

WG1 + WG2

FEEDBACK

WG1

- WG1 - Risk Managements
- Managing risks in an organisation
 - a) Who / why / benefits.
 - b) Metrics
 - c) SME specificities

Who / why / benefits

- a1) Who - Final ownership with CEO,
- www.coso.org operational responsibility in the line.
- a2) Why - to provide guidance and clarity on their cyber risk position and thus allow organisations to understand their short mid and long term actions.
- a3) benefits - Improved resilience and continue and improved market conditions

Metrics

- 1b) Metrics
- Process metrics with Quality scope relating CMMI
- Outcome metrics specific to certain attack vectors and actors, linking also to vulnerabilities

Metrics

- Risk calculation Threats and vulnerabilities impact
- Mitigating measures
- Preventative measures
- Reference initial recommendations from WG1 reports

Verification and audit

- It is cheaper to prevent than to repair
- ETSI
 - Business driven
 - EU recommendation to use standards

Verification and audit

- Verify and audit the quality system
- Report on applicability of the perfect situation

Verification and audit

Who has responsibility? It is collective! Government

- National government agencies cannot understand the business.
- Need independent body
- Create champions of best secure
- Cyber essentials
- Benchmarking Malcolm baldrige award
- Peer to peer auditing
- The right to audit a (SME-) supplier

Verification and audit

- Education

SME focus

- Principles are the same
- Knowledge transfer to SME
- Subsidise SME to reach the baseline level
- Being Cyber Resilient versus Affordability in terms of time, money and resources
- Take action or take risk, mitigate towards insurance, but with required knowledge level.