Your partner
in progress

Building a digital ecosystem that’s best in its class

BSI internal and supplier audit solutions

Audit programmes to address your digital risks, anticipate change and enable your business strategy

Opportunities and risks in digitization

Digitization has transformed organizations' operations and supply chains, enabling them to efficiently scale processes, enhance flexibility, accelerate decision making, drive down costs, and improve visibility and collaboration.

But digitization has also brought similar opportunities for criminals. Ransomware-as-a-service, the industrialization of cybercrime, data breaches, hacking, social engineering – these are growing risks in cyber and information security.

And that's on top of the increased data privacy and compliance requirements that come with the collection and storage of growing volumes of sensitive data, along with the strategic vulnerabilities that come from greater reliance on digital infrastructure.

"Allowing you to mitigate risk, empower employees and create a safer, sustainable future".

88%

of data breach incidents are directly linked to employee mistakes[1]

98%

of organizations have been negatively impacted by a cybersecurity breach that occurred in their supply chain[2]

51%

of organizations have experienced a data breach caused by a third party[3]

1 securitytoday.com
2 bluevoyant.com
3 securitymagazine.com

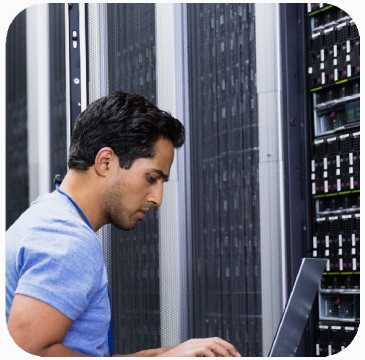
The organization and its supply chain: One cybersecurity ecosystem

Your organization’s supply chain is increasingly vulnerable to cyberattacks due to its expanding digital footprint and interconnected ecosystem. As your attack surface lies both internally and across your supply chain, you must consider the cybersecurity posture of your suppliers as well as your own organisation.

By addressing your organization and its supply chain as one ecosystem, you can take a holistic and comprehensive approach to minimizing network-wide cybersecurity weaknesses and protecting critical assets.

> “You can take a holistic and comprehensive approach to minimizing network-wide cybersecurity weaknesses"

Reasons to view internal and external digital systems as a unified ecosystem:



Data flow and information sharing

Effective supply chain operations also feature the seamless flow of sensitive or proprietary data between entities.

Digital supply chain

The adoption of cloud and cloud-based services is accelerating and increasing data flows further still.

Interconnectedness

The digital interconnectedness of organizations and their supply chains creates an extended attack surface, since breaches in oneelement can ripple through the other.

Regulatory compliance

Many regulatory frameworks and data protection laws require organizations to extend security practices to their supply chains.

Regulatory pressure is growing

Governments have moved to develop cybersecurity disclosure initiatives to encourage organizations to enhance their readiness and capabilities, in recognition of the increasing frequency, sophistication and cost of cyberattacks. The Securities and Exchange Commission (SEC) in the United States and Financial Conduct Authority (FCA) in the United Kingdom both have proposals in the works, for example.

But even where regulators aren't involved, shareholders, customers, and other stakeholders increasingly expect transparency from organizations regarding their cybersecurity practices. Disclosing relevant information provides increased digital trust and safeguards your reputation.

Example intiatives:

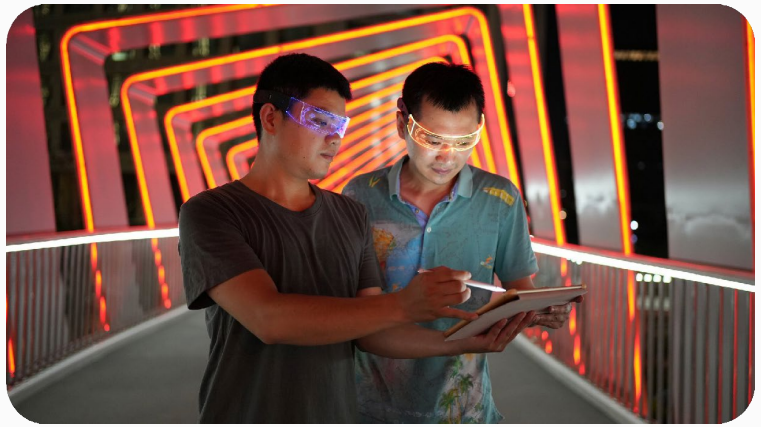
The Financial Conduct Authority (FCA) in the United Kingdom, require effective cybersecurity risk management practices and disclosure of material cyber incidents by financial institutions. They are currently piloting additional disclosure initiatives.

The Securities and Exchange Commission (SEC), in the United States, recently adopted rules requiring public companies to disclose material cybersecurity incidents and on an annual basis, release their cybersecurity risk management, strategy and governance.

How do you enhance digital trust?

Your organization should be able to meet legal and regulatory compliance quickly and cost-effectively – and fulfill stakeholder expectations – for cybersecurity management and disclosures. Doing so will help you better manage risk and increase digital trust.

To ensure your information security (infosec) and privacy posture accurately reflects your organization's requirements, you need to first identify your individual risks and strategies. For example, every organization will have different technologies deployed, varying underlying risk appetites and unique supply chain structures.



Effectively addressing cybersecurity challenges, mitigating risk and meeting regulatory requirements starts with a combination of processes and policies, including:

- An overarching cybersecurity policy, linked to the business strategy
    - Assess risk (including digital, legal, and physical)
    - Align investment with business strategy and risk appetite
- Incident response plans
- Transparent communications
- Monitoring of compliance with applicable laws and regulations
- Drivers for continuous improvement
- Effective training for employers and suppliers

How can your organization get there?

By establishing an audit programme that encompasses your digital ecosystem (including both internal and supplier operations), organizations like yours can confidently and comprehensively align your infosec and cybersecruity practices with noth only the relevant standards, laws, and regulations, but with your own business strategy and risk appetite.

An integrated programme can also help you establish key performance indicators aligned to your business strategy and risk appetite, measure these against insights provided through regularly analyzed data, and use the insights gained to drive continuous improvements.

"An integrated programme can also help you establish key performance indicators aligned to your business strategy"

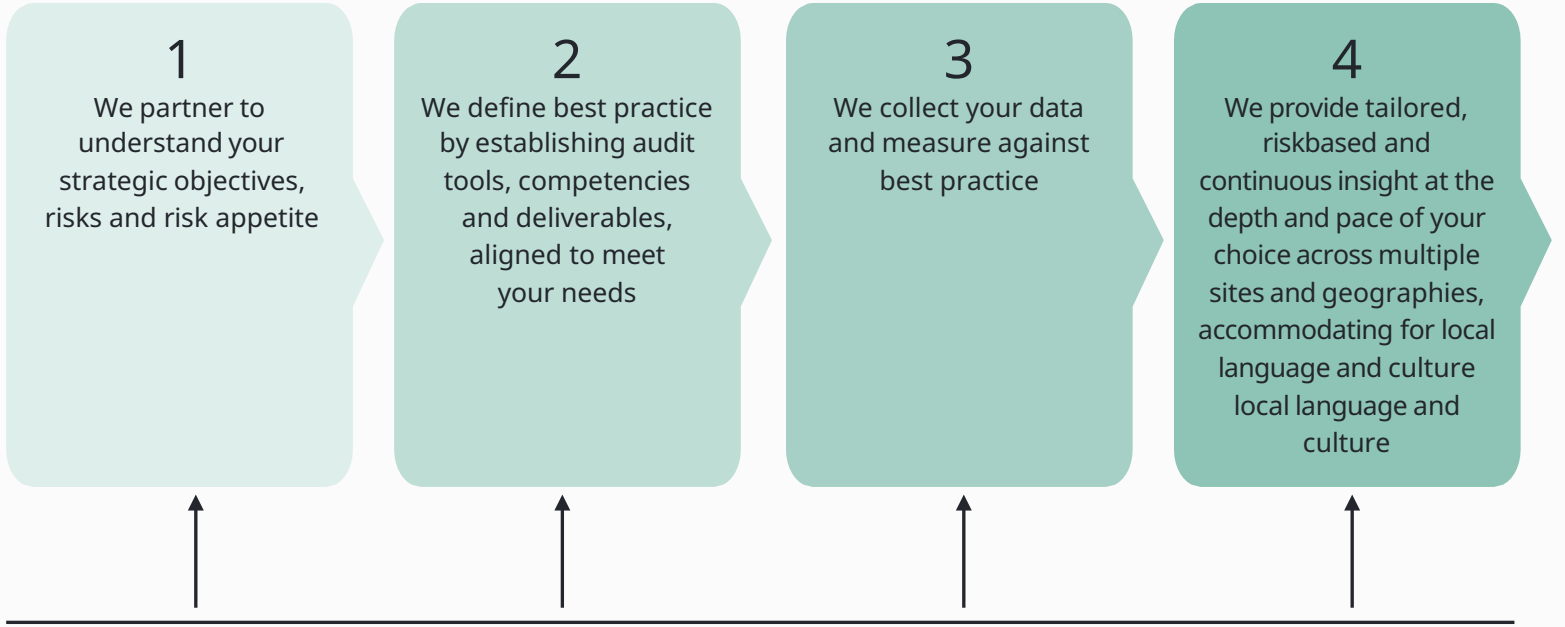
Drive infosec excellence and increase digital trust

BSI's audit programmes can help organizations like yours drive digital trust by overcoming cyber and infosec vulnerabilities across your organization and supply chain

We'll partner with you to understand your strategic objectives and your current risk exposure based on your business practices. For this we can create a tailored audit programme to help you embed and maximize opportunities in line with your business strategy, while meeting all relevant legal and regulatory cybersecurity disclosure requirements. It is also formed in a way that can scale and embed across your whole global organization and supply chain.

Drive infosec excellence inside and outside of your organization through:

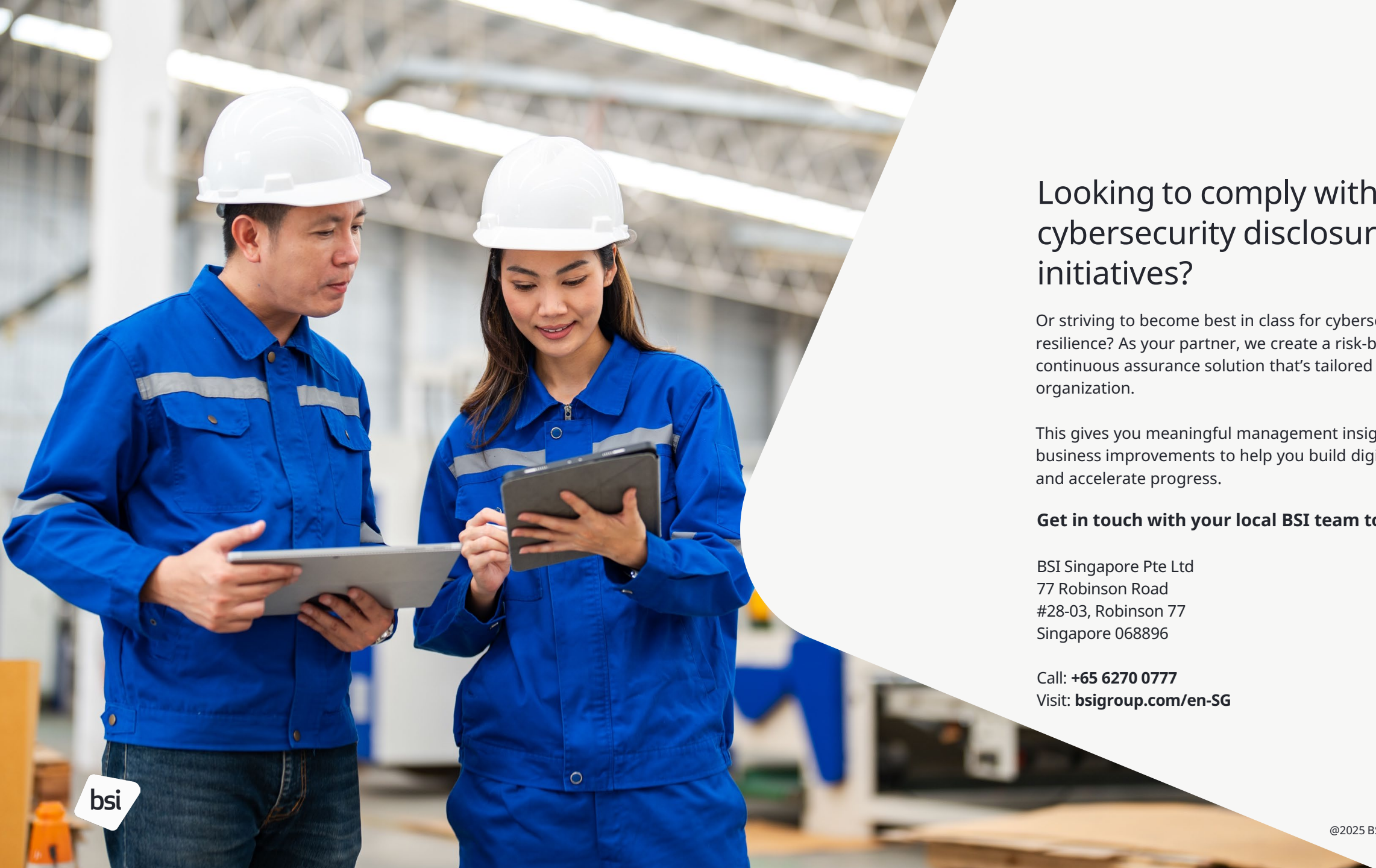
- Aligning to business strategy
- Identifying vulnerabilities
- Evaluating compliance
- Assessing security controls
- Third-party risk management
- Incident response planning
- Continuous improvement
- Enhancing awareness and training



bsi Connect

Data-driven insights
Our Connect tools enable you to collect, analyse and review data to drive business improvement, uncover opportunities, build trust and accelerate progress.

Compile audit findings from programmes, locations, and projects in one central tracking tool, create uniform metrics across your organization and provide easily accessible data and insights to drive business improvements that are measurable and tangible.



Looking to comply with new cybersecurity disclosure initiatives?

Or striving to become best in class for cybersecurity resilience? As your partner, we create a risk-based and continuous assurance solution that's tailored to your organization.

This gives you meaningful management insights and business improvements to help you build digital trust and accelerate progress.

Get in touch with your local BSI team today.

BSI Singapore Pte Ltd
77 Robinson Road
#28-03, Robinson 77
Singapore 068896

Call: **+65 6270 0777**
Visit: **bsigroup.com/en-SG**