

bsi.

# Building Digital Trust

## Challenges and Opportunities from Anti-Virus to AI

David Mudd  
Global Head of Digital Trust Assurance



## Agenda

- **Background**
- **Digital Trust and Why it Matters**
- **Navigating the Cyberverse – trends and threats**
- **Panel Session/Discussion : current challenges/pressing needs for organizations**
- **Preparing for the Future: become AI-ready with global standards and best practice**
- **Q&A**
- **Key Take-aways & Conclusion**

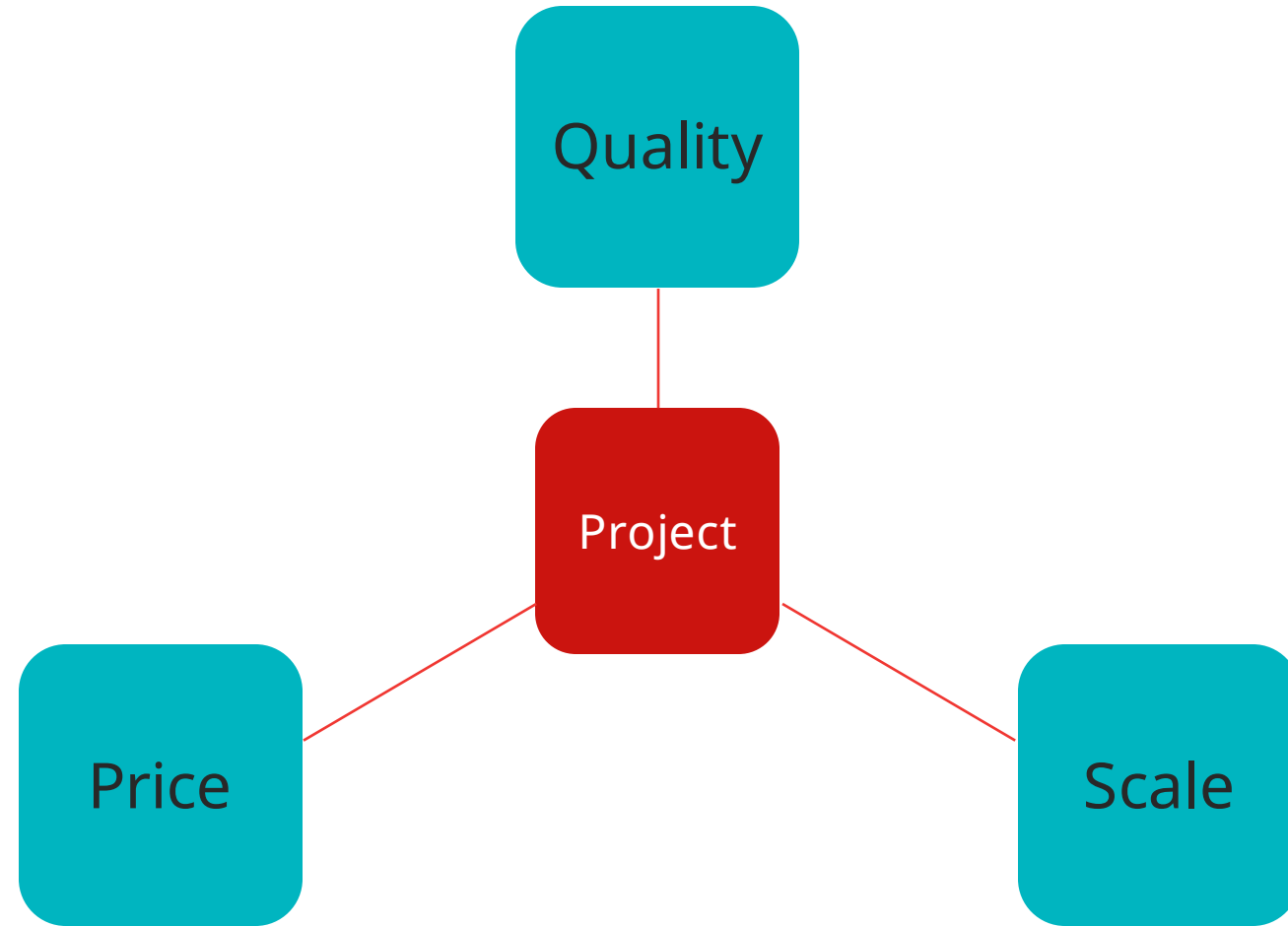


*“Digital trust is about instilling confidence in an **organization**, that empowers the **people**, the **digital systems and the technology** to ensure their safety, security, compliance, privacy and ethical requirements”*



# Why is Digital Trust important: Golden Triangle

---



***“digital trust is the currency that facilitates future innovation and prosperity”***

**World Economic Forum**



# BSI: A trusted catalyst for change

- Bring together leading thinkers, innovators and practitioners:
- Create best practice standards, regulatory frameworks
- Supporting compliance
- Global
- Independent:
  - Government
  - Shareholders

... we are a catalyst for positive change, creating an enduring legacy of improvement for our clients, their customers and society



## Knowledge Solutions

- Creating standards
- Information Solutions

**BS7799 – ISO/IEC 27001 InfoSec, CyberSec, Privacy**



## Assurance Services

- System & Product Certification
- Training

**Global Leader in InfoSec, CyberSec, Privacy**



## Regulatory Services

- Systems and Product Certification of Medical Devices

**EU AI Notified Body**



## Consulting Services

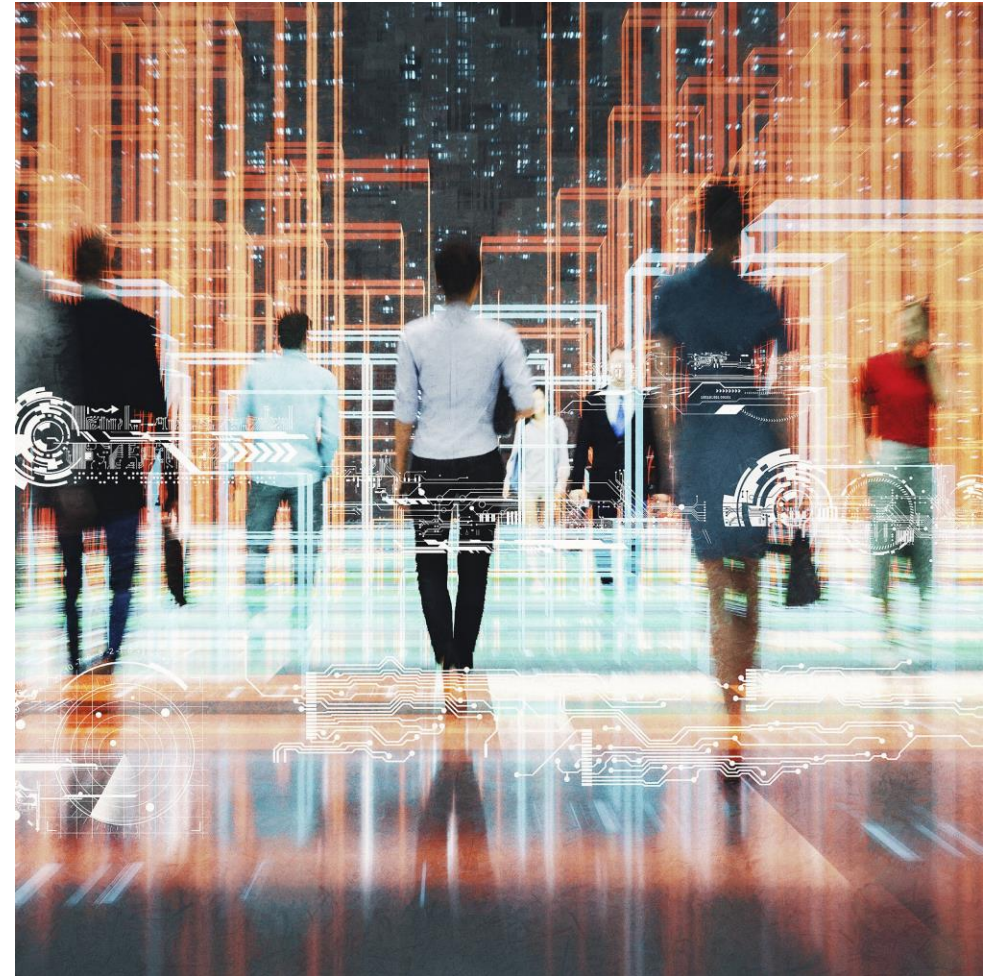
- Assessment
  - Advice
  - Implementation
  - Continual improvement
- CyberSec/Privacy**



We ensure trust in digital interactions and relationships between business, people and things specific to:

- **Cybersecurity**
- **Digital Supply Chain**
- **AI**
- **Data governance and privacy**

**All underpinned by digital governance and risk management**







**Artificial Intelligence**



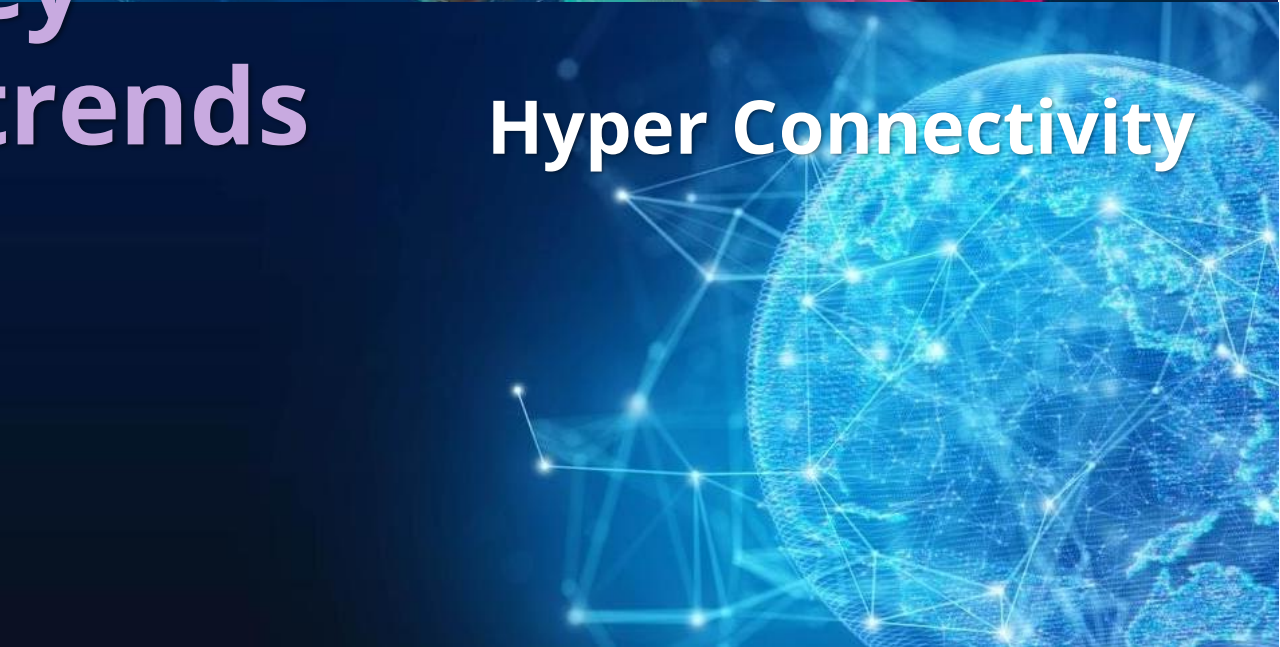
**Metaverse**

**Key**



**Mega Data**

**Megatrends**



**Hyper Connectivity**

# Key considerations...

**Regulation: CSA, NIS2, DSA, DORA, CRA, AI Act...etc**

**Governance/Oversight requirements – SEC  
Cybersecurity Ruling**

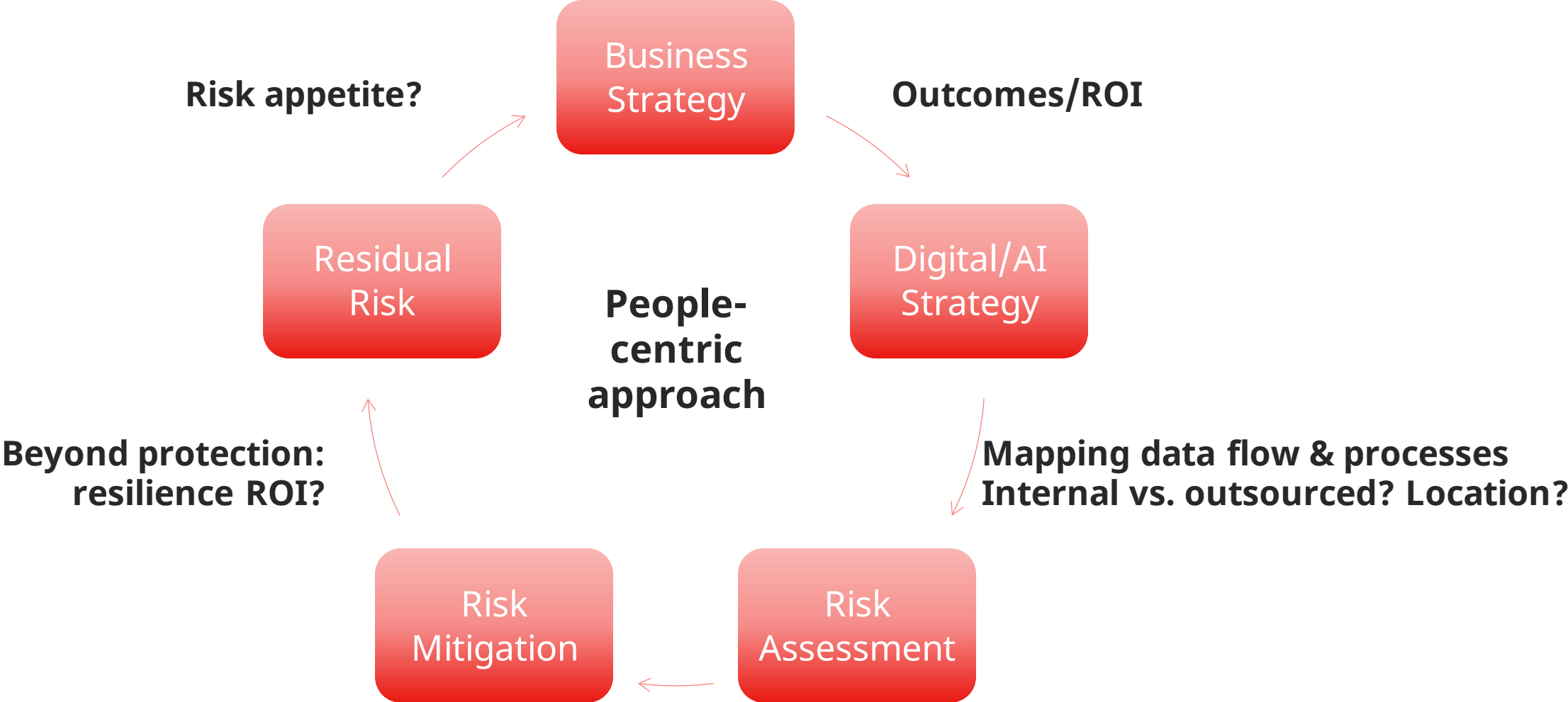
**Industrialization of Cybercrime**

- **Ransomware as a Service**
- **Large scale Denial/Destruction of Service**
- **AI-driven malware**

**Increased focus on Digital Supply Chain**

- **Increased dependency – agile, scalable, cost-effective**
- **Increased risk – key focus for cybercrime**





- Linking digital strategy to business strategy
- Digital risk, risk appetite, business strategy
- Going beyond protection: resilience
- *How aligned is your organization's digital risk with your business strategy and risk appetite?*
- *How resilient is your organization?*



- **Key business risk: criminal/accidental breach risk, legal/regulatory risk**
- **Full eco-system: 3<sup>rd</sup> parties**
- **Changing “people are the weakest link” to “people are the strongest weapon”**
- **Technical controls + People factor + positive culture cyber resilience**
- ***Does your organization understand its full cybersecurity ecosystem?***
- ***What is your organizational culture around cybersecurity?***



- **Your biggest cybersecurity risk?**
- **Cloud, Cloud-based Platforms/Services, SaaS**
- **Increasing dependencies + Increasing risks**
- ***How well does your organization know its digital supply chain and associated dependencies/risk?***



- **AI already impacting society –the next, big disruptor**
- **“AI as a force for good”**: route to smart, sustainable future, but high risk
- **AI issues: ethics, bias, explainable outcomes...etc**
- **Impact on AI subjects and workforce**
- **Start point: building a culture of trusted and responsible AI**
- ***What is your organization’s culture towards AI?***



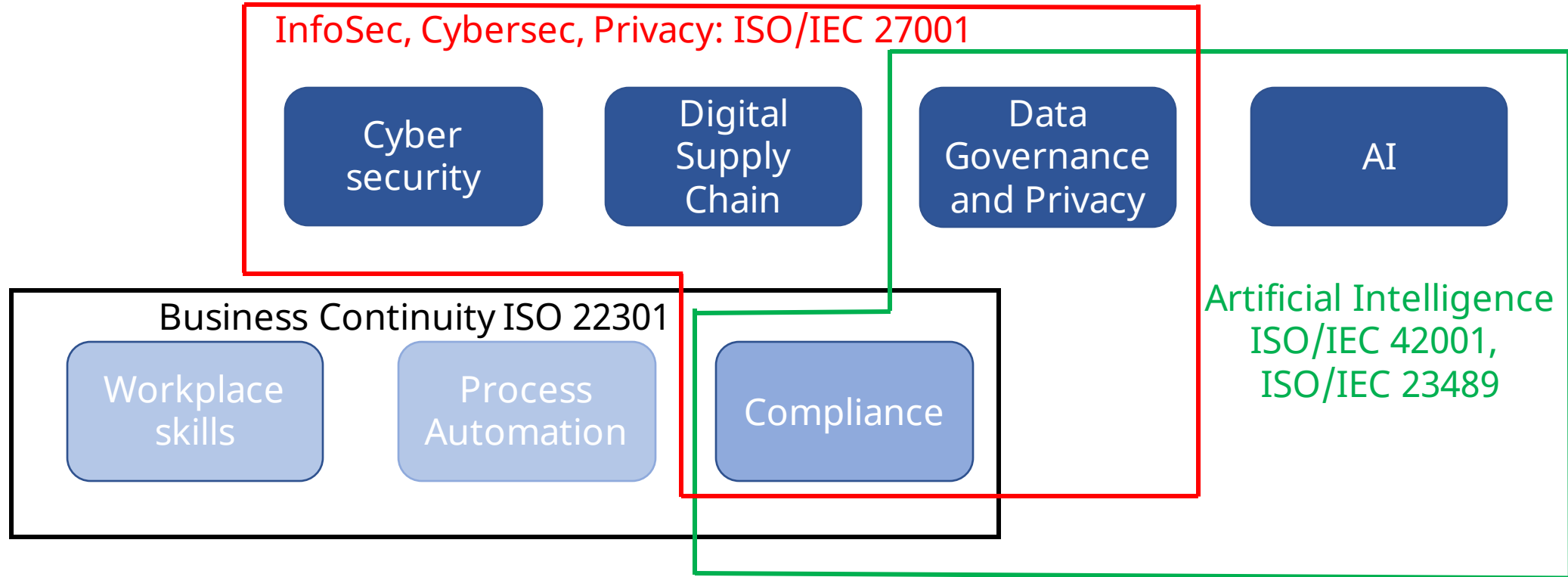
- **Data lifeblood of AI, metaverse, digital twins....  
And business!**
- **Governance: ownership, provenance, quality, integrity, security, use, storage, disposal...etc.**
- **Digital value chain – complex data flows across jurisdictions**
- **Privacy fundamental human right and global legal minefield for data**
- ***How well has your organization mapped its data flow and processes?***





# Addressing Digital Trust with International Standards

## Key Areas of Digital Risk



- Each management system addresses the governance and risk management process.
- Further standards apply as determined by the risk assessment.
- The business continuity process in ISO 22301 drives a proportionate approach to skills and automation risks, considering acceptable levels/duration of disruption



bsi.

# Building Digital Trust

**Summary and key take-aways**

# Digital Trust – Key Questions for your Organization

---

- *How aligned is your organization's digital risk with your business strategy and risk appetite?*
- *How resilient is your organization?*
- *Does your organization understand its full cybersecurity ecosystem?*
- *What is your organizational culture around cybersecurity?*
- *How well does your organization know its digital supply chain and associated dependencies/risk?*
- *What is your organization's culture towards AI?*
- *How well has your organization mapped its data flow and processes?*



**bsi.**

# Building Digital Trust

Challenges and Opportunities  
from Anti-Virus to AI

Thank you!

David Mudd  
Global Head of Digital Trust Assurance

