BSI Cybersecurity and Information Resilience

Protecting your information, people and reputation

bsi.

...making excellence a habit.™

BSI Cybersecurity and Information Resilience

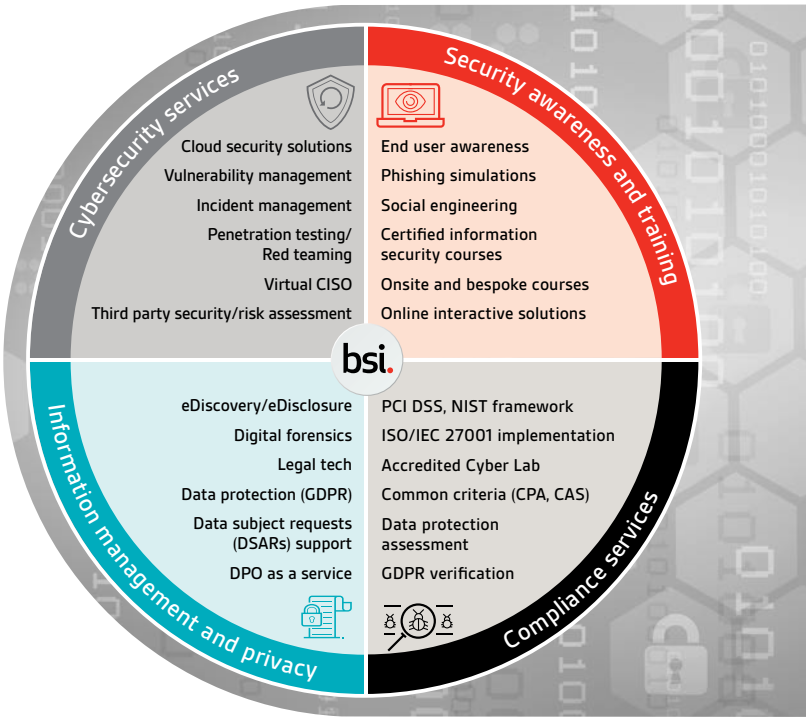
Protecting your information, people and reputation

Organizational Resilience – "A resilient organization is not one that merely survives over the long term but flourishes – passing the test of time." **– Howard Kerr, Chief Executive, BSI Group.**

Information Resilience – a domain of Organizational Resilience, empowers organizations to safeguard its information – physical, digital and intellectual property – throughout its lifecycle from source to destruction. This requires the adoption of information security-minded practices enabling stakeholders to gather, store, access and use information securely and effectively.

Achieving **Information Resilience** requires four interconnecting sub-domains to be addressed with strategies, plans and actions.

1. Cybersecurity
2. Information management and privacy
3. Security awareness and training
4. Compliance to requirements



BSI Cybersecurity and Information Resilience (CSIR) – helps organizations achieve this state of enhanced and sustainable **Information Resilience** through its integrated and woven sets of products and services:

- **Cybersecurity services:** with the proliferation of data breaches and malicious attacks, organizations need to employ the most proficient and best in class cybersecurity strategy available. This ranges across a broad spectrum of testing and vulnerability management services, from penetration testing to gold standard Red Teaming (CREST Approved). Within these services, BSI also provides a host of cloud security solutions, from web security and cloud access security brokerage to identity access management and data protection in the cloud.
- **Information management and privacy:** with the initiation of GDPR, privacy management and data protection has never been under so much scrutiny. Organizations need to be able to be compliant, transparent, open and fair in what they do with personal identifiable information (PII). Organizations need to have controls in place for how they acquire information – *do they have consent?* The use of the data – *do they have permission?* The archiving and destruction of data – *the right to be forgotten and erasure?* When an organization suffers a breach, BSI provides forensic capability to identify where the breach occurred and if the data was compromised.
- **Security awareness and training:** untrained employees – the weakest link in your cybersecurity defence. According to research, 91% of cyber-attacks start with a phishing email. BSI implement robust, agile and compliant training modules and courses to ensure that your weakest link can become your strongest asset in remaining vigilant and resilient to the omnipresent threats. Additionally, BSI offer bespoke, customized, online, inhouse and classroom-based certified training across a mix of information security, cloud security and data protection courses.
- **Compliance services:** from PCI DSS to NIST framework, Cyber Lab certification to ISO 27001 implementation, BSI enables organizations to ensure compliance through our knowledge of the standards and regulatory landscape, with our highly experienced teams of consultants.

Cybersecurity services

Given the cyberthreat landscape, organizations need the correct protocols, policies and procedures in place to keep their information safe, data secure, infrastructure robust and ultimately, to enable an enhanced state of resilience.

Vulnerability management

Designed to identify weaknesses in IT systems, our vulnerability management assessment provides you with a snapshot of your exposure to exploitable vulnerabilities. The process ensures that known weaknesses are identified and addressed in a timely manner.

Our consultants perform a peer review of all vulnerabilities identified, ensuring that the recommended solutions are tailored to your needs and that false positives are removed before reports are released.

Assessments can be performed periodically to ensure you receive continuous updates and remain compliant with industry security standards.

Penetration testing

A penetration test involves the simulation of an attack against an organization's IT assets. At BSI, we examine IT systems for any security issues before they are exploited by an attacker who may wish to disrupt the confidentiality, availability or integrity of a network, application, or associated data.

As approved global CREST penetration testers, our CHECK qualified consultants replicate the mind of a malicious attacker to provide high quality penetration testing across web and mobile applications, and internal, external and cloud infrastructure. Our test reports are clear, concise and provide practical remediation guidance.

Incident management

Implementing an incident response programme enables organizations to quickly react and limit the impact of a security incident.

As a CREST certified incident response organization, we prepare you with the necessary tools, policies and processes to:

- proactively detect a breach or incident
- take the necessary defensive action to contain a breach, and
- reinstate controls

BSI provides real-time support in the event of an attack (e.g. malware) to quickly minimize the impact to your business.

Cloud security solutions

BSI offers a host of cloud security solutions, from web security and cloud access security brokerage to identity access management and data protection in the cloud. We partner with leading cloud technology vendors to provide tailored security solutions to our clients.

125 million threats blocked per day

Secure internet and web gateway

A global cloud-based information security company that provides internet security, web security, next generation firewalls, sandboxing, SSL inspection, antivirus, vulnerability management and granular control of user activity in cloud computing, mobile and Internet of Things environments.

Key features

- Complete cloud security stack: includes Web and URL Filtering, Sandboxing, Cloud Firewall, CASB and DLP
- Unlimited capacity: with over 100 data centre locations, performance is always fast, and you'll never run out of capacity
- Full SSL visibility: unlimited inbound and outbound SSL inspection
- Fully integrated: enjoy integrated policies and contextual threat visibility from day one

Together is power.

The only **CASB** solution that is ranked as **a leader** in all three reports from **IDC, Forrester** and **Gartner**

Cloud access security broker

Helps the world's largest organizations unleash the power of the cloud by providing real-time protection for enterprise data and users across all cloud services.

Key features

- Visibility: continuously discovers cloud service usage, leveraging the world's largest and most accurate cloud registry
- Threat protection: analyses cloud activity, developing an accurate and continuously updated model of user behaviour
- Compliance: identifies sensitive data in motion or at rest in cloud services to meet your compliance requirements
- Data security: enforce data-centric security policies including encryption with your own keys, contextual access control and information rights management

Named a leader in the inaugural Gartner magic quadrant for **Access Management**, Worldwide (2017)

Identity management

Provides secure identity management, multi-factor authentication and single sign-on to any application, whether in the cloud, on-premises or on a mobile device. Join the millions of global employees that use Okta every day to quickly and safely access their apps.

Key features

- Decreases IT costs while increasing operational efficiency
- Provides services to enable the business to grow faster
- Secures your environment by securing your users' identities
- Connects all your apps in days, not months

Druva is **trusted** by over 4,000 global organizations, and **protects** over 40 PB of data

Data protection in the cloud

Druva provides a single pane of glass for protecting, preserving and discovering information across endpoints and cloud applications. Shield Office 365 data from unforeseen risks – close the gaps in recovery, visibility and governance.

Key features

- Accidental deletion: ensure your critical Office 365 data is safe from user error
- Ransomware: full self-service data recovery after ransomware attack
- Data governance: single access point for compliance monitoring, archiving and eDiscovery
- Endpoint backups: provide governance via visibility into data stored on corporate users' devices

Information management and privacy

eDiscovery (eDisclosure) and forensics

"eDiscovery or eDisclosure refers to the process by which Electronically Stored Information (ESI) is sought, located, secured and searched with a view to its use as evidence in a criminal or civil legal dispute."

BSI provides eDiscovery/eDisclosure, digital forensics, and litigation support services to in-house counsel, legal firms, corporations, and government bodies. We understand the challenges that eDiscovery presents and the unremitting investment it demands. We help solve a range of legal and regulatory issues concerning litigation, internal investigation, regulation, risk and compliance, as well as moving eDiscovery in-house.

Legal tech

Our team offer a range of delivery models to overcome the challenges of current legal reviews and evidence sources through the use of legal tech and state of the art eDiscovery solutions.

- Managed service
- On-site service
- Enterprise solution

eDiscovery implementation

We identify the right balance of in-house and externally managed support across your entire process. Whether you apply the Electronic Discovery Reference Model (EDRM) or similar, we recommend how to allocate personnel, processes and technology solutions.

- Implementation of protocols for collecting and preserving ESI
- Identification of relevant data sources
- Process, review, and analysis of data

Digital forensics

Increased digital storage has led to an escalated demand for forensically sound digital investigations. We have the expertise and services to support your organization for investigations.

- Computer and document forensics
- IP and data theft, data misuse and fraud investigation
- Data acquisitions and mobile device analysis

Incident response/Digital forensics

If your organization suffers a data breach, how will you react? How can you find out if any Personally Identifiable Information (PII) has been affected? We help our clients by using the principles of incident response and forensics fields to manage an investigation into the breach, mitigating a possible breach of GDPR.

Data Subject Access Requests (DSARs)

Data subject requests are not new, however with the introduction of GDPR the process for EU citizens to request data searches has simplified, leading to a significant potential rise in the demands placed upon organizations. Through our expertise and discovery solutions, we assist organizations to fulfil any requests imposed and help to identify, manage and present the relevant data, saving you time and cost.

General Data Protection Regulation (GDPR) and privacy

The EU GDPR came into effect on 25 May 2018, placing significant legal responsibilities on organizations that collect, store or process data. The following obligations are enforced on organizations in order to protect the personal data of EU citizens:

1. **Appointment of a Data Protection Officer (DPO)**

   Organizations may be required to appoint a DPO. The DPO must be independent, have expert knowledge of data protection and report directly to the Board of Directors.

2. **Mandatory notification of a data breach**

   Organizations are required to report a data breach to the relevant supervisory authority within 72 hours of becoming aware of the breach. Notification to affected data subjects may also be required.

3. **Ensure transparency**

   Data subjects must be fully and specifically informed at the point of collection on all purposes for which data is used. Data subjects may also remove their consent at any time, and for any reason.

4. **The right to erasure (Right to be forgotten)**

   When an individual no longer wishes for their data to be processed and there are no legitimate grounds for retaining it, the data must be deleted.

5. **Portability of data**

   Data subjects are able to transfer their personal data from one data controller to another without hindrance from the original controller.

6. **Privacy by design**

   Article 25 stipulates that data protection should be designed into the development of business processes and technology solutions.

7. **Significant fines**

   There are two tiers of fines. The first tier is a fine up to €10 million or up to 2% of annual worldwide turnover. The second tier is a fine up to €20 million or up to 4% of annual worldwide turnover.

Data Protection Officer as a Service

The DPO is an important leadership role within an organization's governance structure and its data protection accountability framework as defined by the GDPR. However, appointing an in-house DPO may not be feasible. Our outsourced DPO and Privacy Officer services enable organizations to implement a successful data protection programme so you can continue to focus on core activities. Our services include:

Data Subject Requests

Planning, designing and implementing effective procedures to respond to data subject requests including the right of access, right to be forgotten, right to portability and right to objection / restriction.

Personal Data Breach Support

Developing a personal data breach response plan, and offering real-time support to organizations when a personal data breach is identified.

Data Protection Impact Assessments (DPIAs)

Reviewing key data flows, screening projects and activities to determine whether DPIAs are necessary in line with the GDPR. Monitoring ongoing DPIAs, using PACE (Privacy Assessment Coverage Engine); an automated, self-assessment, SaaS based profiling and reporting solution, helping data guardians assess and improve current data use activity in line with privacy requirements and best practice.

Data Protection Awareness Training

Training options that help your organization's management and employees understand their data protection obligations, including online interactive training to educate all end users on the importance of information security.

Compliance services

Across all industries, regulatory compliance requirements are becoming more demanding and complex. Legislation is evolving, bringing increased accountability for organizations that are already heavily regulated. Through our Accredited Cyber Lab, we provide hardware, software, services and embedded systems testing across a range of regulatory requirements.

PCI DSS audit and advisory services

The Payment Card Industry Data Security Standard (PCI DSS) covers the fundamental aspects of information security and extends through the people, processes and technologies involved in payment card processing systems.

With over 20 Qualified Security Assessors (QSAs), BSI will lead you through the PCI journey from initial review to full alignment in the most efficient and least intrusive manner possible, allowing your business to continue operating while maintaining a secure payment processing environment.

Our PCI DSS consultancy services include:

- PCI DSS scope determination and scope reduction services
- PCI DSS gap analysis and prioritized action planning
- PCI Self-Assessment Questionnaire (SAQ)
- PCI DSS Report on Compliance (ROC) audit
- P2PE implementation assessments
- Penetration testing and vulnerability scanning services

PCI Security Standards Council®
QUALIFIED SECURITY ASSESSOR™

BSI's PCI DSS license covers

- CEMEA
- EU
- USA
- APAC

Assess

- PCI workshops
- SAQ validation
- Prioritized action plans

Implement

- Security controls
- Policies and procedures
- Process improvement
- Log management solutions

Audit

- Remediation check
- Pre-audit
- Onsite QSA audit
- Compliance reporting
- PCI DSS attestation of compliance

Maintain

- Penetration tests
- Vulnerability scans
- Risk assessments
- Security training
- Code reviews
- Customer support

bsi. **PCI DSS compliance** PCI

Accredited Cyber Lab services

As an ISO/IEC 17025 accredited cyber lab and official assessment partner of the National Cyber Security Centre (NCSC), BSI provides a wide selection of evaluations against both commercial and government standards. Our evaluators test hardware, software, services, and embedded systems against relevant client requirements to provide reassurance to the required level. We also use our in-house expertise to develop customized assessments to help you get the very best security assessment for your product.

UKAS TESTING

8237

Accredited to ISO/IEC 17025:2005

Commodity Assured Service (CAS)

CAS for Telecoms

CAS(T) certification is required for any organization that provides connectivity services to public sector bodies.

In order to achieve certification, the service provider must demonstrate compliance with the "Security Procedures Telecommunications Systems and Services" standard, which is based on the ISO/IEC 27001 standard.

CAS for Sanitisation

CAS(S) certification allows organizations to provide secure data wiping and destruction services for public sector bodies.

To achieve certification, the service provider must demonstrate compliance with the HMG IA Standard No. 5 for secure sanitisation, as well as fulfilling the requirements for training, auditing, and secure handling of protectively marked material.

Our experienced CCP Auditors will assess service providers against the CAS service requirement for sanitisation and destruction services up to and including TOP SECRET protective marking.

Commercial Product Assurance (CPA)

CPA provides assurance of security products developed by commercial companies.

The products can be anything from a web application firewall to a smart meter, and they are assessed using a combination of document review and interactive security testing.

Our evaluation team has extensive experience in both commercial and government sectors. We have also worked with NCSC to develop CPA security characteristics for new product types.

Common Criteria (CC)

Common Criteria is an internationally established certification scheme for assessing products across 15 categories, which is recognized by 28 countries.

It provides formal recognition that a product meets the functional claims regarding its security features, defined by the developer or sponsor of the product in the 'security target' document.

Tailored Assurance Service (CTAS)

CTAS evaluates the security of a system, product, or service.

The assessment addresses specific risks highlighted by accreditors and system owners, to inform their risk management decisions. The scope and range of evaluation activities is determined based on your individual requirements for risk management.

Our CTAS team has experienced CHECK Team Leaders and CCP professionals to perform the testing and auditing for CTAS evaluations.

> "iStorage had a requirement for testing our data storage solutions. These solutions are ultra-secure, PIN activated and hardware encrypted in the form of a desktop HDD, portable HDD, and portable SSD; with a wide range of capacities. The BSI Cyber Lab specialised evaluation team supported us in achieving our Commercial Product Assurance (CPA) certification, providing evaluation of our security products. The end-to-end process provided by BSI as trusted evaluators in this space was invaluable for iStorage and thanks to the hard work and dedication, we successfully received our CPA certification from the National Cyber Security Centre (NCSC)."
>
> **John Michael, C.E.O iStorage Limited**

Security awareness and training

End user security awareness

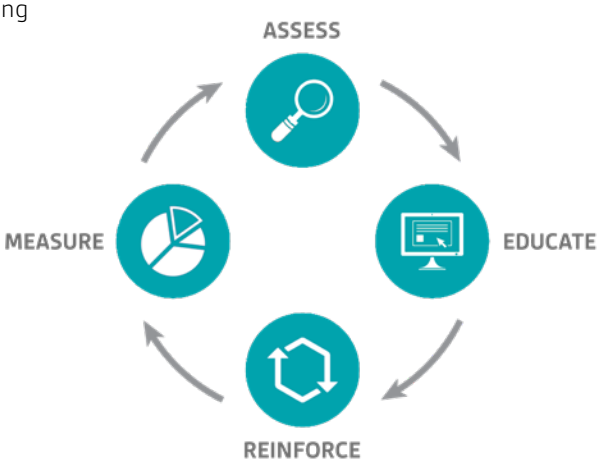
To protect your organization's information, preparation is vital. In any organization's security chain, employees can be the weakest link – but a well trained workforce can also become your first line of defence. Investing in your people gives them the knowledge to protect your information. With our range of online and on-site training courses, we can provide the skills to build resilience around your information security management.

Online interactive training solutions

With breaches increasingly being linked to employee behaviour, an organization's security programme needs continuous improvement and updating. We partner with a Gartner-recognized leading security awareness training solution to provide interactive and memorable cybersecurity awareness training for your end users.

Key elements:

- 30+ interactive and engaging training modules
- Simulated phishing attacks - quickly and easily send phishing assessments and track user interaction
- Knowledge assessment tool – assess cybersecurity awareness beyond phishing



On-site bespoke training

We offer a range of on-site security awareness training programmes to promote changes in employees' security attitudes and behaviour.

Our on-site training demonstrates cyber-attacks and social engineering, focusing on how individual efforts are the difference between improving overall information security in an organization, or possibly exposing the organization to potentially devastating risks.

wombat security
a division of proofpoint.

Results

Organizations have used our solution to reduce successful external phishing attacks and malware infections by up to 90%

Modules covered:

- Anti-phishing
- Email security
- Ransomware
- GDPR
- USB security
- Social engineering
- Data protection and destruction
- Password security
- Security beyond the office
- Security essentials
- URL training
- Mobile device security
- Mobile app security
- Physical security
- Safer web browsing
- Payment Card Industry Data Security Standard (PCI DSS)
- Personably Identifiable Information (PII)
- Protected health information

Training courses

Whether you are seeking a practical workshop or international certification, our courses help you gain the knowledge and skills required to enhance your organization.

In-company training – structured training, delivered in-house

You can select any course from our extensive range and have it delivered to your team on-site, or even request a bespoke course.

Fundamentals of General Data Protection Regulation (GDPR)

Our one day foundation, non-technical course for both technical staff and general management interested in learning about GDPR compliance.

GDPR Implementer/Auditor Self-Assessment

A two day course aimed at stakeholders within organizations who are accountable for ensuring compliance with GDPR; will enable you to start a self-assessment within your own organization.

Certified Information Privacy Professional Europe (CIPP/E)

A two day course examining industry best practices in privacy compliance concepts of data protection and trans-border data flows, the CIPP/E covers critical topics including the EU-U.S. Privacy Shield and GDPR.

Certified Information Privacy Manager (CIPM)

A two-day course that enables you to develop, implement, and measure a privacy programme framework while utilizing the privacy operational lifecycle: access, protect, sustain and respond.

Certified Information Security Manager (CISM)

An intensive four-day training based on the ISACA framework, providing the knowledge to develop and manage a resilient information security programme.

Certified Ethical Hacker (CEH)

A five day practical course giving you hands-on lab experience and allowing you to learn about the tools used by real attackers. You will have the opportunity to scan, test, hack and secure your own system to improve the resilience of your organization.

We have a range of course offerings:

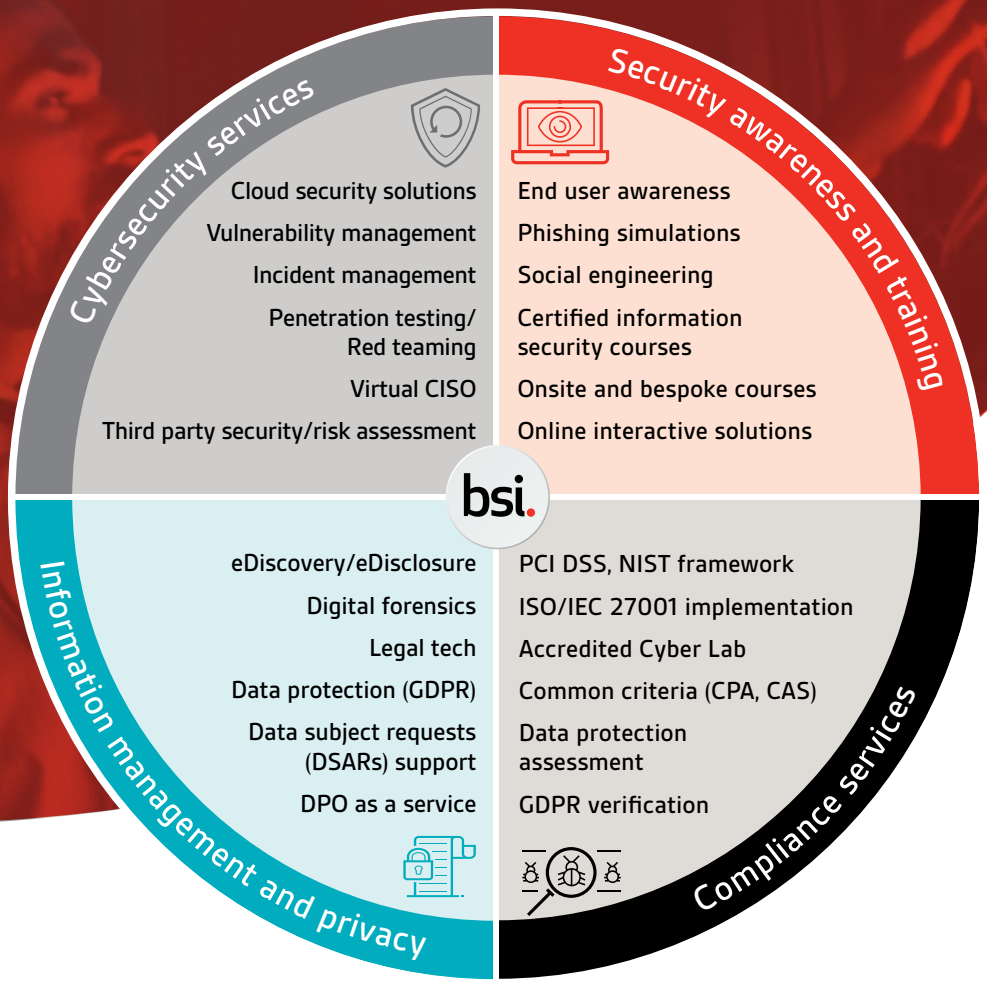
- Security Foundations
- Certified Information Systems Security Professionals (CISSP)
- Incident Response for Managers and Data Protection Officers
- Advanced Hacking: The Weaponised Cyber Range

Contact us for our full listing.

BSI Cybersecurity and Information Resilience

Protecting your information, people and reputation

BSI Cybersecurity and Information Resilience helps you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that affect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:



Our expertise is accredited by:

CREST · PCI Security Standards Council QUALIFIED SECURITY ASSESSOR · CYBER ESSENTIALS · CREST STAR · CHECK IT Health Check Service

Find out more

bsi.

UK

Call: +44 345 222 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com/cyber-uk

IE/International

+353 1 210 1711
cyber.ie@bsigroup.com
bsigroup.com/cyber-ie

Copyright © 2018 The British Standards Institution. All Rights Reserved.