GRC be connected

Measuring Security Success: Unveiling the KPIs of Protection

Mrs. Olga Ghincul

EY Financial services

ORGANIZED BY

CYBER SECURITY COALITION.be

ISACA Belgium Chapter

CGEIT CISA CISM CRISC CSX-P COBIT

SUPPORTED BY

Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT

Measuring Security Success: Unveiling the KPIs of Protection

Olga Ghincul, Senior Manager, EY

olga.ghincul@be.ey.com

Angel

EY
Building a better working world

Angel

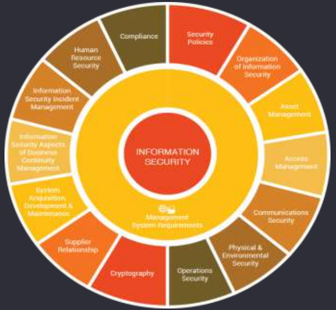
EY
Building a better working world

Angel
DOUGLAS W. HUBBARD & RICHARD SEIERSEN
HOW TO MEASURE ANYTHING IN CYBERSECU
RISK
Forewords by DANIEL E. GEER, J & STUART MCCLU
PRAGMATIC Security Metrics
Applying Metametrics to Information Security
W. Krag Brotby and Gary Hinson
Preface by M. E. Kabay, PhD, CISSP-ISSMP
CRC Press
AN AUERBACH BOOK
MEASURING AND MANAGING FORMATION RISK
A FAIR Approach
nd | Jack Jones
BH

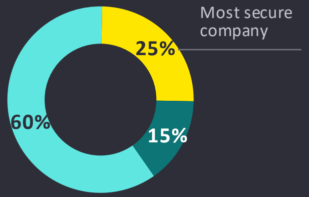
The Security Dashboard

The Security Dashboard

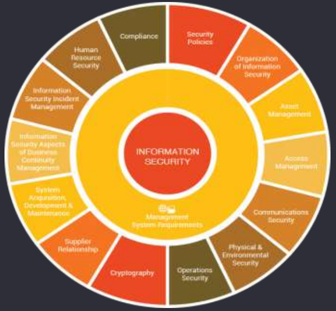
ISO 27001 maturity score


Compliance
Security Policies
Organization of Information Security
Asset Management
Access Management
Communications Security
Physical & Environmental Security
Operations Security
Cryptography
Supplier Relationship
System Acquisition, Development & Maintenance
Information Security Aspects of Business Continuity Management
Information Security Incident Management
Human Resource Security
INFORMATION SECURITY
Management System Requirements

Group targets for information security

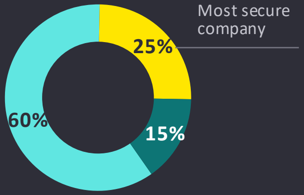


ISO 27001 maturity score

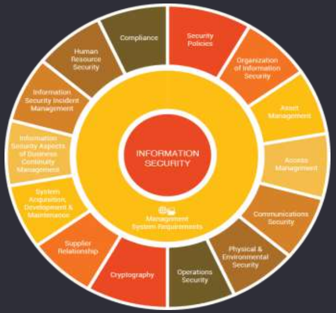

INFORMATION SECURITY
Management System Requirements
Security Policies
Organization of Information Security
Asset Management
Access Management
Communications Security
Physical & Environmental Security
Operations Security
Cryptography
Supplier Relationship
System Acquisition, Development & Maintenance
Information Security Aspects of Business Continuity Management
Information Security Incident Management
Human Resource Security
Compliance

The Security Dashboard

Group targets for information security

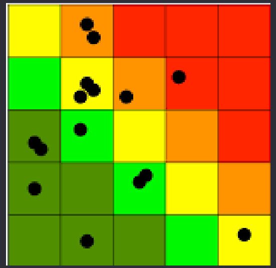


ISO 27001 maturity score


Compliance
Security Policies
Organization of Information Security
Asset Management
Access Management
Communications Security
Physical & Environmental Security
Operations Security
Cryptography
Supplier Relationship
System Acquisition, Development & Maintenance
Information Security Aspects of Business Continuity Management
Information Security Incident Management
Human Resource Security
INFORMATION SECURITY
Management System Requirements

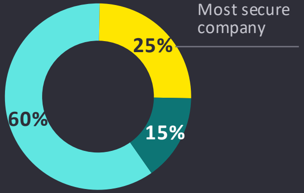
The Security Dashboard

Top security risks treatment status

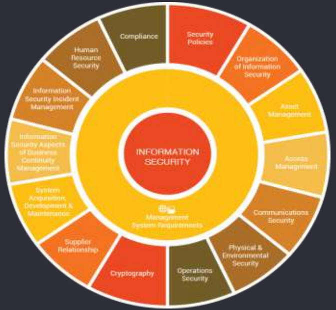


The Security Dashboard

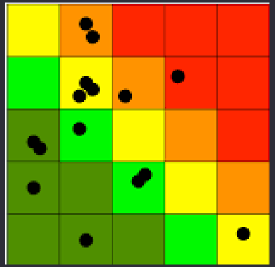
Group targets for information security



ISO 27001 maturity score


Compliance
Security Policies
Organization of Information Security
Asset Management
Access Management
Communications Security
Physical & Environmental Security
Operations Security
Cryptography
Supplier Relationship
System Acquisition, Development & Maintenance
Information Security Aspects of Business Continuity Management
Information Security Incident Management
Human Resource Security
INFORMATION SECURITY
Management System Requirements

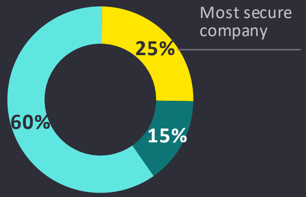
Top security risks treatment status



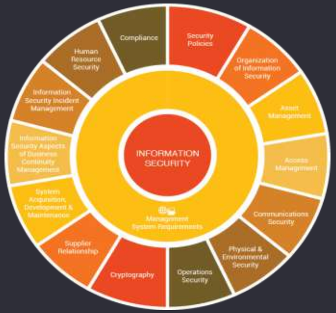
Baseline security controls implementation

Security Baseline controls	Q1	Q2	Q3
	42%	**63%**	**92%**

Group targets for information security

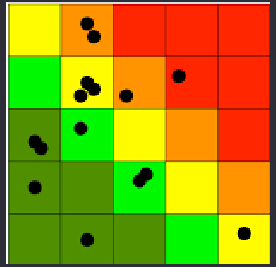


ISO 27001 maturity score

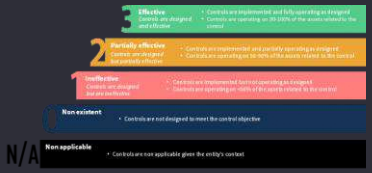

INFORMATION SECURITY
Management System Requirements
Security Policies
Organization of Information Security
Asset Management
Access Management
Communications Security
Physical & Environmental Security
Operations Security
Cryptography
Supplier Relationship
System Acquisition, Development & Maintenance
Information Security Aspects of Business Continuity Management
Information Security Incident Management
Human Resource Security
Compliance

The Security Dashboard

Top security risks treatment status



Security control effectiveness



3 **Effective**
Controls are designed and effective
- Controls are implemented and fully operating as designed
- Controls are operating on 90-100% of the assets related to the control

2 **Partially effective**
Controls are designed but partially effective
- Controls are implemented and partially operating as designed
- Controls are operating on 50-90% of the assets related to the control

1 **Ineffective**
Controls are designed but are ineffective
- Controls are implemented but not operating as designed
- Controls are operating on <50% of the assets related to the control

0 **Non existent**
- Controls are not designed to meet the control objective

N/A **Non applicable**
- Controls are non applicable given the entity's context

Baseline security controls implementation

Security Baseline controls	Q1	Q2	Q3
	42%	63%	92%

Illustration by Open AI: DALLE

“I need **one** security KPI...”

Replacing fear, uncertainty and doubt

https://commons.wikimedia.org/wiki/File:1596_America_Sive_India_Nova.jpg

Illustration by Open AI: DALLE

The Cobra effect

Domesticating information security risk

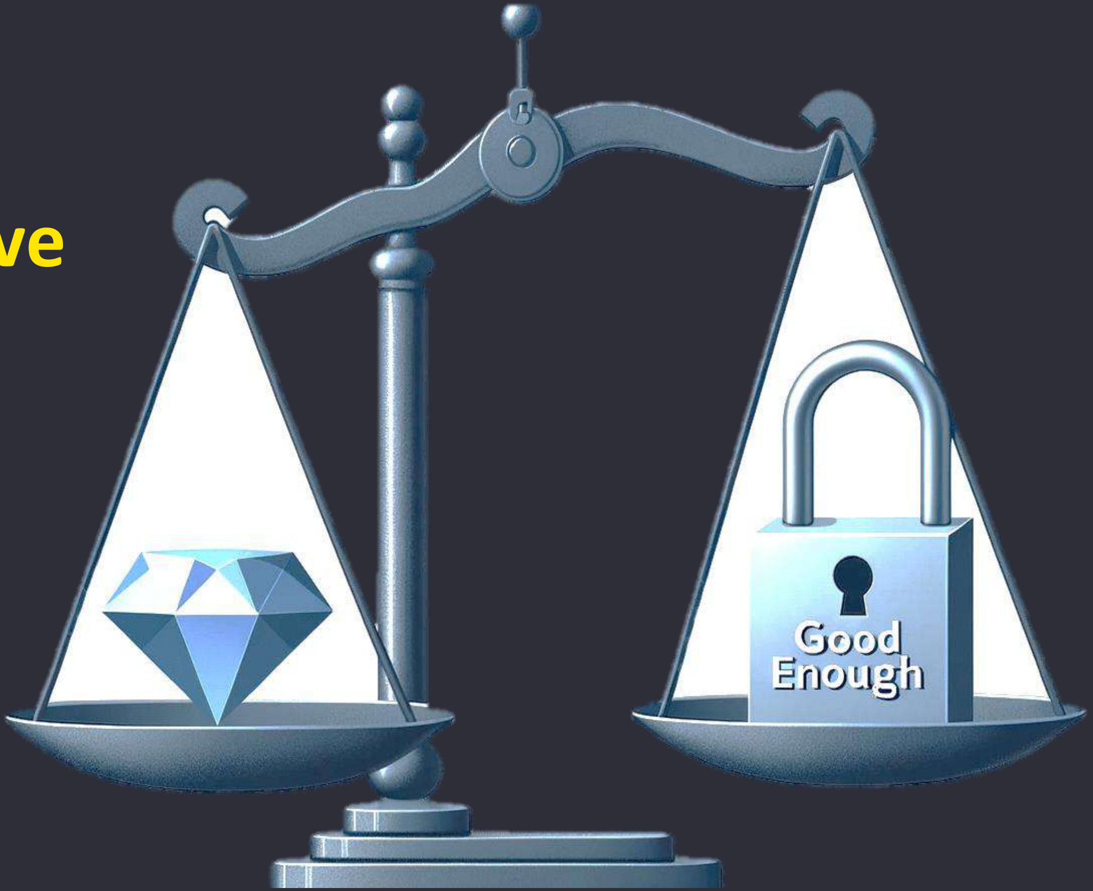
Illustration by Open AI: DALLE

Be careful what to report to management

Illustration by Open AI: DALLE

Illustration by Open AI: DALLE

Striving for perfection can be counterproductive



objective actionable

measurable comparable

achievable

timely **reliable** consistent

understandable quantifiable

efficient **effective**

relevant

objective actionable

measurable comparable

achievable

timely **reliable** consistent

understandable quantifiable

efficient **effective**

relevant

- ✓ **Support effective decision making**
- ✓ **Decrease uncertainly**
- ✓ **Highlight issues that matter**

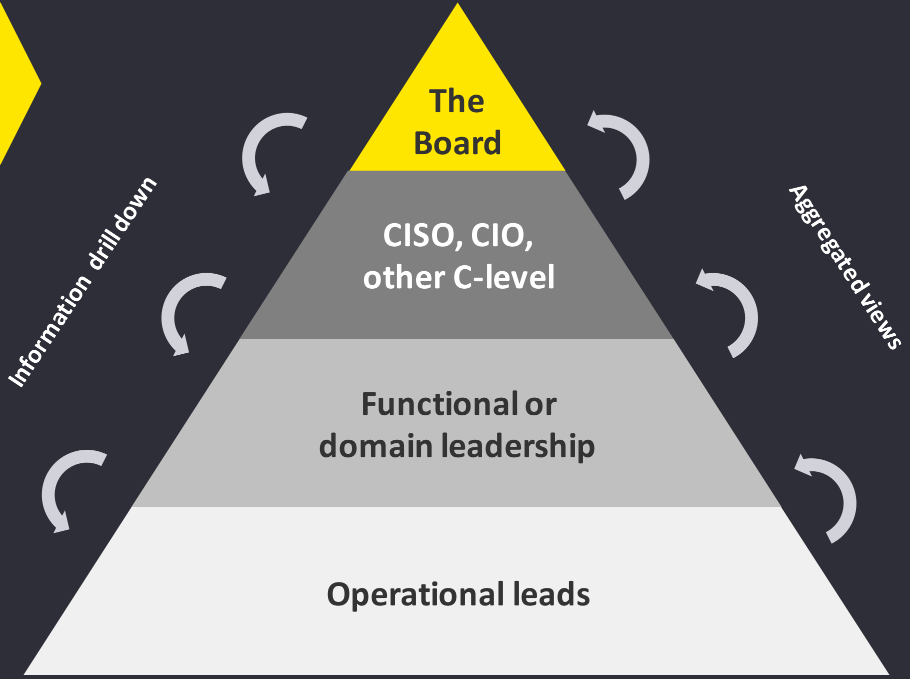
Change the message for your audience

- Critical incidents
- Risk posture/trend
- Spend status/ROI
- Compliance

- Portfolio status/health
- Organizational health (e.g., budget, headcount)

- Control health (e.g., patching, malware protection)
- Mapping to controls (e.g., NIST, ISO)
- Project status/health

- Operational risk (e.g., incidents, threats, vulnerabilities)
- Activities status



Top down approach to select metrics

Strategic

Risk, Threats, Investments

Tactical

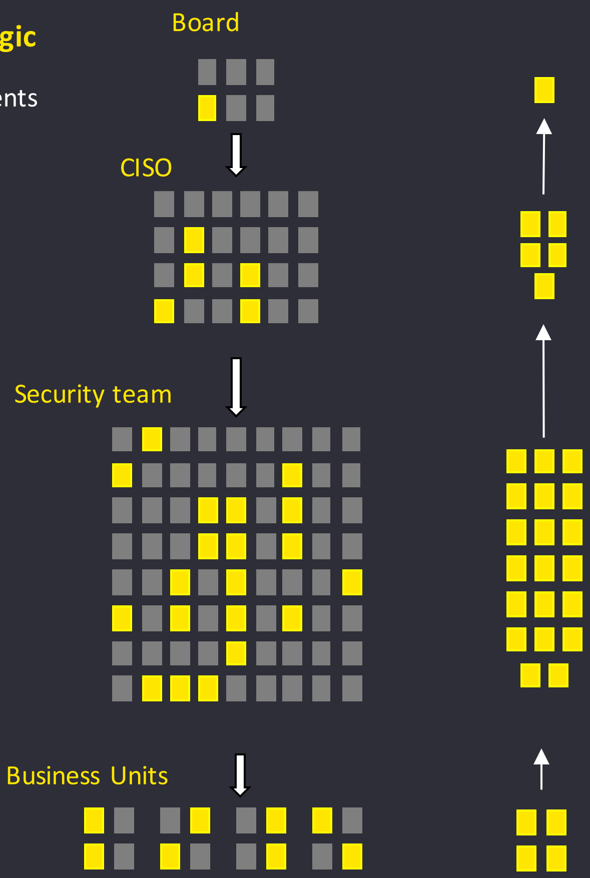
Risk, Threats, Investments, Program Activity/Progress

Tactical

Program Activity/Progress, Tactical Level Decisions

Operational

Program level decision making



To answer the board's question, I need the following metrics

I can use these 5 metrics I am tracking which are supported by the 20 operational level metrics

My operational framework includes essential metrics, of which 20 are tailored to address the inquiries of the CISO and Board

To support my operational area I need to collect a set of required metrics and a few additional metrics for consolidation above

What is board really interested in?

Revenue

Revenue

Cost

Illustration by Open AI: DALLE

What is board really interested in?

Revenue

Cost

Risk

Illustration by Open AI: DALLE

Illustration by Open AI: DALLE

Executives are advised to…

- ✓ **Target level 5 maturity**
- ✓ **Spend x% of revenue on security**
- ✓ **Be accountable for incidents**
- ✓ **Use benchmarks**
- ✓ **Follow a checklist**

Executives are advised to…

- ✓ Target level 5 maturity
- ✓ Spend x% of revenue on security
- ✓ Be accountable for incidents
- ✓ Use benchmarks
- ✓ Follow a checklist

We advise CISOs to ask…

- ✓ What is the board's background?
- ✓ What role do they serve on the board?
- ✓ Is there a cybersecurity expert in the board?
- ✓ What are their biases?
- ✓ What are their passions?

Once upon a time...

Illustration by Open AI: DALLE

Security can be simple

Illustration by Open AI: DALLE

Focus on your critical assets (errors in configuration, software)

Focus on people that use your critical assets

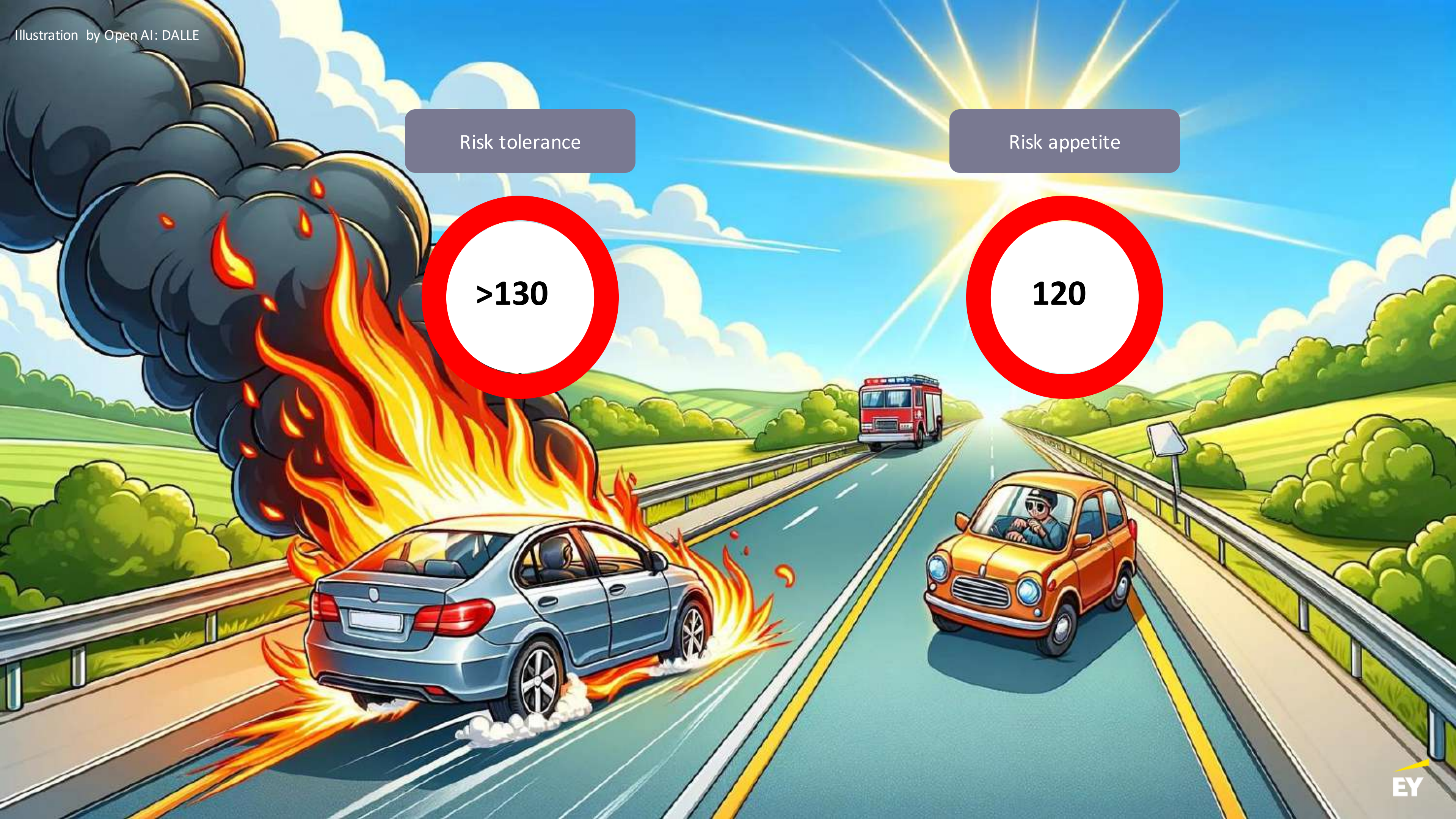
Focus on credentials that control systems

Illustration by Open AI: DALLE

Why security controls matter

Balanced security controls

Illustration by Open AI: DALLE



Risk tolerance

>130

Risk appetite

120

Illustration by Open AI: DALLE

NIST CSF – a management-friendly framework

Illustration by Open AI: DALLE

The measurement cycle

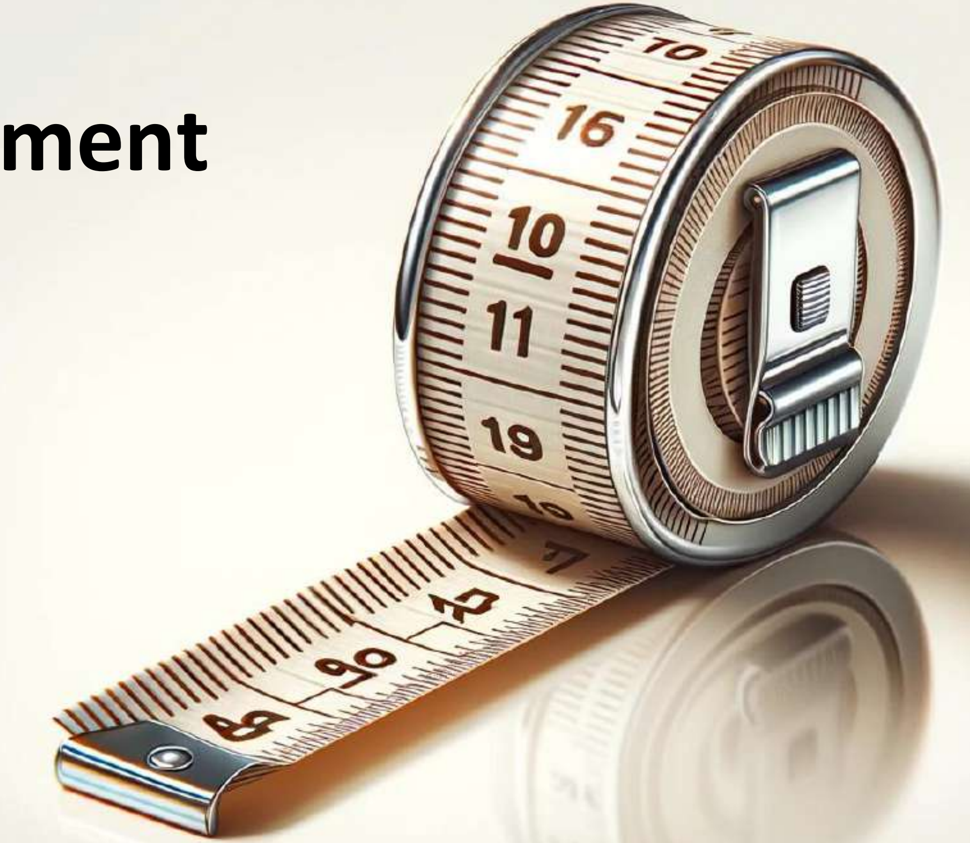
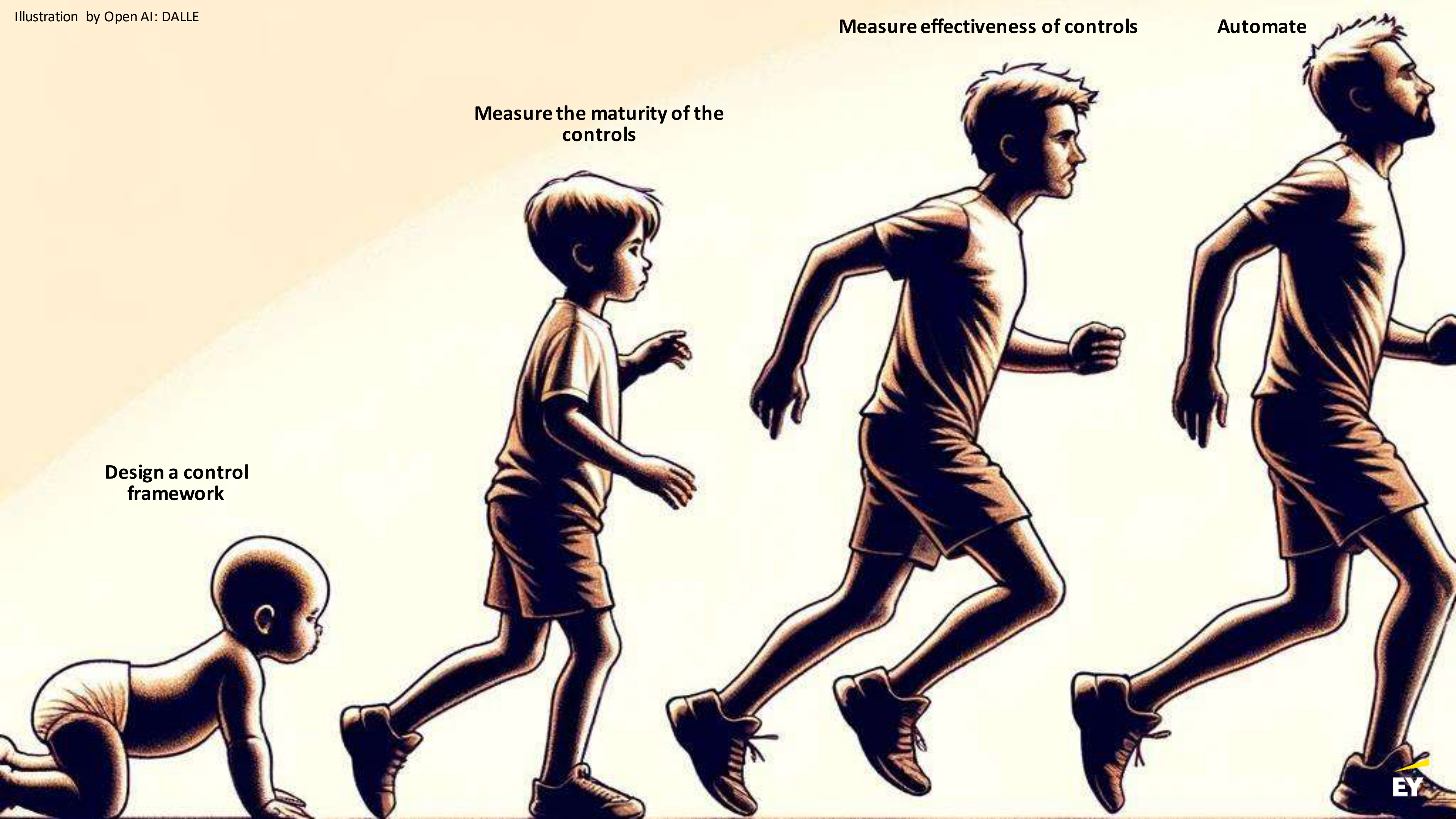


Illustration by Open AI: DALLE



Design a control framework

Measure the maturity of the controls

Measure effectiveness of controls

Automate

The measurement cycle

1. Define

- Metric Owner
- Data Owner
- Description
- Assumptions
- Calculation
- Data Sources
- Thresholds
- Frequency
- Status

2. Collect

- Iterative process
- Continual improvements
- A set framework
- Methodology

3. Validate

- Clear steps to validate
- Responsibility of the collector, initially
- Over time, moves to metric and data owner
- Brings confidence level of the data collected

4. Manage

- Begin with manual collection and analysis
- Gradually moving towards automation
- Not take resources away from their main tasks

Building the metrics story

1 Threat actors and threats

- Top 5 threats
- Top 5 threat actors

2 Assets and business at risk

- Top 5 Crown Jewels aligned with business
- Financial value and value at risk

3 Security posture

- Health
- Effectiveness
- Defensibility
- Recoverability
- External security ratings

4 Top risk scenarios

- Risk scenarios
- Risk exposure

5 Ongoing risk reduction efforts

- Ongoing Initiatives
- Risk reduction value

6 Recommended risk reduction efforts

- Recommended initiative
- Initiative cost
- Initiative risk reduction value
- Initiative return on security investment

Building the metrics story

1 Threat actors & threats

The company is in the news, threat actors are highly motivated and well financed

- ATP1
- Lazarus
- Cobalt

- Ransomware
- Spear phishing
- Supply chain attacks

Building the metrics story

1

Threat actors & threats

The company is in the news, threat actors are highly motivated and well financed

- ATP1
- Lazarus
- Cobalt

- Ransomware
- Spear phishing
- Supply chain attacks

2

Assets & business at risk

Loss amount is based on productivity, response, replacement, fines, reputation loss

PII Data	IP	E-commerce	Data centers	Applications
€500 m	€150 m	€200 m	€300 m	€600 m

Building the metrics story

1 Threat actors & threats

The company is in the news, threat actors are highly motivated and well financed

- ATP1
- Lazarus
- Cobalt

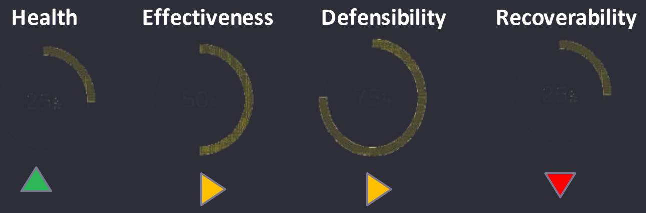
- Ransomware
- Spear phishing
- Supply chain attacks

2 Assets & business at risk

Loss amount is based on productivity, response, replacement, fines, reputation loss

PII Data	IP	E-commerce	Data centers	Applications
€500 m	€150 m	€200 m	€300 m	€600 m

3a Security Posture (Metrics)



External monitoring score 725 ▲

Building the metrics story

1 Threat actors & threats

The company is in the news, threat actors are highly motivated and well financed

- ATP1
- Lazarus
- Cobalt

- Ransomware
- Spear phishing
- Supply chain attacks

2 Assets & business at risk

Loss amount is based on productivity, response, replacement, fines, reputation loss

PII Data	IP	E-commerce	Data centers	Applications
€500 m	€150 m	€200 m	€300 m	€600 m

3a Security Posture (Metrics)

Health	Effectiveness	Defensibility	Recoverability
▲	▶	▶	▼

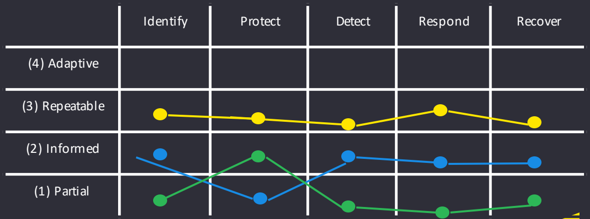
External monitoring score 725 ▲

3b Security Posture (Frameworks)

MITRE ATT&CK

	Initial access	Gain control	Lateral mov.	Data access	Data transf.
Coverage	25%	25%	25%	25%	25%
Tested	15%	15%	15%	15%	15%
Detection	65%	65%	65%	25%	25%

NIST CSF



EY

Building the metrics story

1 Threat actors & threats

The company is in the news, threat actors are highly motivated and well financed

- ATP1
- Lazarus
- Cobalt

- Ransomware
- Spear phishing
- Supply chain attacks

2 Assets & business at risk

Loss amount is based on productivity, response, replacement, fines, reputation loss

PII Data	IP	E-commerce	Data centers	Applications
€500 m	€150 m	€200 m	€300 m	€600 m

3a Security Posture (Metrics)

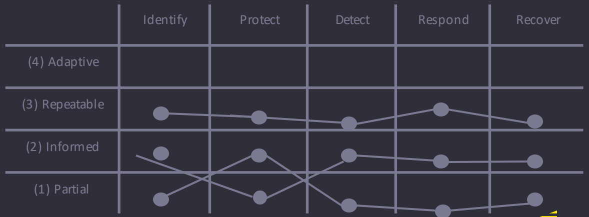
External monitoring score: 725 ▲

3b Security Posture (Frameworks)

MITRE ATT&CK

	Initial access	Gain control	Lateral mov.	Data access	Data transf.
Coverage	25%	25%	25%	25%	25%
Tested	15%	15%	15%	15%	15%
Detection	65%	65%	65%	25%	25%

NIST CSF



4 Top risk scenarios

	Exposure
Successful ransomware attack	€20M
Top executive spear phishing	€10M
IP stolen by internal employee	€5M
Account takeover due to critical vulnerability	€25M
Major disruption to a critical service caused by DDoS	€2M

Building the metrics story

1 Threat actors & threats

The company is in the news, threat actors are highly motivated and well financed

- ATP1
- Lazarus
- Cobalt

- Ransomware
- Spear phishing
- Supply chain attacks

2 Assets & business at risk

Loss amount is based on productivity, response, replacement, fines, reputation loss

PII Data	IP	E-commerce	Data centers	Applications
€500 m	€150 m	€200 m	€300 m	€600 m

3a Security Posture (Metrics)

Health	Effectiveness	Defensibility	Recoverability
▲	▶	▶	▼

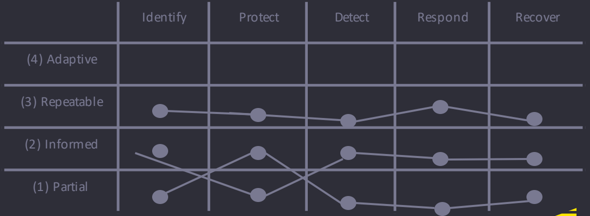
External monitoring score 725 ▲

3b Security Posture (Frameworks)

MITRE ATT&CK

	Initial access	Gain control	Lateral mov.	Data access	Data transf.
Coverage	25%	25%	25%	25%	25%
Tested	15%	15%	15%	15%	15%
Detection	65%	65%	65%	25%	25%

NIST CSF



4 Top risk scenarios

	Exposure
Successful ransomware attack	€20M
Top executive spear phishing	€10M
IP stolen by internal employee	€5M
Account takeover due to critical vulnerability	€25M
Major disruption to a critical service caused by DDoS	€2M

5 Ongoing risk reduction efforts

	Cost	Reduction	ROI
Revamp vulnerability management	€10M	€5M	50%
PII data inventory & protection	€5M	€5M	50%
Review firewall rules	€5M	€1M	25%

Building the metrics story

1 Threat actors & threats

The company is in the news, threat actors are highly motivated and well financed

- ATP1
- Lazarus
- Cobalt

- Ransomware
- Spear phishing
- Supply chain attacks

2 Assets & business at risk

Loss amount is based on productivity, response, replacement, fines, reputation loss

PII Data	IP	E-commerce	Data centers	Applications
€500 m	€150 m	€200 m	€300 m	€600 m

3a Security Posture (Metrics)

Health
Effectiveness
Defensibility
Recoverability

Health	Effectiveness	Defensibility	Recoverability
▲	▶	▶	▼

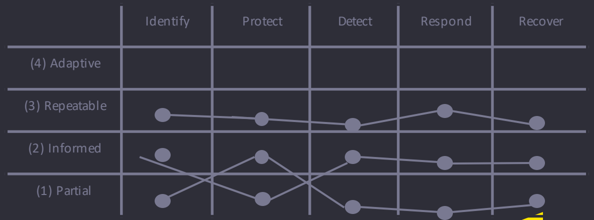
External monitoring score 725 ▲

3b Security Posture (Frameworks)

MITRE ATT&CK

	Initial access	Gain control	Lateral mov.	Data access	Data transf.
Coverage	25%	25%	25%	25%	25%
Tested	15%	15%	15%	15%	15%
Detection	65%	65%	65%	25%	25%

NIST CSF



4 Top risk scenarios

	Exposure
Successful ransomware attack	€20M
Top executive spear phishing	€10M
IP stolen by internal employee	€5M
Account takeover due to critical vulnerability	€25M
Major disruption to a critical service caused by DDoS	€2M

5 Ongoing risk reduction efforts

	Cost	Reduction	ROI
Revamp vulnerability management	€10M	€5M	50%
PII data inventory & protection	€5M	€5M	50%
Review firewall rules	€5M	€1M	25%

6 Recommended risk reduction efforts

Recommendation	Cost	Risk reduction	ROI
Xyz tool for DLP protection	€1M	€5M	15%
Purchase cyber insurance	€2M	€100M	55%

Building the metrics story

1 Threat actors & threats

The company is in the news, threat actors are highly motivated and well financed

- ATP1
- Lazarus
- Cobalt

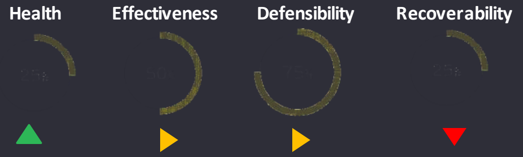
- Ransomware
- Spear phishing
- Supply chain attacks

2 Assets & business at risk

Loss amount is based on productivity, response, replacement, fines, reputation loss

PII Data	IP	E-commerce	Data centers	Applications
€500 m	€150 m	€200 m	€300 m	€600 m

3a Security Posture (Metrics)



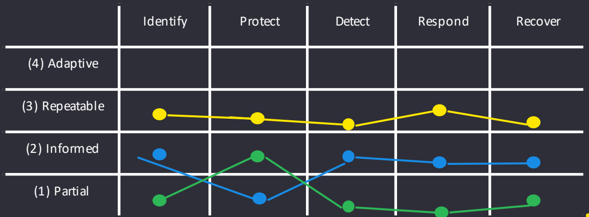
External monitoring score 725 ▲

3b Security Posture (Frameworks)

MITRE ATT&CK

	Initial access	Gain control	Lateral mov.	Data access	Data transf.
Coverage	25%	25%	25%	25%	25%
Tested	15%	15%	15%	15%	15%
Detection	65%	65%	65%	25%	25%

NIST CSF



4 Top risk scenarios

	Exposure
Successful ransomware attack	€20M
Top executive spear phishing	€10M
IP stolen by internal employee	€5M
Account takeover due to critical vulnerability	€25M
Major disruption to a critical service caused by DDoS	€2M

5 Ongoing risk reduction efforts

	Cost	Reduction	ROI
Revamp vulnerability management	€10M	€5M	50%
PII data inventory & protection	€5M	€5M	50%
Review firewall rules	€5M	€1M	25%

6 Recommended risk reduction efforts

Recommendation	Cost	Risk reduction	ROI
Xyz tool for DLP protection	€1M	€5M	15%
Purchase cyber insurance	€2M	€100M	55%

EY

Thank you!

Olga Ghincul

CISM, CRISC
Senior Manager, EY

olga.ghincul@be.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

ey.com/be