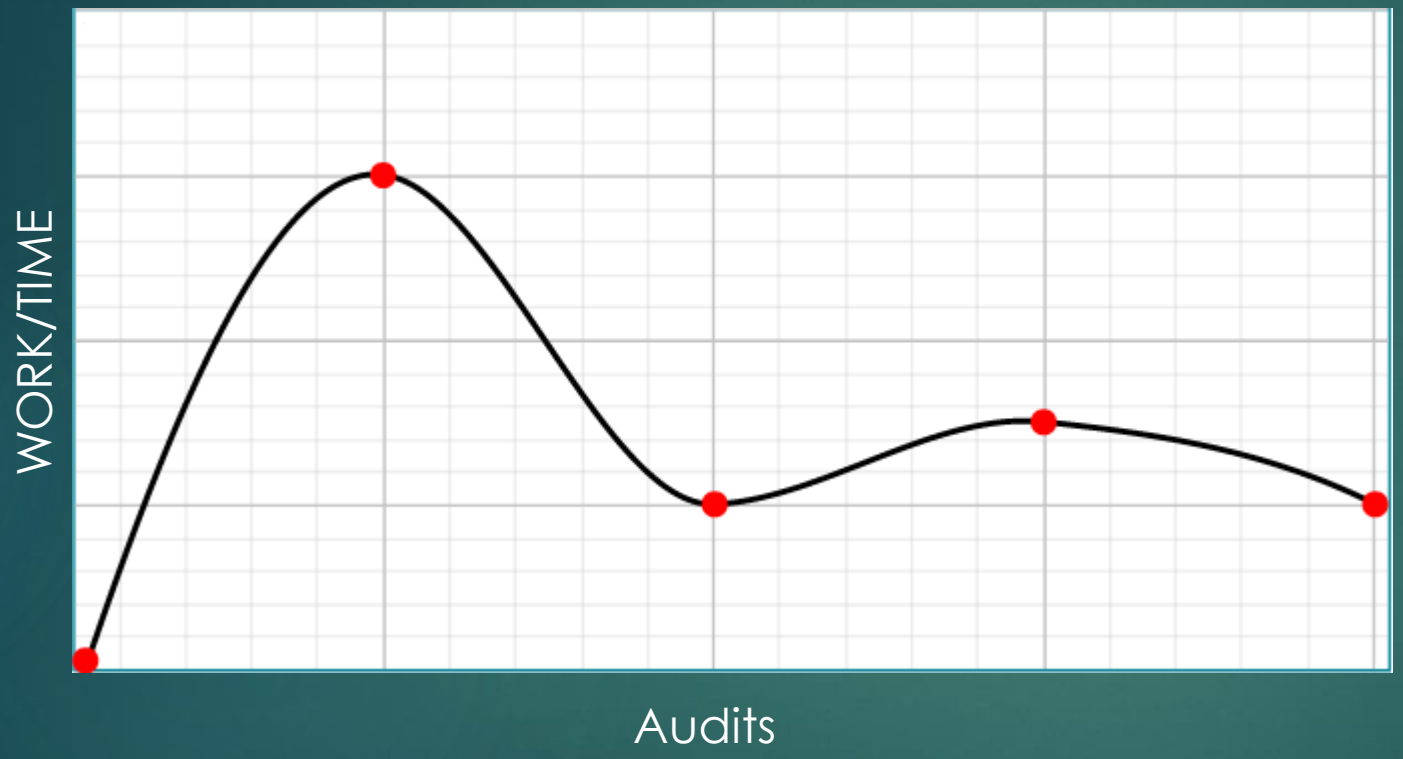
Learn by doing



CISA® Certified Information Systems Auditor®
An ISACA® Certification

"CISA candidates must have a minimum of five years of professional experience in information systems auditing, control, or security"

The audits



The gain?

IT controls

"specific activities performed by persons or systems designed to ensure that business objectives are met"

IT general controls

IT application controls

Standards and Frameworks

	ISO 27001	CIS Controls™	NIST CYBERSECURITY FRAMEWORK
Controls:	114	121	98

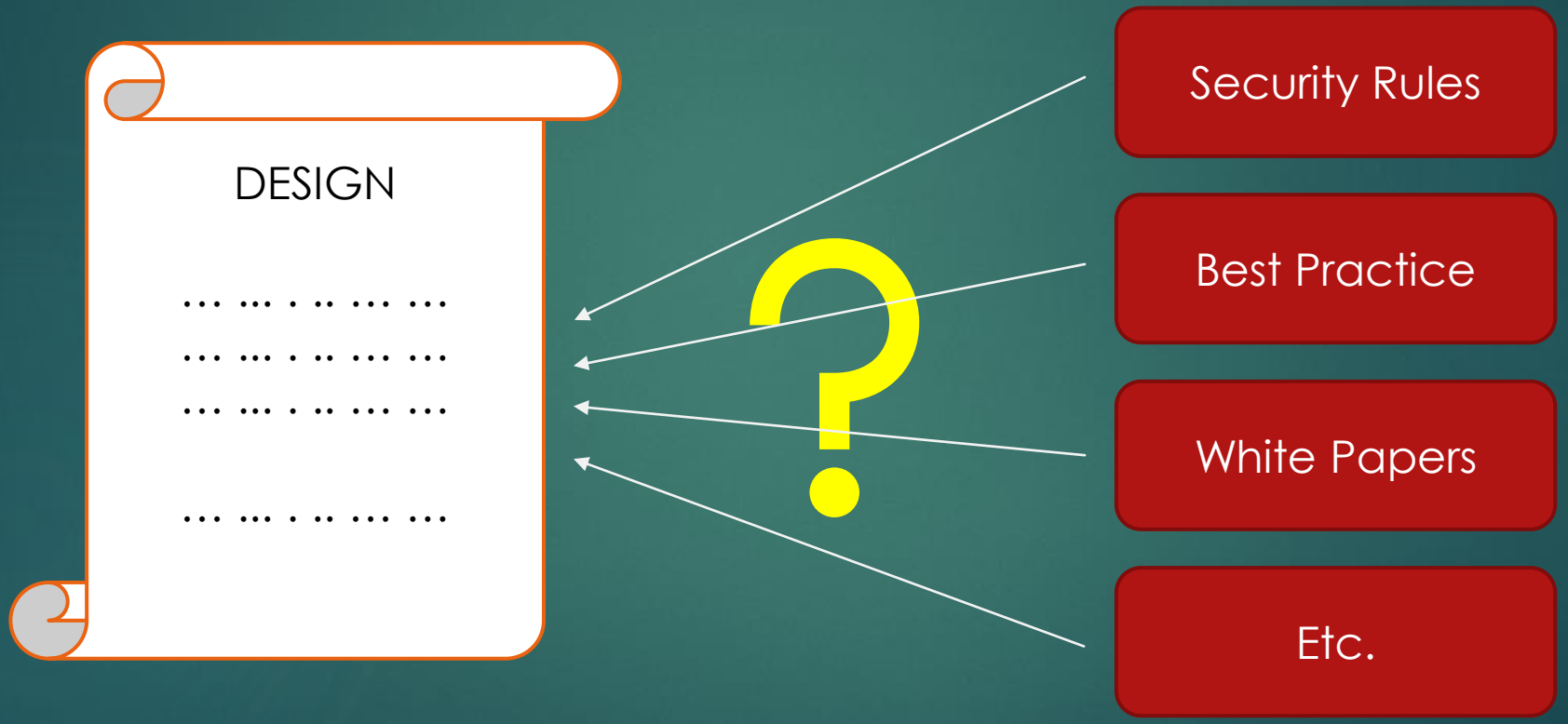

How's the new CISO job?
CFO got phished.
Budget got cut in half after COVID.
Marketing launched new website without informing me and got hacked.
But, we passed the security audit!
Balbix

MEME TIME!!!!

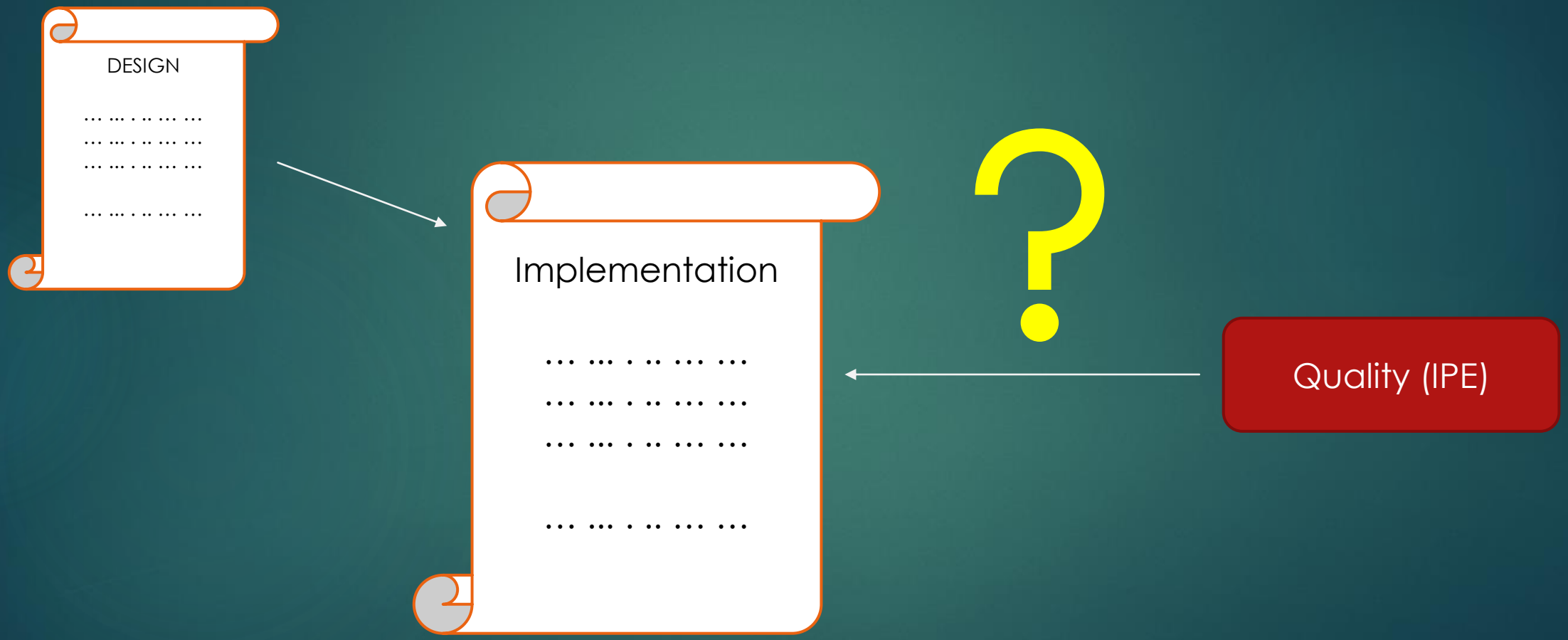
Basic Auditing

- **Testing controls:**
  - Design
  - Implementation
  - Operational Efficiency

Testing controls - Design



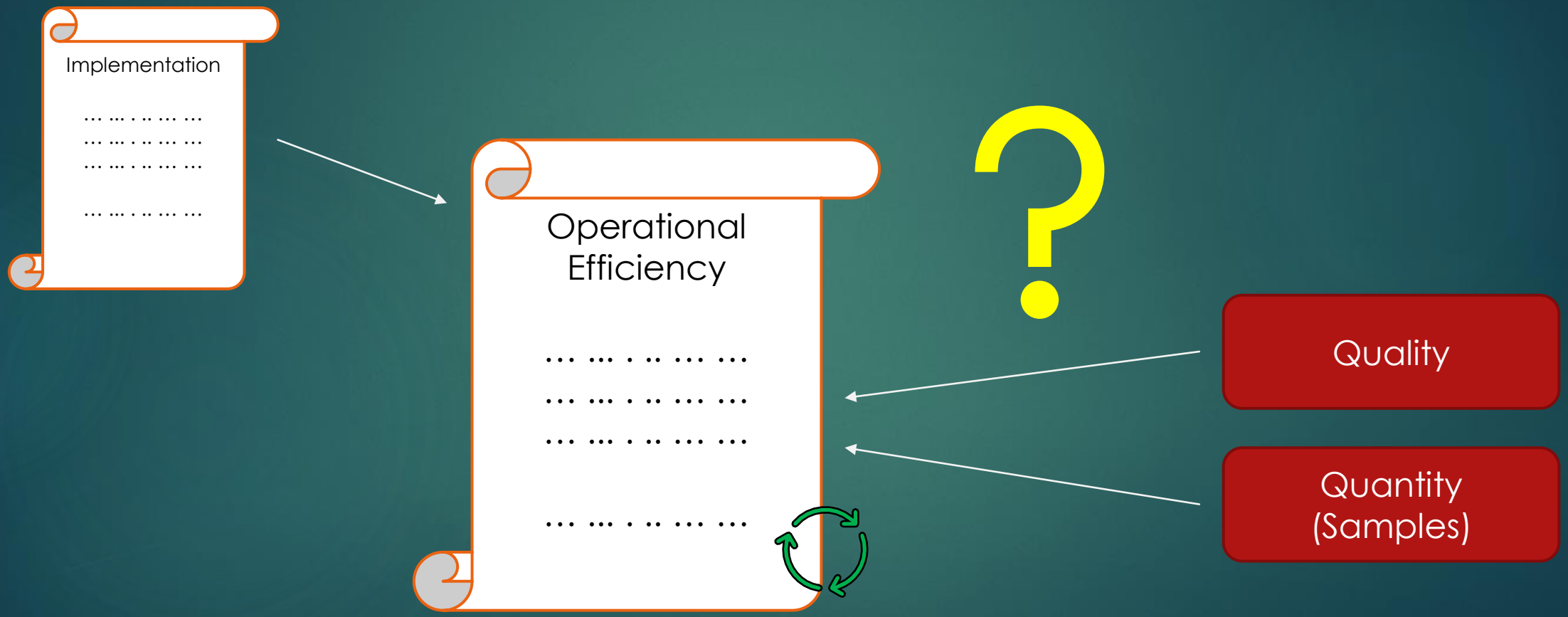
Testing controls - Implementation



Information provided/ produced by the entity (IPE)

- Source Data – where does it come from
- Report Logic – how is it constructed
- Report Parameters – only relevant informations
- Accuracy – is data correct
- Completeness – is all data considered

Testing controls - Operational Efficiency



Control example

```
kenneth@kali:~$ cat controls.log
Machine01 - Setting=Setting01
Machine02 - Setting=Setting01
Machine03 - Setting=Setting02
Machine04 - Setting=Setting01
Machine05 - Setting=Setting02
.......
.......
kenneth@kali:~$
```

```
kenneth@kali:~$ grep "Setting03" controls.log
kenneth@kali:~$
```

```
kenneth@kali:~$ grep "Setting02" controls.log
Machine03 - Setting=Setting02
Machine05 - Setting=Setting02
kenneth@kali:~$
```

```
kenneth@kali:~$ grep "setting02" controls.log
kenneth@kali:~$
```

```
kenneth@kali:~$ grep -i "setting02" controls.log
Machine03 - Setting=Setting02
Machine05 - Setting=Setting02
kenneth@kali:~$
```

```
kenneth@kali:~$ wc -l controls.log && grep -i "setting02" controls.log
7 controls.log
Machine03 - Setting=Setting02
Machine05 - Setting=Setting02
kenneth@kali:~$
```

Think out of the box

Think like a Product/Application Owner - Productivity

Think like a Security Manager - Security

Think like a Hacker - Exploits

Think like an Auditor - Risks

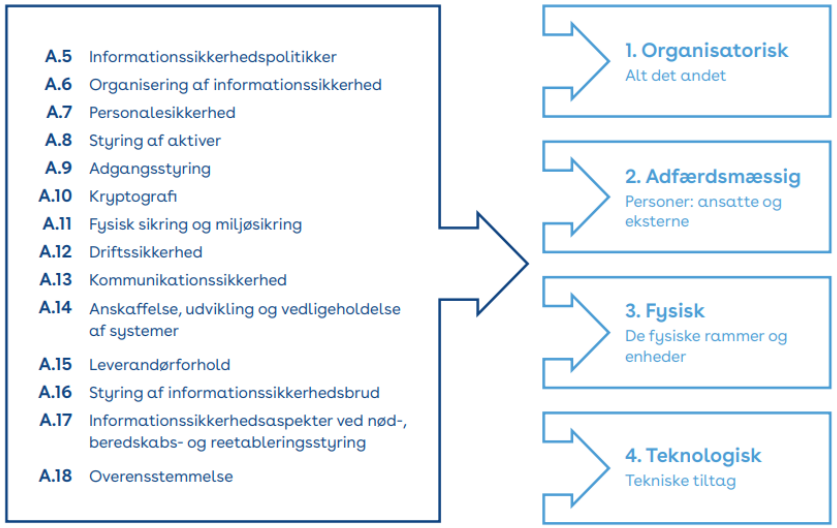
Gain insight / change area

So…

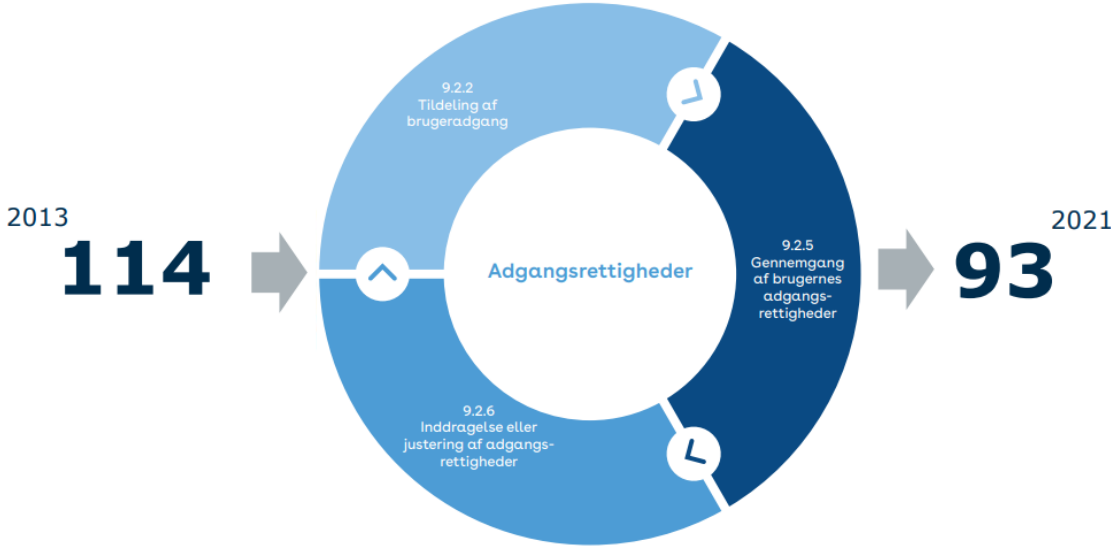
Helping or disrupting?

New ISO/IEC 27002:2021 (1/2)

14 areas → 4 areas



Figur 1: Fra 14 kapitler i ISO/IEC 27002:2012 til 4 kapitaler i ISO/IEC 27002:2021[7].



Figur 2: Eksempel på hvordan tre foranstaltninger sammenlægges til én i ISO/IEC 27002:2021.

New ISO/IEC 27002:2021 (2/2)

Adfærdsmæssig	Fysisk Physical security monitoring
Organisatorisk Threat intelligence Information security for use of cloud services ICT readiness for business continuity	**Teknologisk** Configuration management Information deletion Data masking Data leakage prevention Monitoring activities Web filtering Secure coding

Figur 3: Illustration af de nye foranstaltninger indplaceret i deres tilhørende tema.

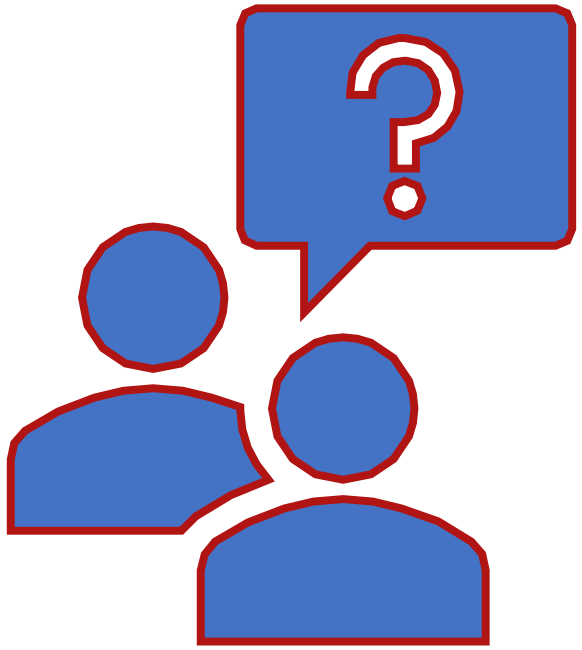
Type af foranstaltning (Se 4.1)	Egenskaber for informations-sikkerhed (Se 4.2)	Cyber-sikkerheds-koncept (Se 4.3)	Operationelle ressourcer (Se 4.4)	Sikkerheds-domæne (Se 4.5)
#Forebyggende	#Fortrolighed #Integritet	#Protect	#Secure_ configuration	#properties

Figur 4: Eksempel på anvendelsen af attributter som inddeling på foranstaltningen Use of Cryptography.

(NIST Cyber Security Framework)

Questions?

Time for questions




And now for something completely different!!!

Who's using the binaries?!?!

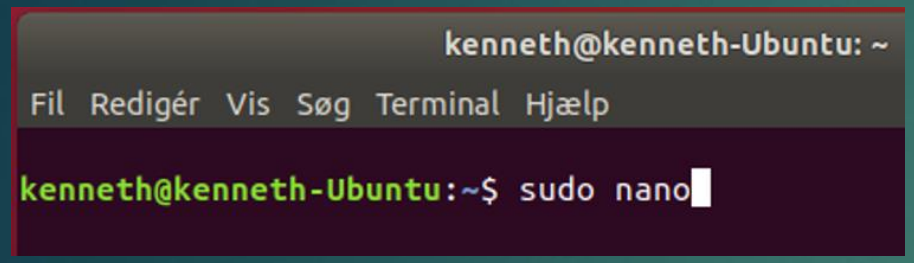
sudo

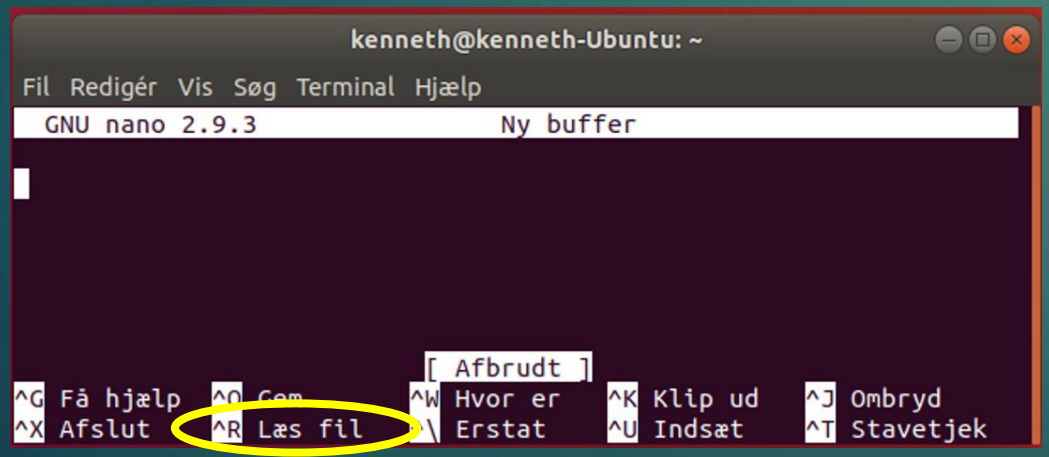
```
$ sudo -l
```

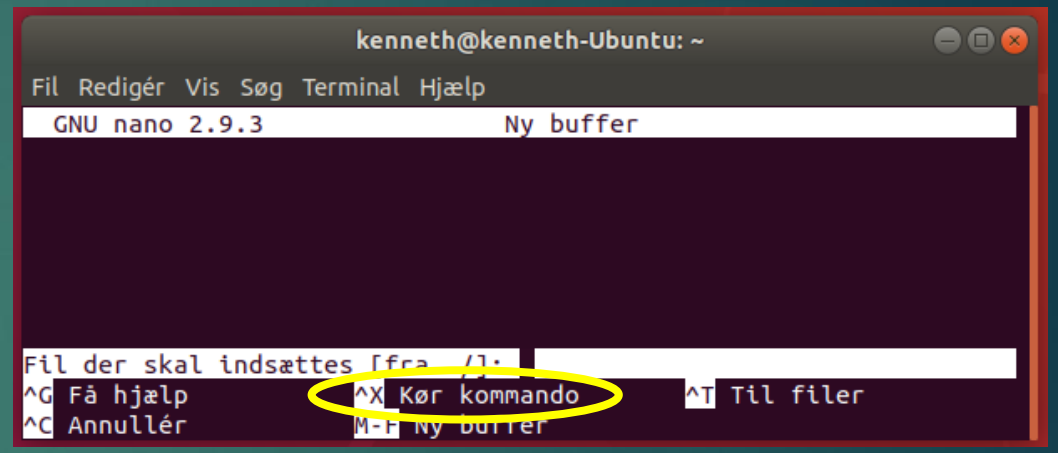
SUID

```
$ find / -type f -perm -4000 -user root 2>/dev/null
```

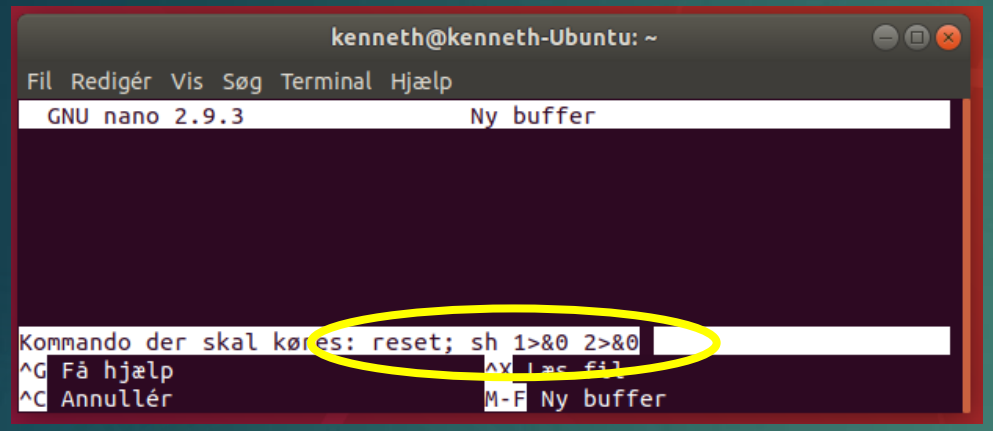
GTFO Bin – POC (1/2)





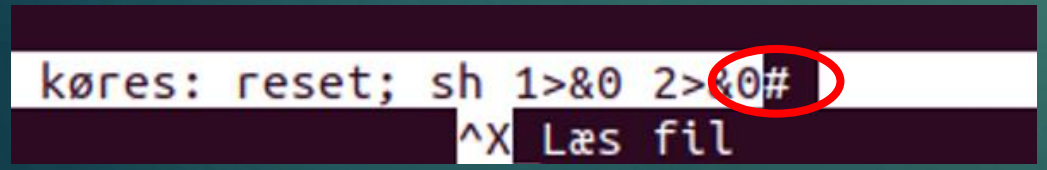


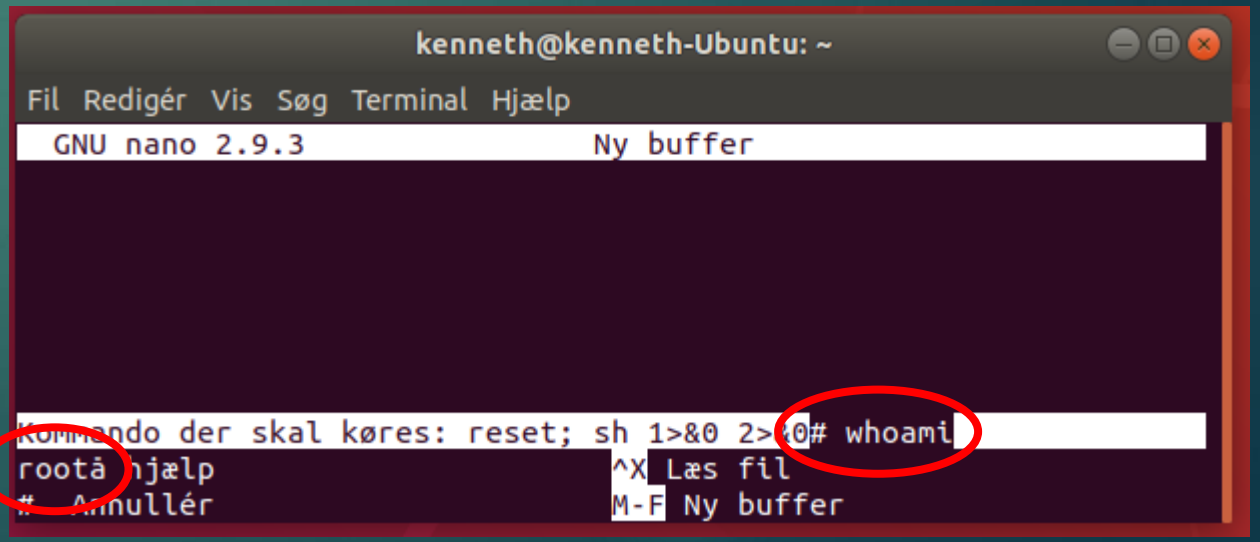
GTFO Bin – POC (2/2)



And the quick way…

```
kenneth@kenneth-Ubuntu:~$ sudo find /bin -name nano -exec /bin/sh \;
[sudo] adgangskode for kenneth:
# whoami
root
#
```





Securing and monitoring binaries

Securing

```
$ sudo nano /etc/sudoers
```

```
$ find / -type f -perm -4000 -user root 2>/dev/null
```

Monitoring