The Human Factor in Cyber Resilience

Leveraging International Best Practice

David Mudd

Global Head of Digital Trust Assurance, BSI

2024-09-19

Accelerating progress towards a better society and sustainable world

For more than 120 years BSI has shaped society in a profound and unique way.

We reinvest our profits into our knowledge and services to accelerate progress and increase trust between clients, consumers, governments and organizations.

BSI exists to have a positive impact on society. We partner with clients and stakeholders to deliver solutions to society's biggest challenges.

By Royal Charter

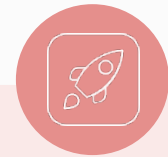SUSTAINABLE DEVELOPMENT GOALS

An agent for positive change

What we deliver for clients and stakeholders is trust... and trust fosters innovation, opportunity and growth.

Our strategic themes enable us to focus on our clients' greatest challenges:

How to shape a sustainable future

How to thrive in a digital world

Creating impact through a unique combination of services and solutions

Knowledge Solutions

- Creation and sharing of standards
- Information Solutions

Assurance Services

- Systems Certification
- Product Certification
- Training

Regulatory Services

- Medical Devices
- Artificial Intelligence
- Product Certification

Consulting Services

- Assessment
- Advice
- Implementation
- Continual improvement

Cybersecurity Key Trends

Human factor remains a key issue: vast majority of incidents triggered by human

Cost of Cybercrime

- Estimated at $8 trillion in 2023
- will grow to $10.5 trillion by 2025

Evolution of Ransomware

- RaaS market maturation and consolidation
- Rise of double-extortion: encryption + exfiltration
- Rise in demands > 317 million attempts reported in 2023

Supply Chain Attacks

- Shift of focus
- Was "supplier as weakest link"
- Now "supplier as biggest "blast area"
- Primary attack vector

Increasing vulnerabilities

- Total Common Vulnerabilities and Exposures (CVEs) expected to increase by 25% in 2024

The Human Factor

The role of employee engagement in cyber resilience

Key Learning Point

Tools and processes have their place....

"But it is people who are your best defence against an incident

and it is people who will get you out of trouble when it happens."

Engagement of C-suite, managers, experts, workers

Engagement – mental wellbeing

International Best Practice

ISO/IEC 27001

Management System for Information Security:

Confidentiality, Integrity and Availability

- Embeds culture of digital trust throughout an organisation

- Specifically addresses cybersecurity and privacy protection

- Specifically addresses management of the supply chain

- Enables security governance, management and continual improvement

- Includes > 90 security controls, but flexible

- > 120,000 sites certified globally

BS EN ISO/IEC 27001:2023
Incorporating corrigendum July 2023

BSI Standards Publication

Information security, cybersecurity and privacy protection — Information security management systems — Requirements
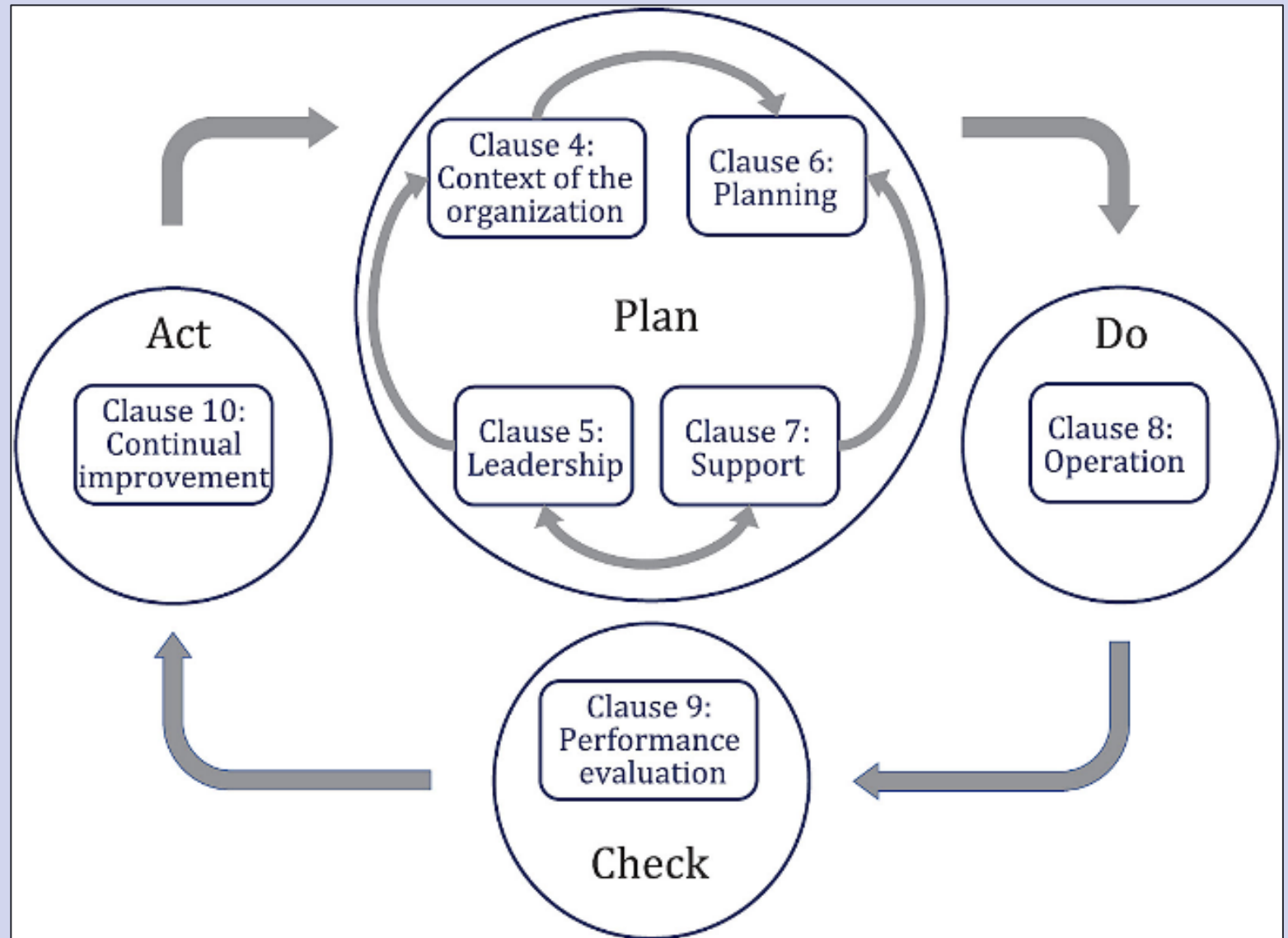
bsi.

ISO/IEC 27001 Key Concepts and Structure

- Risk-based thinking

- Management System global best practice

- Continual Improvement

- Flexibility

"The rock upon which digital trust is built."

Why ISO/IEC 27001?

From NHS Trust certified to 27001

- "...hugely beneficial when submitting DSPT, CAF frameworks and meeting legal requirements."

- "... massively enhances Information Security at the Trust."

- **"For us, the fog was lifted, and Information Security became clear, organised and effective."**

bsi

Learn more

https://page.bsigroup.com/l/73472/2024-08-06/2c7xrm9

Live Webinar

Protecting patient data: Addressing the vital role of cybersecurity in healthcare

Date: Tuesday, 1 October 2024 | Time: 11:00- 12:00 (BST)

Register now

The Human Factor in Cyber Resilience

Leveraging International Best Practice

Thank you

David Mudd

Global Head of Digital Trust Assurance, BSI

2024-09-19