ПЛАНЕТА ITSM

от проторенных дорог -
к новым горизонтам!

VII Всероссийская конференция itSMF

4-5 октября 2016 | Москва & Инфопространство

APPROVED BY EXPERTS
itSMF
СООБЩЕСТВО ПРОФЕССИОНАЛОВ ITSM

WWW.ITSMFCON.RU/2016/

ITIL® Practitioner and Resilia™ - More than just new exams

optimal
Service Management Ltd

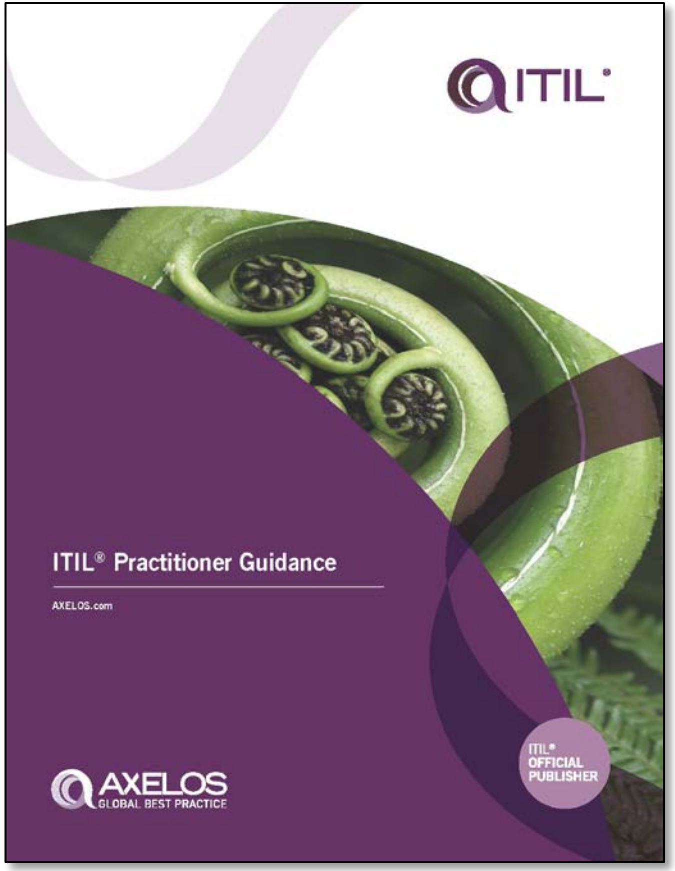
Stuart Rance

Consultant, trainer, author
Information security and IT service management
@StuartRance

ITIL Practitioner

What customers asked for

- More focus on adopt and adapt
- We need guidance on the 'how to'
- Make it relevant to solving business problems

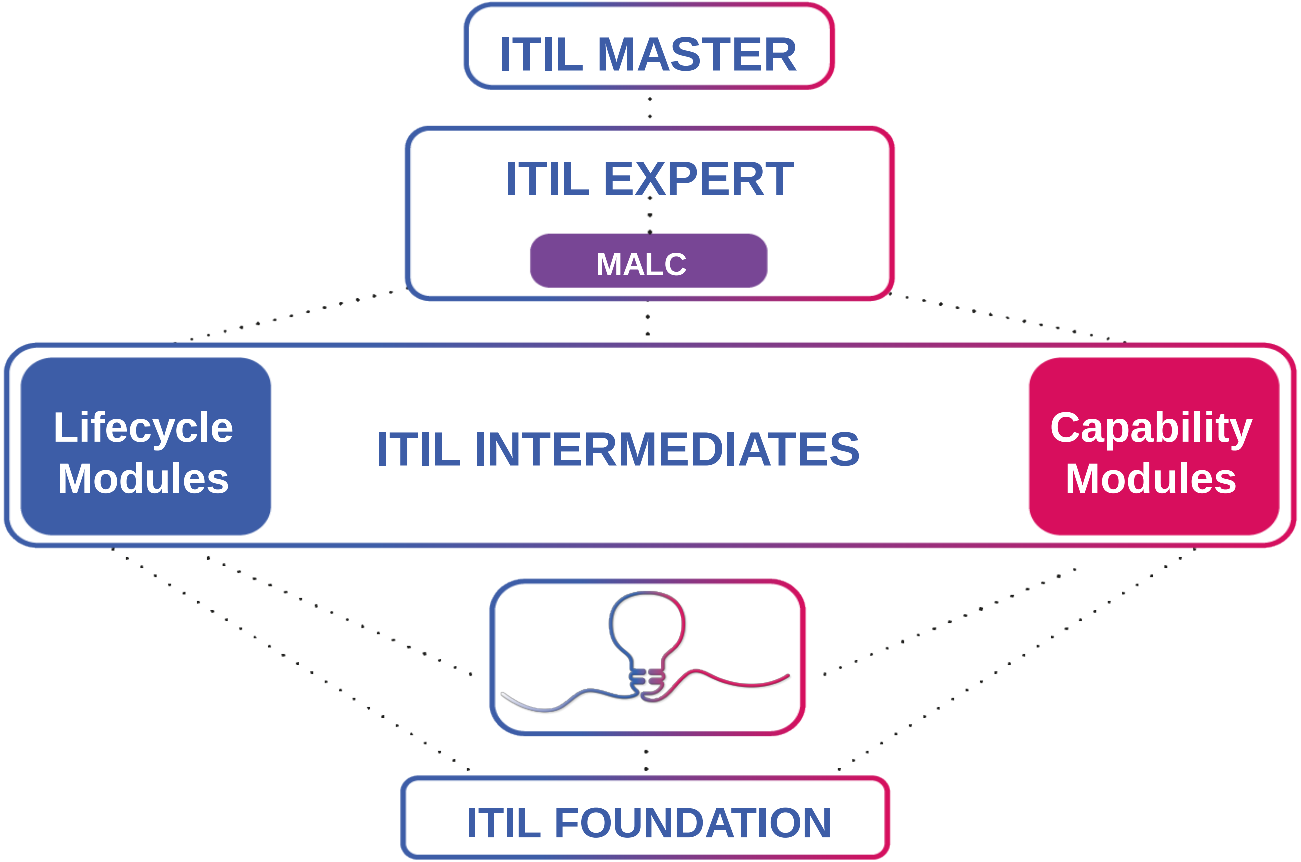


ITIL Practitioner

ITIL Practitioner Architect Team (PAT)

- Kevin Behr (US)
- Karen Ferris (AU)
- Lou Hunnebeck (US)
- Barclay Rae (UK)
- Stuart Rance (UK)
- Paul Wilkinson (NL)

ITIL Practitioner



ITIL MASTER

ITIL EXPERT

MALC

Lifecycle Modules

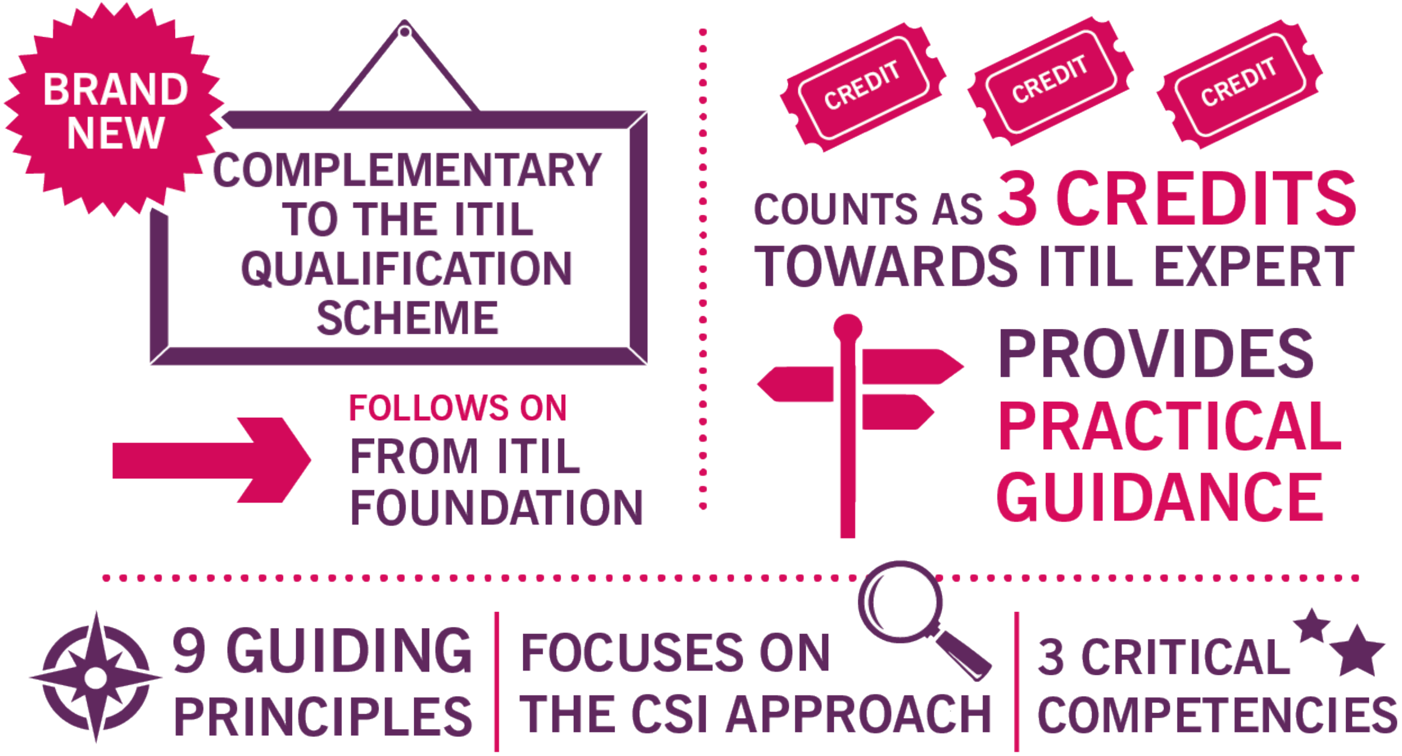
ITIL INTERMEDIATES

Capability Modules

ITIL FOUNDATION

ITIL Practitioner

optimal
Service Management Ltd



BRAND NEW

COMPLEMENTARY TO THE ITIL QUALIFICATION SCHEME

FOLLOWS ON FROM ITIL FOUNDATION

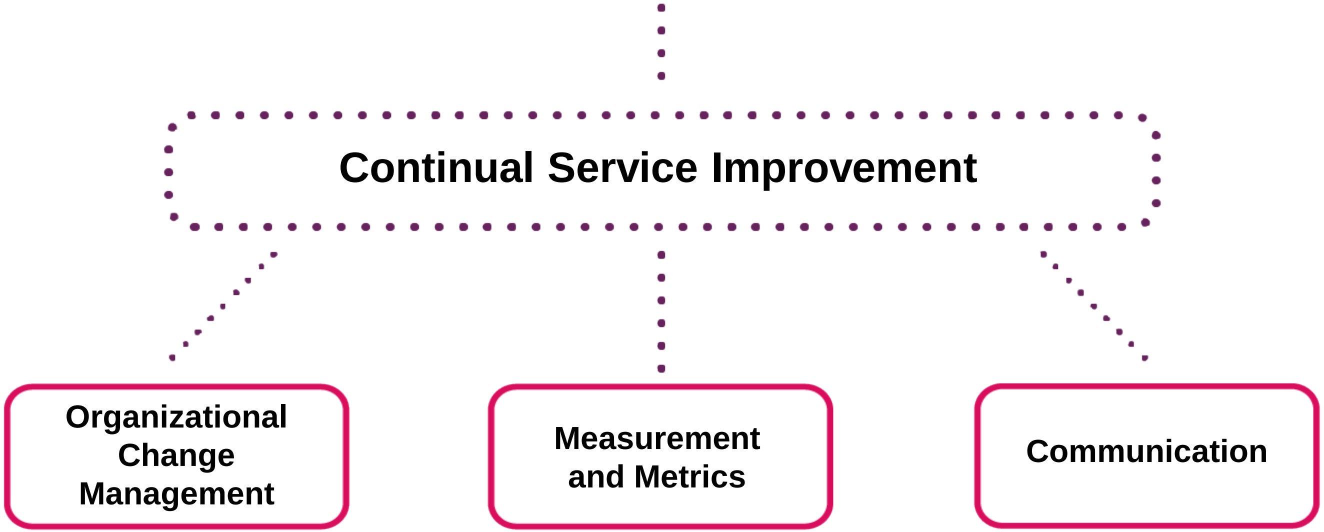
COUNTS AS 3 CREDITS TOWARDS ITIL EXPERT

PROVIDES PRACTICAL GUIDANCE

9 GUIDING PRINCIPLES

FOCUSES ON THE CSI APPROACH

3 CRITICAL COMPETENCIES



Continual Service Improvement

Organizational Change Management

Measurement and Metrics

Communication

Organizational Change Management

- A clear and bought-into vision
- Strong and committed leadership
- Empowerment and teamwork
- Willingness to participate
- Right skills and relevant knowledge
- A sustainable approach to improvement

Measurement and Metrics

- Supports validating decisions & assumptions
- Sets a clear direction for improvements
- Justifies what we do and why we do it
- Provides the means of healthy intervention
- Utilizes balanced, meaningful KPIs
- Links vision, objectives, goals, CSFs, & KPIs

Communication

- Communication is a 2-way process
- We are all communicating all the time
- There is no single way of communicating
- Timing and frequency matter
- The message is in the medium

Continual Improvement

- Understanding the context
- Assessing the current state
- Describing the desired state
- Planning and executing
- Confirming value delivery
- Ensuring continuity

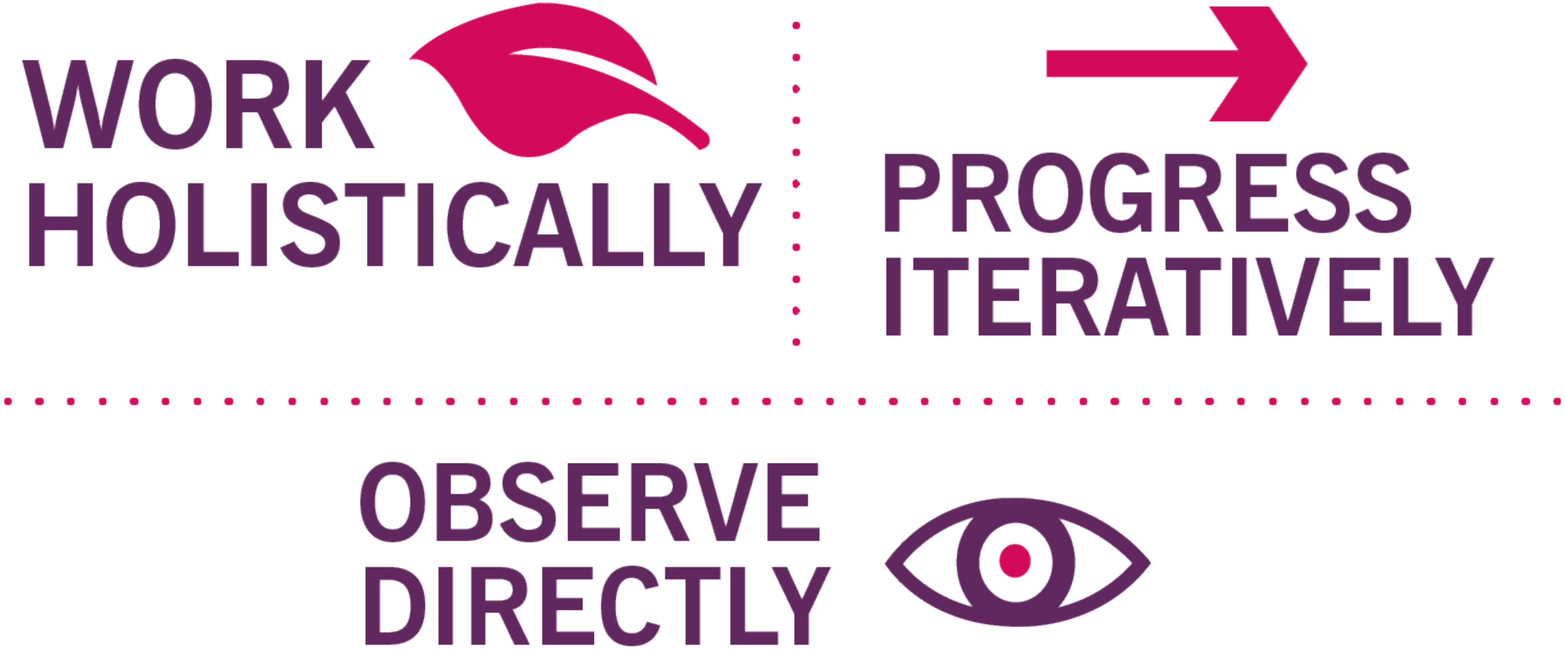
Guiding Principles

FOCUS ON VALUE

DESIGN FOR EXPERIENCE

START WHERE YOU ARE

Guiding Principles

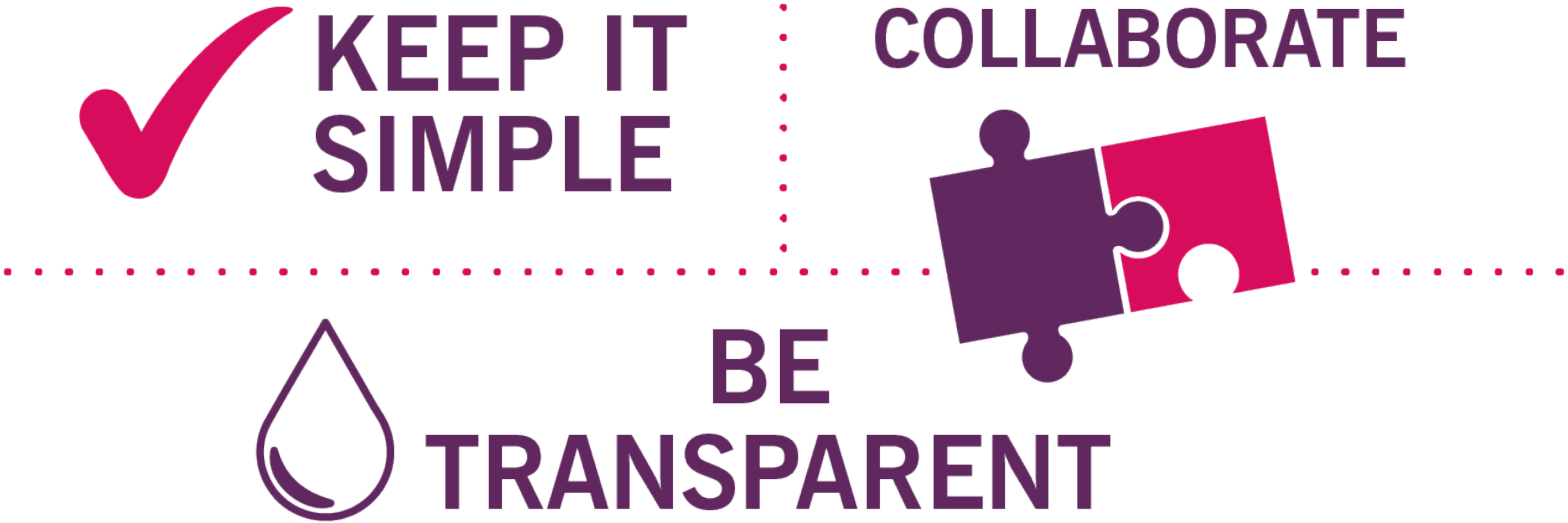


WORK HOLISTICALLY

PROGRESS ITERATIVELY

OBSERVE DIRECTLY

Guiding Principles



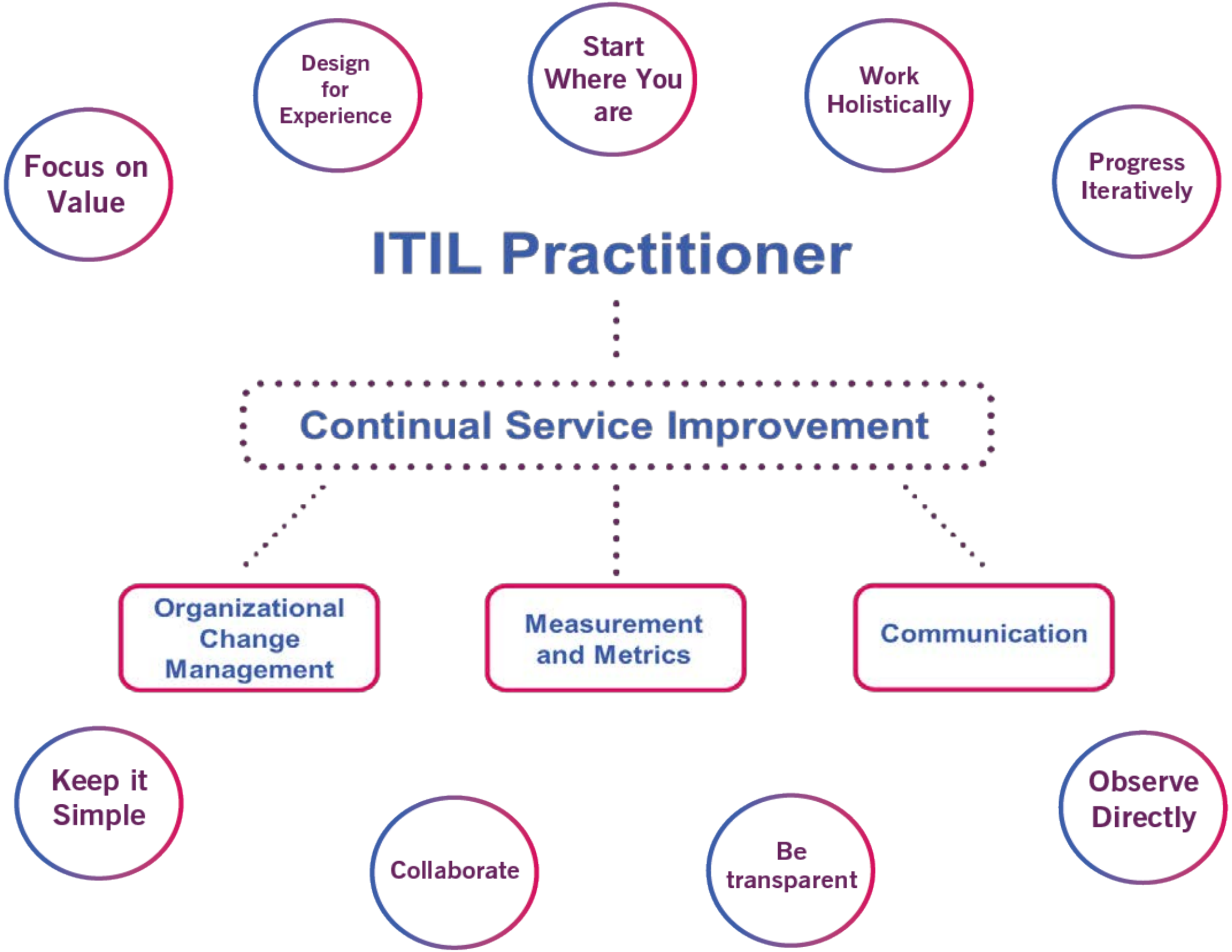
KEEP IT SIMPLE

COLLABORATE

BE TRANSPARENT

9 Guiding Principles

- FOCUS ON VALUE
- DESIGN FOR EXPERIENCE
- START WHERE YOU ARE
- WORK HOLISTICALLY
- PROGRESS ITERATIVELY
- OBSERVE DIRECTLY
- KEEP IT SIMPLE
- COLLABORATE
- BE TRANSPARENT



Focus on Value

Design for Experience

Start Where You are

Work Holistically

Progress Iteratively

ITIL Practitioner

Continual Service Improvement

Organizational Change Management

Measurement and Metrics

Communication

Keep it Simple

Collaborate

Be transparent

Observe Directly

DRIVING ORGANIZATIONAL CHANGE

MEASURING & DEMONSTRATING SUCCESS & VALUE

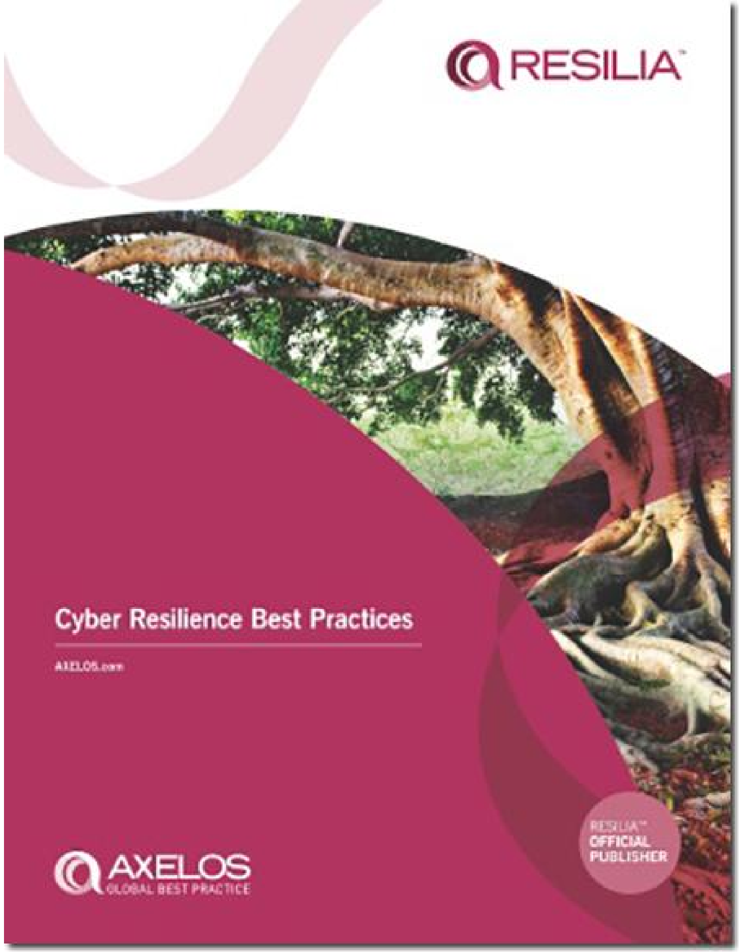
IMPROVING COMMUNICATION

Which all results in

AN ENGAGED AND MOTIVATED WORKFORCE WITH THE KNOW-HOW TO ACTION INITIATIVES

A CONTINUALLY IMPROVING SERVICE, ALIGNED TO BUSINESS GOALS

A HAPPY CUSTOMER



RESILIA™

Cyber Resilience Best Practices

AXELOS.com

AXELOS
GLOBAL BEST PRACTICE

RESILIA™
OFFICIAL
PUBLISHER

Resilia: Cyber Resilience Best Practice

- Why does cyber resilience matter?
- The need for balance
- ITSM and Infosec collaboration
- RESILIA™ overview

Why does cyber resilience matter?

CUSTOMERS

$£€¥

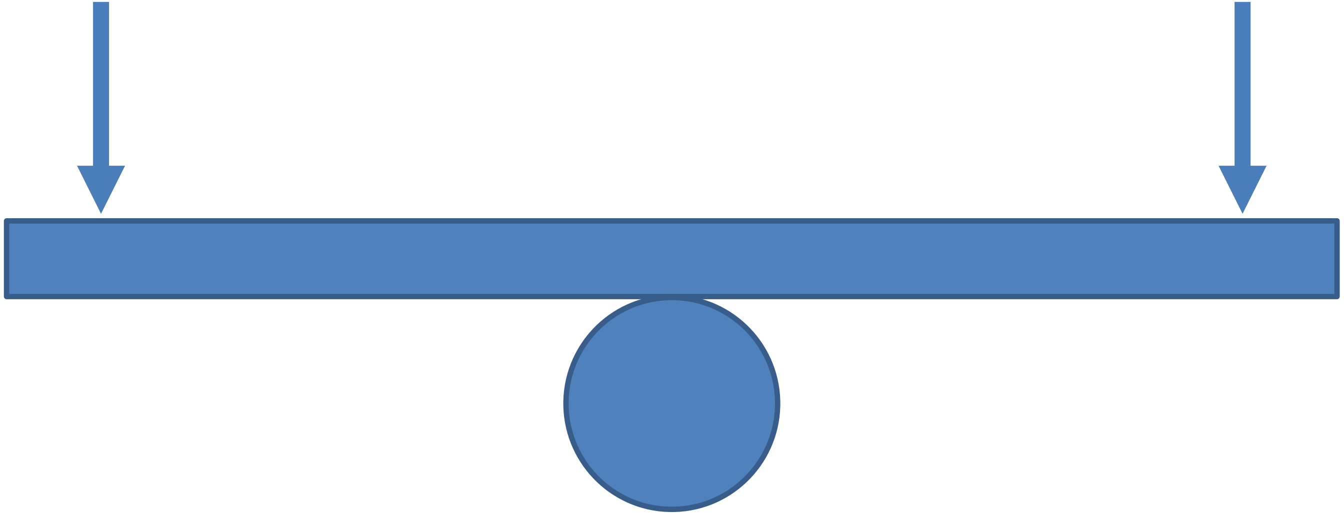
Why does cyber resilience matter?

Security breaches are reported in the press daily

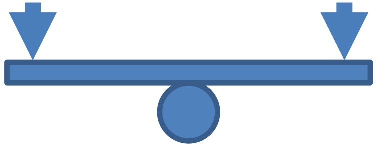
- Large and small organizations are affected
- Organizations in every industry are affected
- Breaches impact many millions of end customers
- Losses typically run into millions of $£€¥
- CEOs and CIOs have been forced to resign

If you think you've never been breached then you probably aren't monitoring well enough to know!

The need for balance



The need for balance

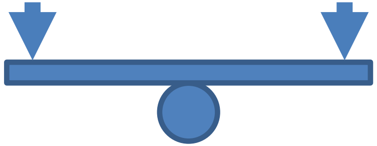


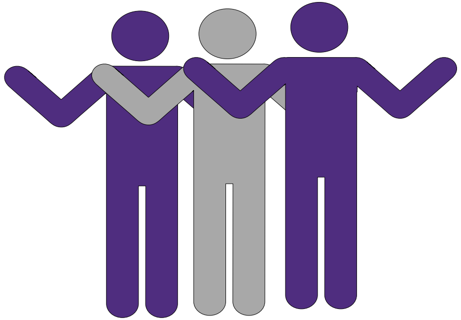
Prevent

Detect

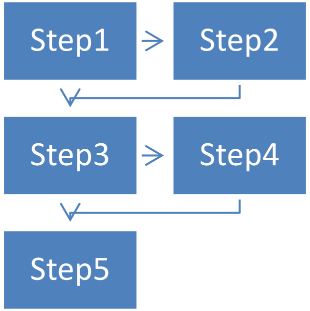
Correct

The need for balance





People

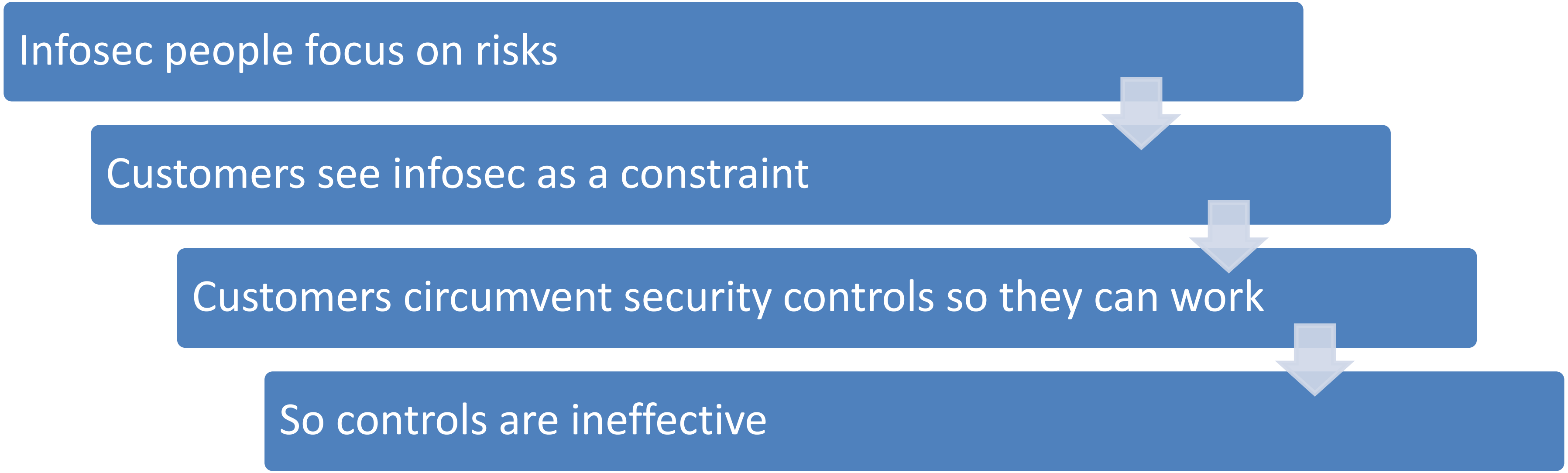


Process

Technology

The need for balance

Risks v Opportunities



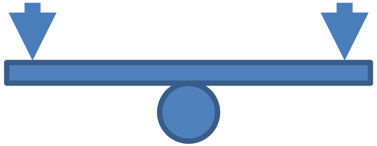
Infosec people focus on risks

Customers see infosec as a constraint

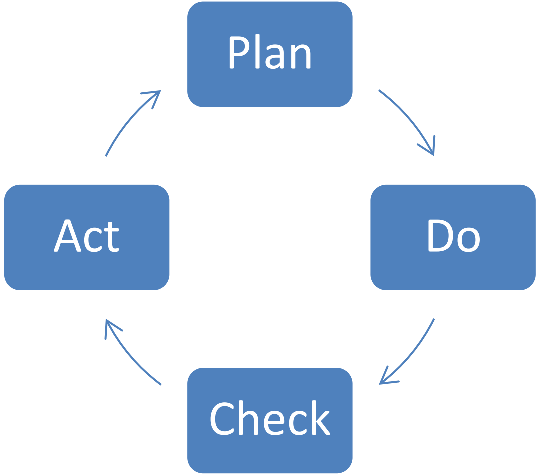
Customers circumvent security controls so they can work

So controls are ineffective

The need for balance



Getting it right



Continual improvement

Audit is your friend, it's not something to avoid

ITSM and Infosec collaboration

ITSM and Infosec collaboration

- IT service management is about managing INFORMATION technology services

- Infosec is about managing INFORMATION security

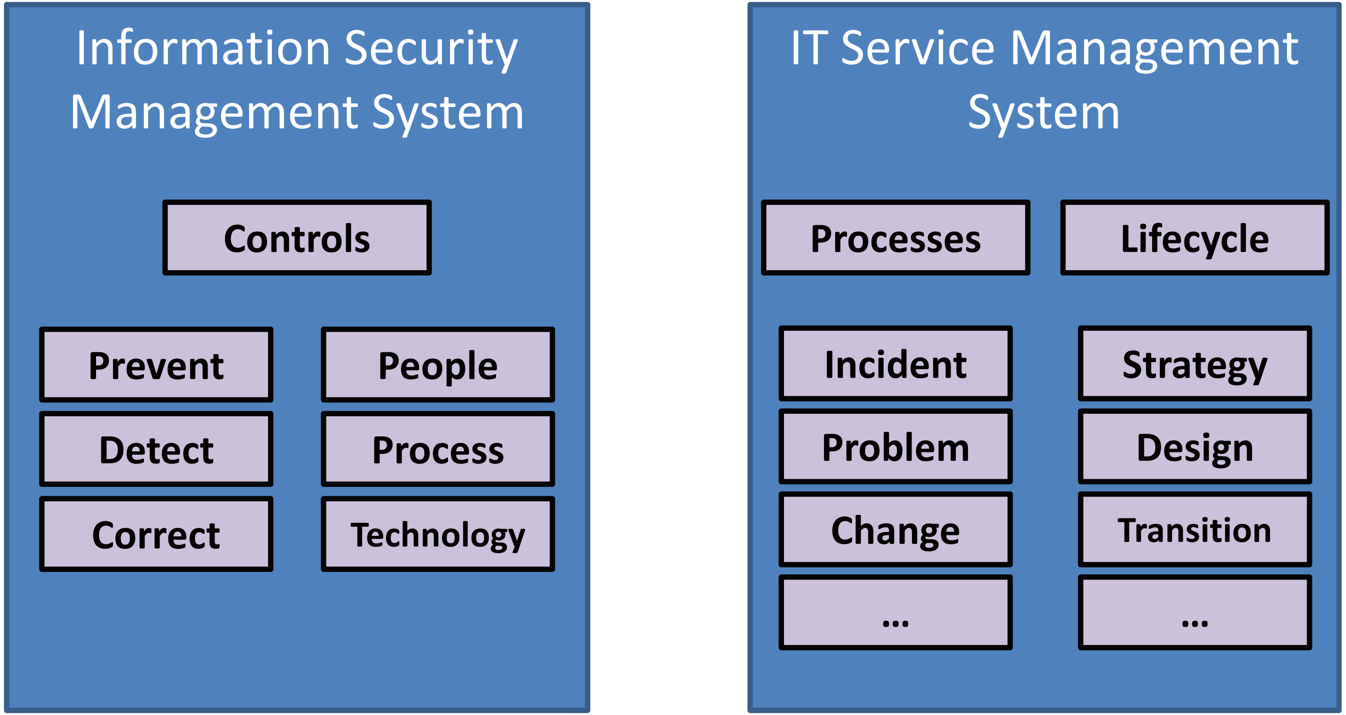
- They are both dealing with
  - *The same information*
  - *The same IT services*
  - *The same need to manage*

ITSM and Infosec collaboration

- Many organizations implement
  - *An information security management system*
  - *AND an IT service management system*

- BUT they are trying to manage the same information
  - *This will never work*
  - *What is needed is collaboration*
  - *Work together on designing, building and running information systems and information technology*

ITSM and Infosec collaboration



Information Security Management System

Controls

Prevent

Detect

Correct

People

Process

Technology

IT Service Management System

Processes

Incident

Problem

Change

…

Lifecycle

Strategy

Design

Transition

…

ITSM and Infosec collaboration

Every ITSM process

- Can contribute to infosec
- Needs a contribution from infosec

For example

- Asset and configuration management
  - *Infosec provides required security controls for the CMS*
  - *Infosec provides tools to detect unauthorized changes*
  - *ITSM provides data about numbers and revisions of assets*
  - *ITSM detects unauthorized changes*

ITSM and Infosec collaboration

Security incident management

- This is an enormous area of overlap

- If you haven’t been involved in testing scenarios
  - *Find the infosec people in your organization*
  - *Discuss how they plan security incident responses*
  - *Understand how this impacts nearly every ITSM process*
  - *Work together to design interfaces and improve processes*
  - *Get involved in testing recovery scenarios*

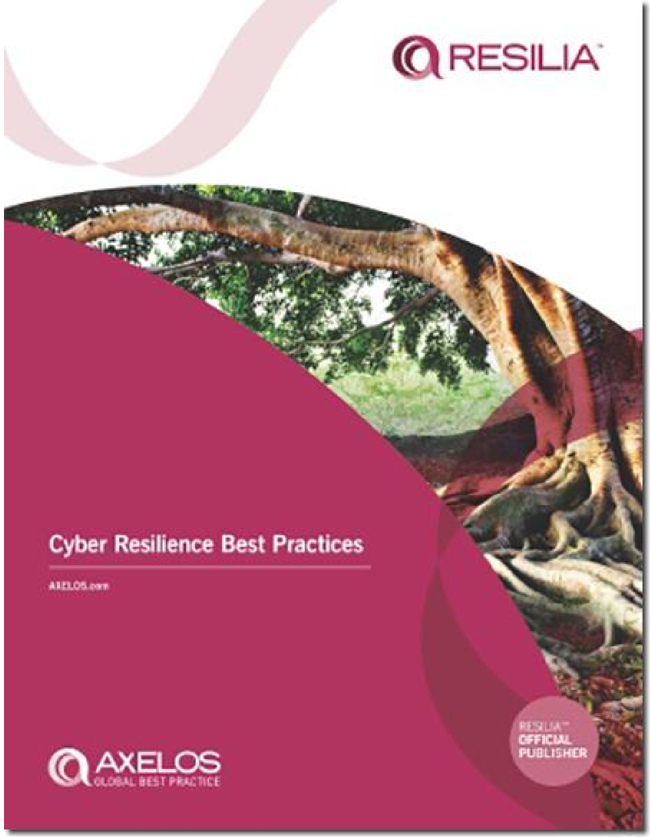
ITSM and Infosec collaboration

ITSM professionals have an enormous opportunity

Seek out the infosec people in your organization

- Ensure they understand how ITSM processes could contribute to information security
- Learn how security controls could contribute to ITSM
- Start building the relationships needed to
  - *Work together to jointly create value*
  - *Collaboratively improve every aspect of infosec and ITSM*

RESILIA™ overview



RESILIA™

Cyber Resilience Best Practices

AXELOS.com

AXELOS
GLOBAL BEST PRACTICE

RESILIA™
OFFICIAL
PUBLISHER

Resilia: Best Practice Overview

RESILIA is documented in a single publication

- Covering the entire lifecycle of cyber resilience

RESILIA describes a similar lifecycle to ITIL

- Strategy, design, transition, operation, continual improvement
- The RESILIA lifecycle is about cyber resilience
- RESILIA integrates well with ITSM and other management system approaches

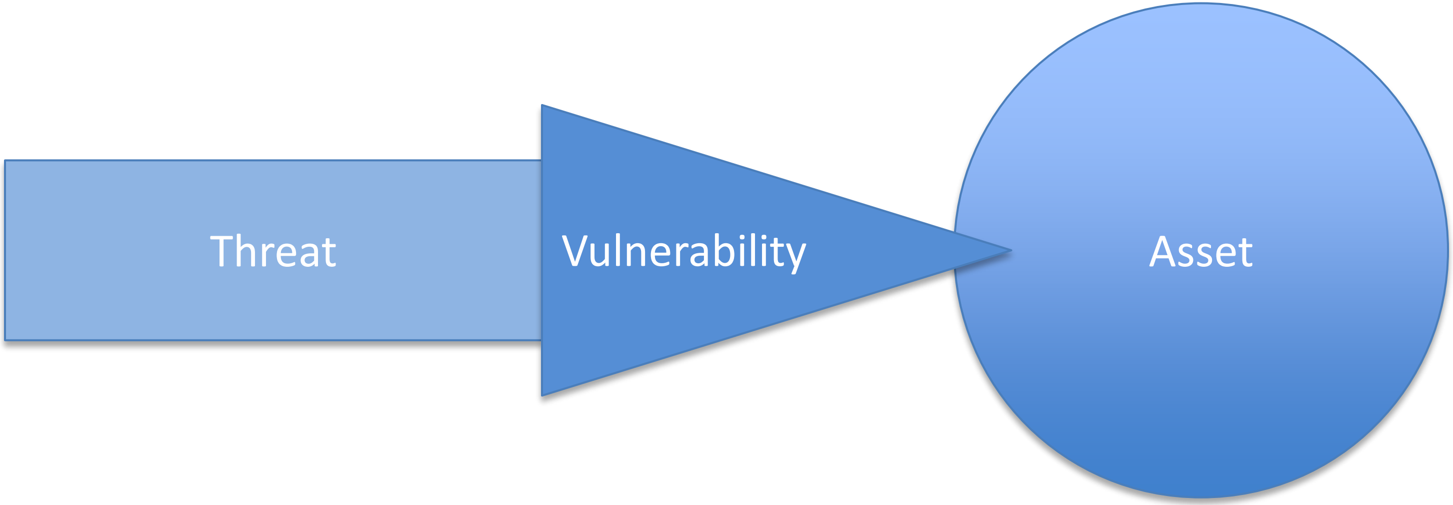
Publication structure

1. Introduction
2. Risk management
3. Managing cyber resilience
4. Cyber resilience strategy
5. Cyber resilience design
6. Cyber resilience transition
7. Cyber resilience operation
8. Cyber resilience continual improvement
9. Roles and responsibilities

Three case studies about fictional organizations are threaded through all the chapters

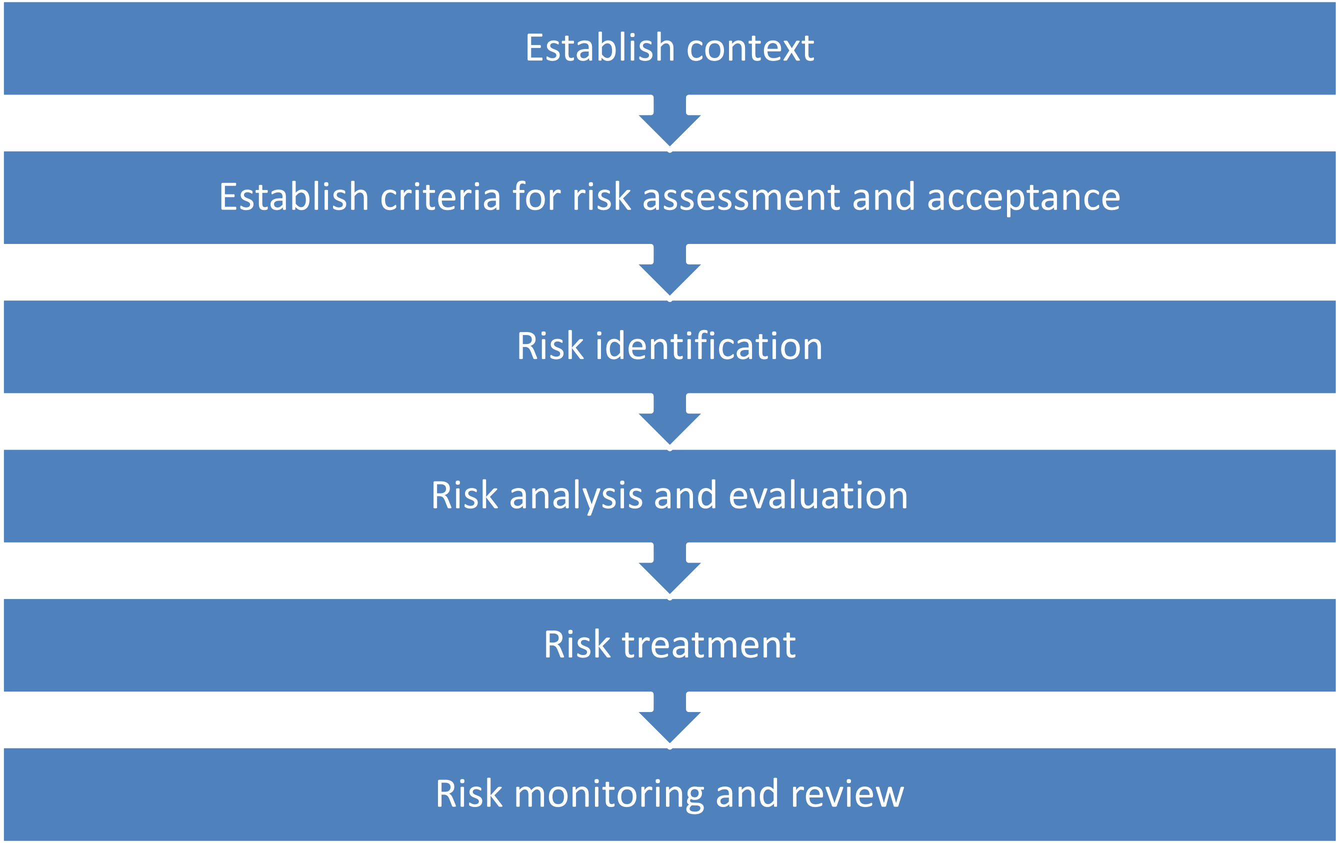
Risk Management

Cyber resilience is largely about managing risks



A risk is created by a threat exploiting a vulnerability to impact an asset

Risk Management



Establish context

Establish criteria for risk assessment and acceptance

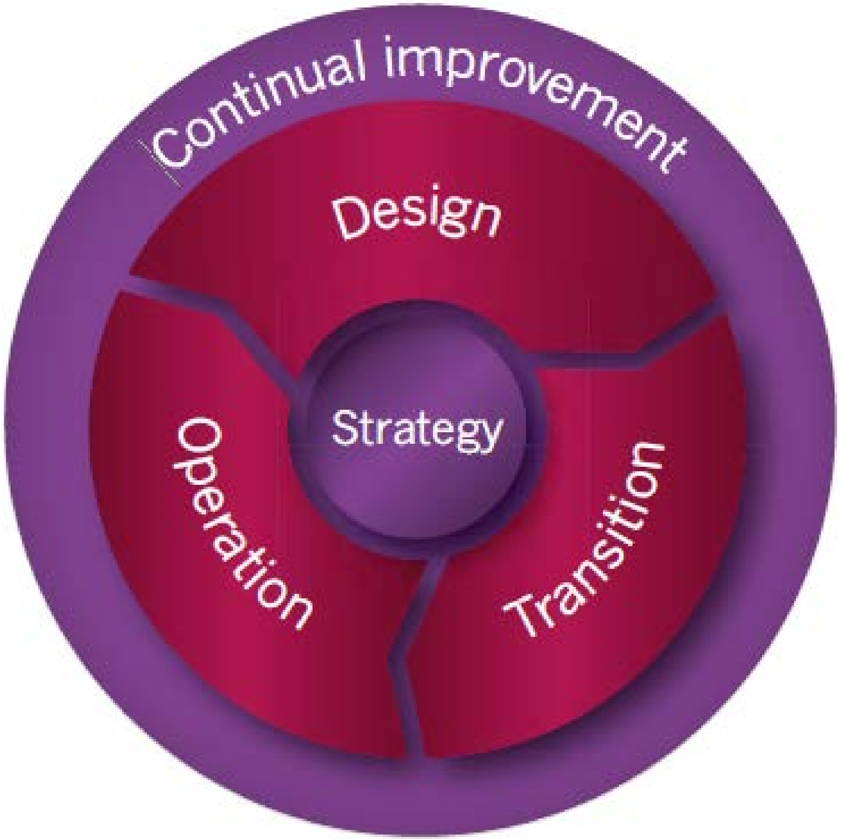
Risk identification

Risk analysis and evaluation

Risk treatment

Risk monitoring and review

Cyber Resilience Life Cycle



RESILIA

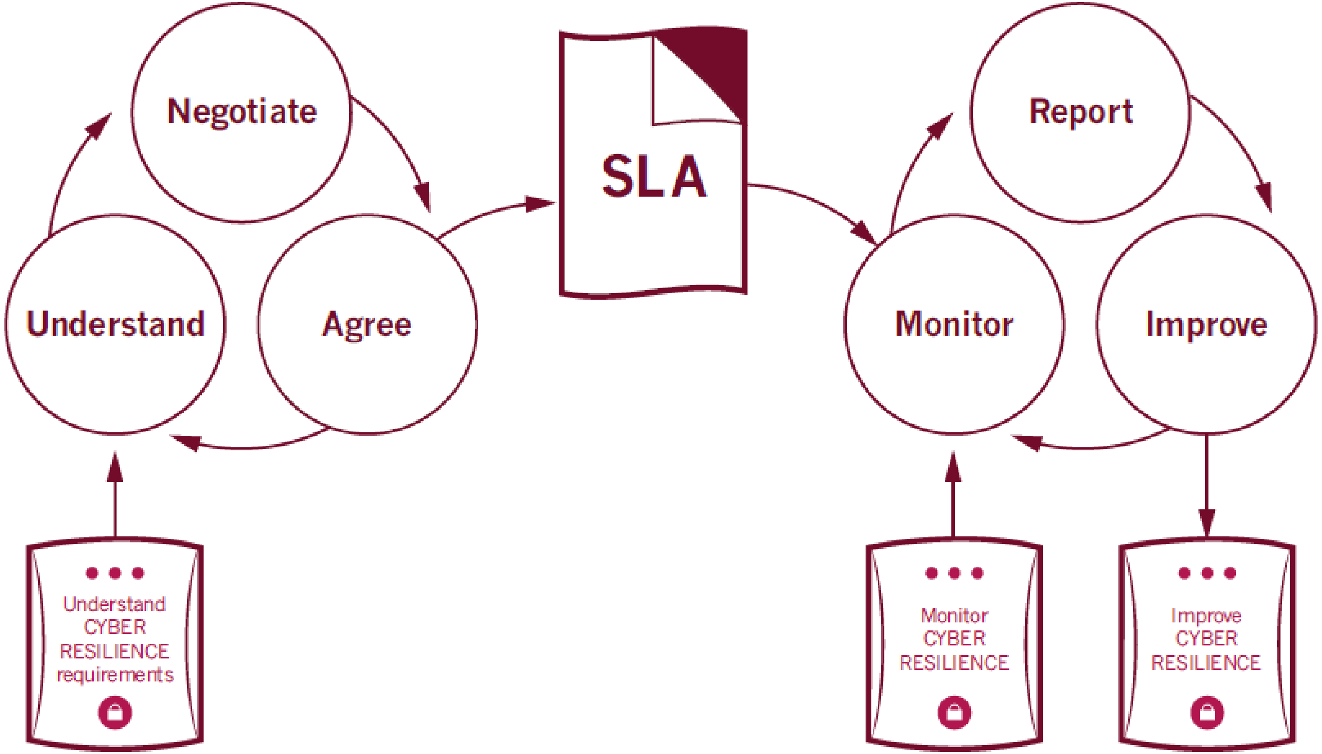
Cyber Resilience Best Practices

AXELOS

All lifecycle stages

- Lifecycle stage summary
- Control objectives and controls
- Aligning with ITSM
- Scenarios (from the three case studies)
- Questions (to help you think about applying the ideas)

Aligning with ITSM - example



Resilia

Strategy controls

- Governance
- Stakeholder management
- Policies
- Audit and compliance

Resilia

Design controls

- HR security
- System acquisition, development, architecture and design
- Supplier and 3rd party security
- Endpoint
- Cryptography
- Business continuity management

RESILIA

Cyber Resilience Best Practices

AXELOS

Resilia

RESILIA

Cyber Resilience Best Practices

AXELOS

Transition controls

- Asset and configuration management
- Change management
- Testing
- Training
- Document management
- Information retention and disposal

Resilia

RESILIA

Cyber Resilience Best Practices

AXELOS

Operation controls

- Access control
- Network security
- Physical security
- Operations security
- Security incident management

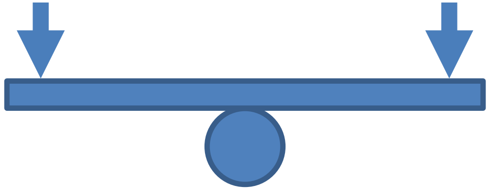
Resilia

optimal
Service Management Ltd

Continual improvement controls

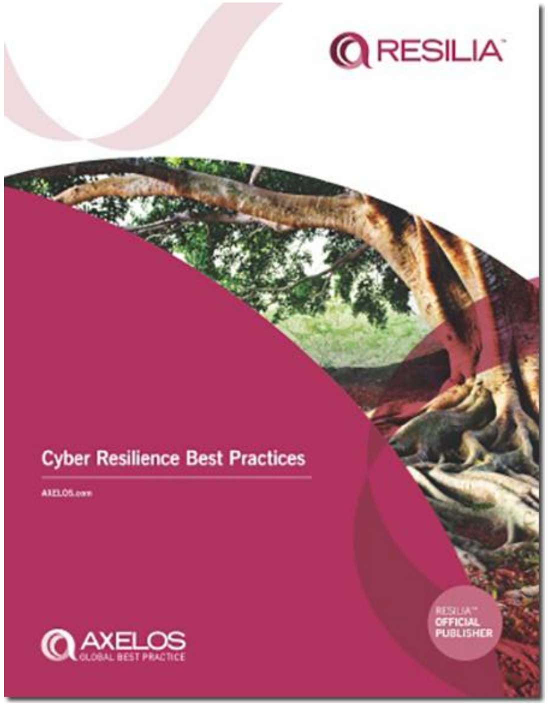
- Audit and review
- Control assessment
- Remediation and improvement planning

Resilia Summary



- Prevent, detect and correct
- People, process and technology
- Risks and opportunities
- Getting it right and continual improvement

- Cyber resilience can contribute to ITSM
- ITSM can contribute to cyber resilience
- Collaboration can create increased business value



RESILIA

Cyber Resilience Best Practices

AXELOS.com

AXELOS
GLOBAL BEST PRACTICE

RESILIA
OFFICIAL
PUBLISHER

What about the exams?

- Resilia Foundation
- Resilia Practitioner
- ITIL Practitioner

Resilia Foundation

Similar to other Axelos foundation certifications

- Three day training course (online or face-to-face)
- 50 question multiple choice exam
- Covers all chapters of the publication
  - *General understanding of cyber resilience*
  - *Purpose of risk management and how to do it*
  - *Purpose of each lifecycle stage*
  - *Key features of each control*
  - *Interactions between cyber resilience and ITSM*

EXAMPLES AND CASE STUDIES ARE NOT EXAMINED

Practitioner exams

Similar to other Axelos practitioner certifications

- Foundation is a pre-requisite
- Two day training course (online or face-to-face)
- 50 question multiple choice exam
  - *With a case study and scenarios*
  - *More complex questions, but still only one correct answer*
- Content
  - *Resilia: Same content knowledge as foundation*
  - *ITIL: Content based on the ITIL Practitioner Guidance*
- Demonstrates that you can apply the knowledge

Example Resilia foundation question

Which could be a vulnerability?

A. A secret document

B. Anti-virus software on a laptop

C. A poorly trained staff member

D. A breach of credit card data

Example Resilia practitioner question

Which is the biggest risk in the scenario?

A. There might be no virus controls on the laptop

B. The confidential data might be leaked

C. The factory might be unable to operate

D. The firewall might be breached by a hacker

Example ITIL practitioner question

What should be improved to resolve this issue?

A. Stakeholder management

B. Metrics and measurement

C. Interfaces between processes

D. The software development process

Thank you

@StuartRance

StuartR@OptimalServiceManagement.com

optimal
Service Management Ltd

www.optimalservicemanagement.com