WELCOME TO THE RISKNZ LUNCHTIME SEMINAR
2 March 2021

Website: www.risknz.org.nz | Linkedin: www.linkedin.com/company/risknz/

RiskNZ would like to thank the support of our Sponsors and Supporters

PREMIER SPONSOR

MARSH

LUNCHTIME SEMINAR SPONSORS

SAI GLOBAL

Safety Associates

LUNCHTIME SEMINAR SUPPORTERS

KPMG

NAVIGATUS CONSULTING

Watercare
An Auckland Council Organisation

Christchurch City Council

POWERCO

What I wish Enterprise Risk Managers knew about cybersecurity

By: Ahmed ElAshmawy
Consulting Practice Lead
Axenic Ltd.

Get ready for a quiz

Using your mobile visit

www.menti.com

Use code 74 91 57 1

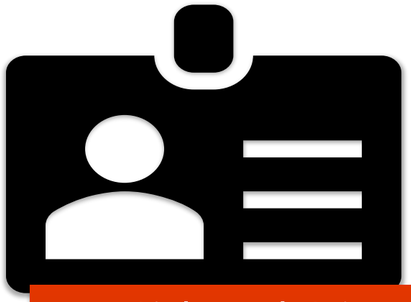
PCI Security Standards Council™ QUALIFIED SECURITY ASSESSOR

bsi ISO/IEC 27001 Information Security Management CERTIFIED

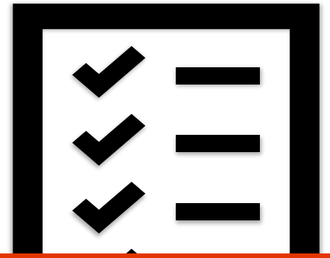
axenic Pure Security

About Axenic

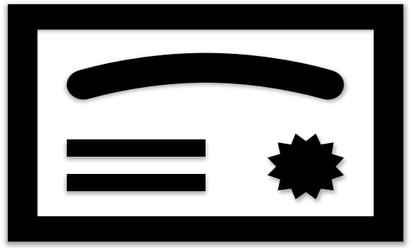
GCDO Governance, Risk and Assurance



Risk and Privacy Consulting

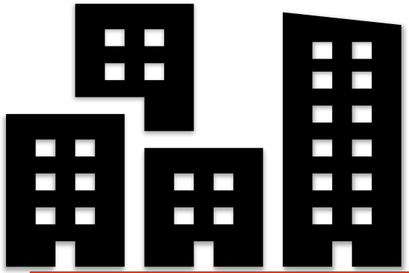


PCI DSS Audit and Consulting

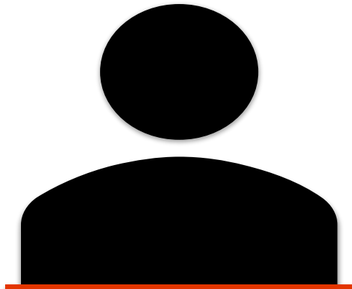


ISO27001 certification

Security Strategy/DevOps



Enterprise Security Architecture



Virtual CISO

Security Programme Implementation

PCI Security Standards Council™ QUALIFIED SECURITY ASSESSOR

bsi ISO/IEC 27001 Information Security Management CERTIFIED

axenic Pure Security

Roles

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

bsi
ISO/IEC 27001
Information Security Management
CERTIFIED

axenic
Pure Security

Roles

Go to **www.menti.com** and use the code **74 91 57 1**

Mentimeter

The main role of the ICT team in Cybersecurity (or information security) risk management is

QUALIFIED SECURITY ASSESSOR

ISO/IEC 27001 Information Security Management CERTIFIED

axenic
Pure Security

Roles

Go to **www.menti.com** and use the code **74 91 57 1**

Mentimeter

The main role of the Security (or Information Security) team is (Choose all that applies)

PCI Security Standards Council™ QUALIFIED SECURITY ASSESSOR

bsi ISO/IEC 27001 Information Security Management CERTIFIED

axenic Pure Security

Roles

Go to **www.menti.com** and use the code **74 91 57 1**

The main role of busines in Cybersecurity (or information security) risk management

Mentimeter

PCI Security Standards Council™ QUALIFIED SECURITY ASSESSOR

bsi ISO/IEC 27001 Information Security Management CERTIFIED

axenic Pure Security

So, What did I wish Enterprise Risk Managers knew about cybersecurity?

Cybersecurity Risk Management

- Not a technical problem
- Related to other operational risks
- Integrated in ERM
- Rating scales need adaptation

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

bsi ISO/IEC 27001 Information Security Management CERTIFIED

axenic
Pure Security

Business sees opportunity, we see …

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

bsi
ISO/IEC 27001
Information Security Management
CERTIFIED

axenic
Pure Security

Business sees opportunity, we see …

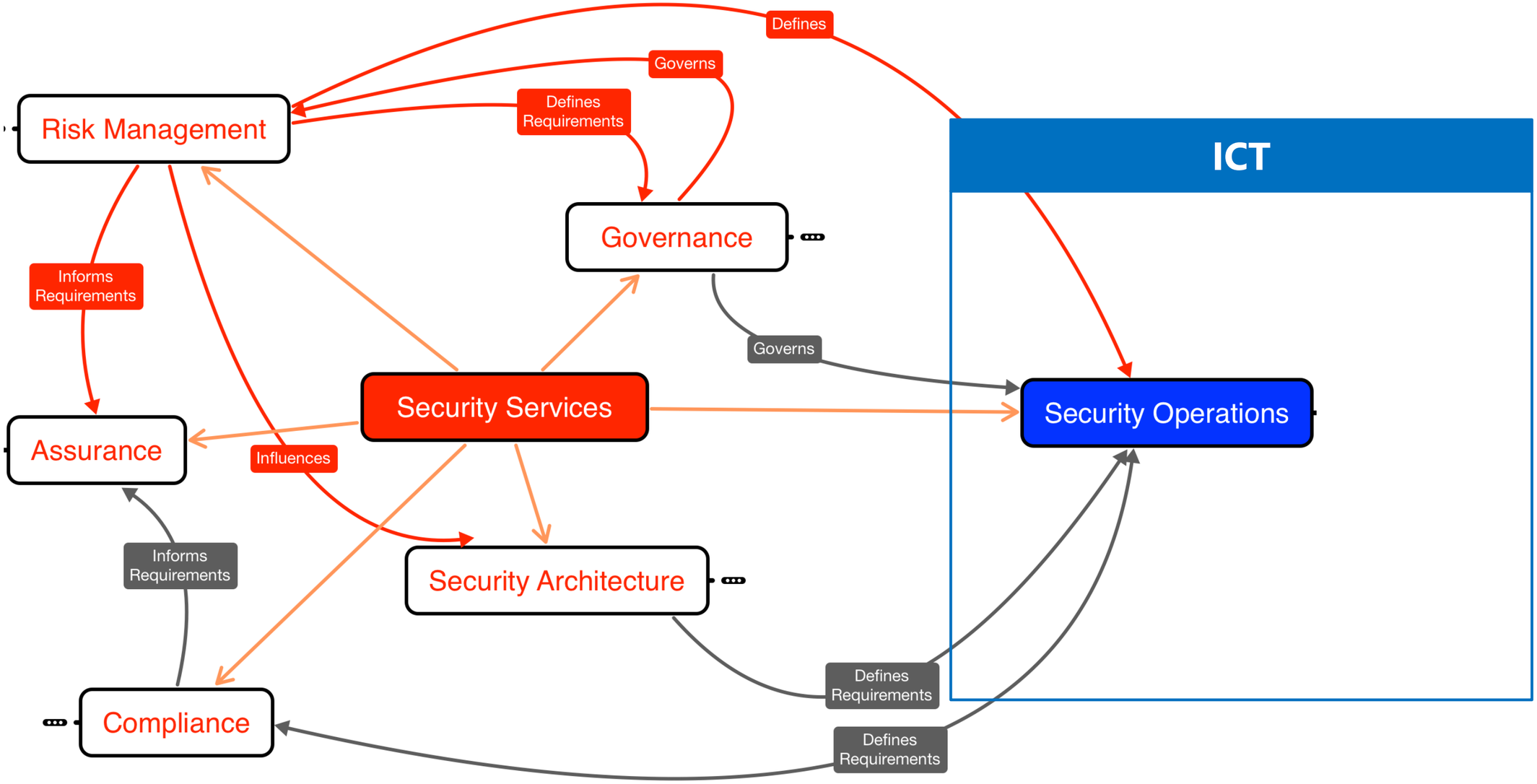
Risk people forensically spot risks when everyone sees opportunities

PCI Security Standards Council™ QUALIFIED SECURITY ASSESSOR

bsi ISO/IEC 27001 Information Security Management CERTIFIED

axenic Pure Security

Information Security Services



PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

bsi ISO/IEC 27001 Information Security Management CERTIFIED

axenic
Pure Security

Cybersecurity Risk Management

Initial Consult

Help!
I need Security work or C&A

Cybersecurity Activity

Outsourced Activity

Customer Activity

Plan and SOW

Kick-off and scheduling

Context Workshops

Risk and Control Workshops

initiation / concept / plan / requirements / design

Risk Management and System Security Plans

System build and development

Security Test (Penetration Test)

development / acquisition / integration / test

Control Validation Plan and Audit

Certification Report

implementation / go-live

Close-out

Follow-up Audit

operations and maintenance

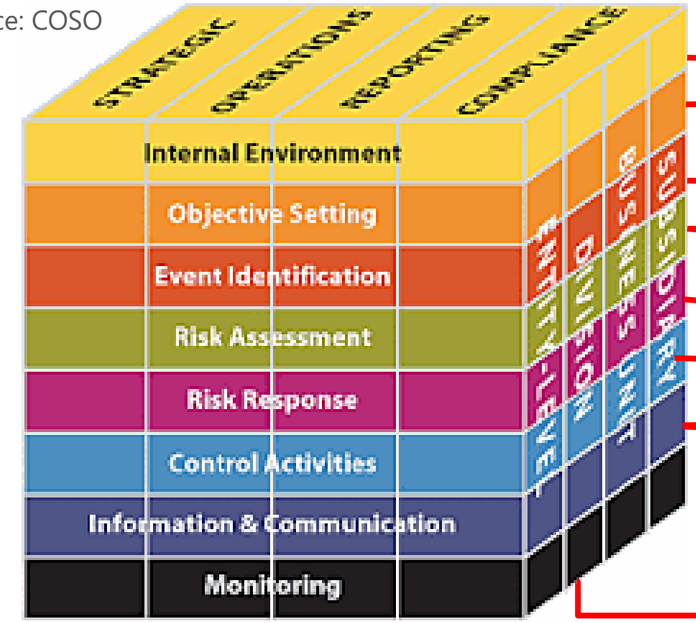
GCDO 105 Questionnaire
Security Risk Assessment (SRA)
Privacy Threshold Assessments (PTA)
Privacy Impact Assessments (PIA)

Security Risk Management Plan (SRMP)
System Security Plan (SSP)
Security, Vulnerability Scan, Penetration Test Report

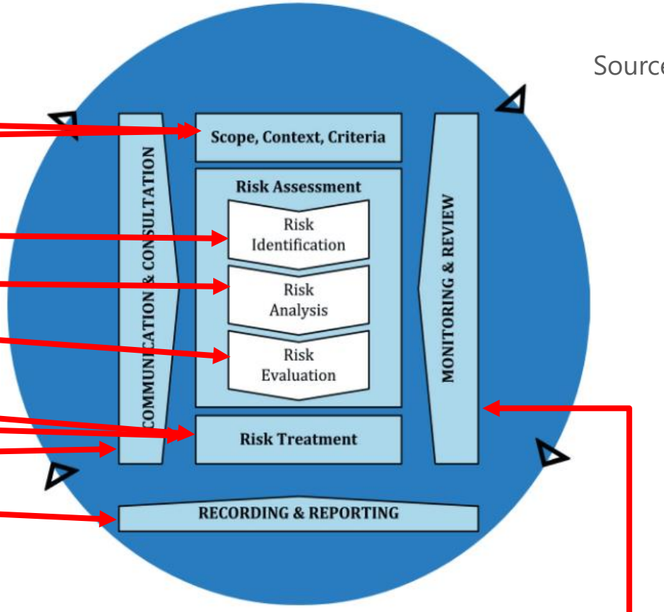
Controls Validation Plan and Audit (CVP / CVA)
Security Audit Report
Remediation Plan
System Security Certificate

Integrating Cybersecurity RM in ERM

Source: COSO



Source: ISO 31000



Scope & Context

Plan and SOW

Kick-off and scheduling

Context Workshops

Assessment

Risk and Control Workshops

Treatment

Risk Management and System Security Plans

System build and development

Security Test (Penetration Test)

Assurance & Communication

Control Validation Plan and Audit

Certification Report

Monitoring & Review

Close-out

Follow-up Audit

Scales

Risk scales are not always fit for purpose

- Health & Safety and Strategic Likelihood scales
- Service delivery and Legal impact scales
- Reputational scales
- Aggregated value and compound impacts

PCI Security Standards Council™ QUALIFIED SECURITY ASSESSOR

bsi ISO/IEC 27001 Information Security Management CERTIFIED

axenic Pure Security

So, What did I wish Enterprise Risk Managers knew about cybersecurity?

Cybersecurity Risk Management

- Not a technical problem
- Related to other operational risks
- Integrated in ERM
- Rating scales need adaptation

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

bsi ISO/IEC 27001 Information Security Management CERTIFIED

axenic
Pure Security

Questions

www.axenic.co.nz/contact

www.linkedin.com/in/aaelashmawy

@aaelashmawy

axenic

Pure Security

www.axenic.co.nz/contact

www.linkedin.com/in/aaelashmawy

@aaelashmawy

RiskNZ would like to thank the support of our Sponsors and Supporters

PREMIER SPONSOR

MARSH

LUNCHTIME SEMINAR SPONSORS

SAI GLOBAL

Safety Associates

LUNCHTIME SEMINAR SUPPORTERS

KPMG

NAVIGATUS CONSULTING

Watercare
An Auckland Council Organisation

Christchurch City Council

POWERCO

THANK YOU FOR JOINING OUR LUNCHTIME SEMINAR

Website: www.risknz.org.nz | Linkedin: www.linkedin.com/company/risknz/