BSI Digital Trust – Digital Risk and Advisory (DRA) Service

G-Cloud 14 Service Description

Supplementary information document

Expiration of Commercial Offer

This proposal and pricing expire in 20 days from receipt.

Statement of Confidentiality

This proposal, associated quotation pricing, and functionality description in whole and in part is considered confidential information

By Royal Charter

06 May 2024

Version	Description	Author	Date
1.0	Final version	Joe Halberda	06/05/2024

Contents

Service Overview

Service summary

BSI Cyber Risk & Advisory (CRA) will support you in counteracting the threat of global cybercrime. We have invested in expanding our global expertise to provide services to meet your business' needs and enable a focused response to cyber threats and improve resilience around your critical information and IT infrastructure.

Key features

Key features of the BSI CRA service are as follows:

- ISO 22301:2019 Business Continuity Management Services (BCMS)
- ISO 27001:2013 Information Security Management System (ISMS)
- ISO 27005:2018 IT Risk Management Framework Development
- Managed Security Service
- NIST Threat Based Mitigation and Capability Assessment
- PCI DSS Qualified Security Assessor (QSA) Consultancy
- Security Architecture Review and Assessment
- Security Assurance Service (supported by CCP)
- SOC 2 Type II Assessment and Attestation Report
- Virtual Chief Information Security Officer (vCISO)

Key benefits

Key benefits of the BSI CRA service are as follows:

- ISO 27001 & ISO 9001 certified consultancy and reporting
- Vendor-agnostic, information security consultants providing independent and impartial services
- Improved compliance using risk-based approaches without compromising internal resources
- Flexible, scalable, services facilitating regular consultancy and on-demand support
- Significant knowledge of frameworks, methodologies and industry best practices
- Specialist advice and pragmatic recommendations tailored to business context
- Proven methodologies and templates to support early improvement activities
- Cross-domain security specialisms to support provision of holistic services
- Professional certifications in CISSP, CCP, CCSP, CISM, BCI, ISO
- Experienced engaging with stakeholders at IAO and SIRO level

Service Description

ISO 22301:2019 Business Continuity Management Services (BCMS)

Organisations rely on meeting product and service delivery agreements. The challenge is to ensure that, if a disruption occurs, an organisation can still meet these agreements and mitigate the risk of operational impact, reputational damage, or financial loss. Arrangements for business continuity management can be diverse and complicated including internal operational functions, business elements, external partners, service providers, suppliers, supply chain and support contracts.

BSI provides tailored consultancy services supporting organisations to mature their business continuity, disaster recovery, and operational resilience capabilities. BSI's highly experienced and qualified consultants are certified in CISSP, CCP, CISM, ISO 22301, and Business Continuity Institute (BCI). BSI can support the implementation of frameworks, policies, objectives, solutions and plans to improve the maturity of business continuity management.

BSI can support an organisation to manage operational disruptions through the identification of critical services, developing business risk & impact assessments, plans and testing schedules, and integrating into existing management systems that support alignment to ISO 22301 or BCIs' Good Practice Guide.

BSI can also advise on leadership and governance, conduct gap analysis, assess impacts and risks, aid in the development of plans and improvement solutions, provide employee training, and perform testing of plans and solutions to give your organisation and its customers the assurance it requires. BSI can support the ongoing review of your business continuity management by carrying out internal reviews, establishing measurement monitoring activities aligned to strategic objectives, and facilitating continual improvement, to ensure that risks have been identified, and that plans to mitigate are progressed and effective.

Features

- Identification and categorisation of business services and their criticality
- Review and workshop of current business continuity maturity and readiness
- Provide advice on applicable frameworks and best practice standards
- To support implementation of relevant frameworks, policies, plans and processes
- Support development of business continuity plans and testing approach
- Support undertaking of business impact assessments and business continuity exercises
- Support identifying single points of failure and inadequate resilience measures

Benefits

- Reduces operational impact of unplanned disruptions to business services
- Managing service disruptions reduces risks to reputation damage and operations
- Specialist unbiased advice and pragmatic recommendations tailored to business context
- Experienced professional advisors certified in CISSP, CCP, CISM, ISO22301, BCI
- UK-based consultants with extensive public sector and industry experience
- Proven methodologies and templates to support early improvement activities

- Proportionate planning advice commensurate with financial and business operations risk

ISO 27001:2013 Information Security Management System (ISMS)

BSI offers support for the implementation of ISO/IEC27001 and a range of HMG Accreditation approaches for cloud services and service compositions including cloud services in support of transition and ongoing operation. The service is flexible and can range from strategic advice, through to the implementation of policies and procedures. ISO/IEC 27001 helps make businesses more resilient and responsive to threats to information security.

It helps keep your business secure so you can focus on doing "business as usual" whilst clearly showing clients and suppliers your commitment to protecting information.

Today, in this highly interconnected world, it is important for organizations to ensure their operations are run efficiently and that data is secure.

The Government sector process large volumes of personal and other sensitive data, and relies on the confidentiality, integrity and availability of its systems to support the delivery of core business functions. Increasingly, it is leveraging the benefits of using Cloud computing, with services being commoditised and scalable, but this also brings new security challenges for the client.

BSI offers a full range of NCSC Certified Cyber Professional (CCP) roles to assure cloud services through ISO 27001 certification and public sector accreditation schemes.

BSI is experienced in conducting Information Assurance (IA) audits as well as reviewing security policy documentation. We have a large team of experienced ISO/IEC 27001 Lead Auditors, as well as CCP IA Auditors and PCI DSS QSAs.

We frequently undertake process audits and policy reviews of key policies and procedures, with a view to identifying any missing policies or any requiring updates, according to the client's security requirements and the environment in which they operate.

BSI offers consultancy for implementing ISO 27001 Information Security Management Systems (ISMS), as required for certification. The approach typically involves:

- Defining scope of the ISMS
- Gap Analysis to identify required improvements
- Developing a Risk Management framework
- Information Security Policy, Standards and Guideline creation
- IT / Cyber Security advice on appropriate controls
- Audits, either pre-certification or within an ongoing ISO 27001 programme.
- Training and Awareness
- Security Incident Management and Response
- Disaster Recovery (DR)
- Supply Chain Security Management

Features

- Information Security Management System (ISMS strategy, development and implementation
- Produce and agree ISMS Scope and Policies
- Risk assessments methods supported include IS1, IRAM, IRAR and CRAMM
- Carry out Risk Assessment and produce Risk Assessment Report
- Conduct initial Gap Analysis and produce the Statement of Applicability (SoA)
- Establish and operate Security Forums including Terms of Reference (ToR)
- Produce risk acceptance and risk treatment plan and ISMS procedures
- Conduct internal compliance assessments and audits
- Provide operational security management, including incident and protective monitoring management
- Review operational security reports and attend security forums / management reviews
- Security incident management and investigation

Benefits

- Service suitable for public, private, community and composed cloud solutions
- Experience with assurance approaches including MoJ, Policing, DfES and PSN
- Experience with solutions including Skyscape, AWS, Azure and Office 365
- Service resources have worked with multiple UK public sector clients
- Consultants qualified as ISO27001 Lead Auditors/Implementers and CCP IA Auditors
- Carried out by qualified consultants
- ISO 27001 Lead Auditors / Implementers
- CCP Security and Information Risk Advisor (SIRA)

ISO 27005:2018 IT Risk Management Framework Development

ISO/IEC 27005 provides guidelines for the establishment of a systematic approach to Information Security risk management which is necessary to identify organizational needs regarding information security requirements and to create an effective information security management system. Moreover, this international standard supports ISO/IEC 27001 concepts and is designed to assist an efficient implementation of information security based on a risk management approach.

ISO 27005 is the international standard that describes how to conduct an information security risk assessment in accordance with the requirements of ISO 27001.

Risk assessments are one of the most important parts of an organisation's ISO 27001 compliance project. ISO 27001 requires you to demonstrate evidence of information security risk management, risk actions taken and how relevant controls from Annex A have been applied.

ISO 27005 is applicable to all organisations, regardless of size or sector. It supports the general concepts specified in ISO 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

Features

- BSI can assist in identifying and assessing risk
- Development and implementation of strategy and policy
- Understanding risk likelihood and the consequences for the business
- BSI can provide staff awareness training of risks and the actions being taken to mitigate them
- Development, implementation and training for policy and procedures

Benefits

- Proactively improve operational efficiency and governance
- Apply management system controls to risk analysis to minimize losses
- Respond to change effectively and protect your business as you grow
- Build stakeholder confidence in your use of risk techniques
- Improve management system performance and resilience

Managed Security Service

BSI offers active, on-going information security management to protect cloud services. The service can be tailored to provide support for planning, implementation, migration and ongoing operation. The service can engage with accreditors or business risk owners to meet client needs.

The Government sector process large volumes of personal and other sensitive data, and relies on the confidentiality, integrity and availability of its systems to support the delivery of core business functions. Increasingly, it is leveraging the benefits of using Cloud computing, with services being commoditised and scalable, but this also brings new security challenges for the client.

BSI offers active, on-going management of information security to ensure information assets are appropriately protected and that legal and regulatory compliance requirements are met. BSI offer:

- Risk assessment, to identify the real risks faced by each organisation
- Consultancy on securing systems and services, proportionate to the risks
- Gap analysis or audit of compliance with recognised security standards such as ISO 27001
- Advising on or producing a business case for introducing security controls
- Security incident prevention and management

The benefits of using BSI Managed Security Services include:

- Increased compliance and support in demonstrating Information Assurance Maturity Model in a Cloud environment, whilst reducing risks to reputational damage

- Reduced costs and timescales in achieving and maintaining compliance and certification tried and tested methodologies, and security resource can be used "on demand" rather than having a large in-house security team
- Allows Government-based organisations to focus internal resources on the core activities of the department, whilst security management functions are maintained by a specialist, independent information assurance organisation
- Extensive experience of delivering and managing HMG Cloud-related security management functions across Government
- Services can be tailored to suit requirements (e.g. provision of all security management functions, or just specific services to supplement departmental internal resource teams)

Features

- Developing and gaining approval for accreditation and security strategy
- Operational auditing support against IAP, SPF, CMAT, CPNI and PASF
- Accreditor service option offers direct engagement with business risk owners
- Operational Security Management including incident management and protective monitoring management
- Provision and review of design and accreditation documentation
- Production of accreditation documents including conventional and lightweight RMADS

Benefits

- Service suitable for Public, Community, Hybrid and Private Cloud
- Experienced working with AWS, Azure, Skyscape and Office 365
- Flexible engagement with client accreditors or business risk owners
- Experienced engaging with business stakeholders at IAO and SIRO level
- Resources certified at CCP Senior and Lead levels
- Resources certified as SIRA, IA Auditor and IA Architect
- Service supports knowledge transfer and transition to client staff
- Vendor agnostic supplier providing unbiased independent advice

NIST Threat Based Mitigation and Capability Assessment

The National Institute of Technology (NIST) created the Cyber Security Framework (CSF), is a voluntary framework to provide organizations with guidance on how to prevent, detect, and respond to cyberattacks. It consists of standards, guidelines, and best practices to manage cybersecurity-related risk. Quickly becoming a globally recognized assessment, the framework provides a harmonized approach to cybersecurity.

As the leading independent certification body for information security, and a major contributor to the NIST framework, BSI has the specialist knowledge to help you validate your NCFS compliance, reduce risk and reassure your stakeholders. Our information and cybersecurity teams are regularly trained to ensure they have the latest information, understand best practice and continually develop their expertise to support

you through your NIST CSF journey. We can help you whether you're starting your business improvement journey or looking to enhance current knowledge and capabilities.

Features

- Threat Workshop
- Threat Workshop Analysis
- NIST Cybersecurity Posture Assessment
- NIST Threat Based Mitigation Capability Assessment

Benefits

- Helps you better understand, manage, and reduce cybersecurity risks, data loss, and the subsequent costs of restoration
- Enables you to determine your most important activities to deliver critical operations and service delivery
- Demonstrates that you're a trusted organization who secures your critical assets
- Helps to prioritize investments and maximize the impact of each dollar spent on cybersecurity
- Addresses contractual and regulatory obligations

PCI DSS Qualified Security Assessor (QSA) Consultancy

BSI is a leading independent Qualified Security Assessor (QSA) company, qualified and accredited by the PCI Security Standards Council to provide QSA services and assess compliance to PCI DSS. BSI's experienced team of QSAs have developed a "one-stop-shop" set of PCI DSS compliance services aimed at assisting both merchants and service providers to achieve and maintain compliance, which includes proven methodologies and document templates to support rapid, successful compliance quickly and effectively.

BSI supports PCI DSS compliance from initial scoping and planning of compliance programmes through to issuing full audit reports. BSI will work with clients to help manage their scope and control, as well as the cost and complexity of achieving compliance.

Our trusted methodology is defined by six key phases:

- Project Information & Scoping
- Gap Analysis and Risk Assessment
- Remediation Planning
- Remediation Activity
- Self-Assessment or Audit & Certification
- Compliance Management

This service portfolio is available across many industry sectors and, as part of an overall business as usual security strategy, it can also provide ongoing compliance maintenance by ongoing internal audit, security awareness training, remediation planning, and re-certification activities. BSI has large security testing and assurance teams with wide, varied experience to assist with providing increased compliance, whilst reducing risks to reputational damage or financial loss. BSI provides unbiased and independent information

security services, with holistic advice and recommendations with all reports reviewed in the context of ISO 27001 and 9001 certified environments.

Features

- Project Information / Scoping – architecture, card data flow analysis and processing of cardholder information
- Gap Analysis / Risk Assessment – report on PCI compliance using industry standard methodologies
- Remediation Planning: outlining / prioritising work, and resources based on inherit risks
- Remediation Activity: security policies, technical / security design, service management
- Audit / Certification: independent audit or support self-assessment as appropriate
- Compliance Management: assistance with ongoing management of compliance through:
    - Penetration tests and quarterly scans by our certified security testers
    - Ongoing internal audit and remediation planning
- Security Awareness Training
- Stakeholder Engagement including acquiring banks and payment brands
- Provision of remediation consultancy, including "trusted security advisor" services
- Re-certification audits

Benefits

- Carried out by PCI-DSS Qualified Security Assessors (QSA)
- Highly experienced UK-based senior and principal consultants, specialising in both the public and private sectors
- Proven methodologies and document templates to support rapid, successful compliance
- "One-stop shop" PCI-DSS compliance services to quickly achieve and maintain compliance
- Large security testing and assurance teams with wide, varied experience
- Reduced risk of delays as resource made available as required
- Increased compliance, whilst reducing risks to reputation damage
- Advice and recommendations given with a truly holistic security view
- ISO 27001 and 9001 certified, with all reports independently reviewed
- As independent information security specialists, we provide unbiased services

Security Architecture Review and Assessment

Security Architecture is the practice of designing computer systems to achieve security goals. It is a set of security principles, methods and models designed to align to organisation's objectives and help keep the organisation safe from threats.

As per National Cyber Security Centre (NCSC), Security Architecture is the practice of designing computer systems to achieve security goals.

The security goals are to:

- Make initial compromise of the system difficult
- Limit the impact of any compromise
- Make disruption or further compromise of the system difficult
- Make detection of a compromise easy

Features

- Designing or reviewing whether security controls for a computer system are suitable
- Researching and developing new techniques or tools to address more systemic security problems
- Advising technical leaders on cyber security when making strategic decisions
- Assessment can be risk, contract or compliance focused
- Assessment can include procedural and technical aspects

Benefits

- Assessment provides repeatable measures
- Assessment addresses business risks rather than individual technologies
- Consultants have experience designing, procuring and operating protective monitoring
- Flexible testing approach can be supported by qualified security testers

Security Assurance Service (supported by CCP)

The BSI Security Assurance Service can flexibly support organisations in ensuring their cloud solutions deliver and maintain compliance with a range of standards and governance approaches in used across HMG. BSI deliver the service with Certified Cyber Professionals (CCP).

The Government sector process large volumes of personal and other sensitive data, and relies on the confidentiality, integrity and availability of its systems to support the delivery of core business functions. Increasingly, it is leveraging the benefits of using Cloud computing, with services being commoditised and scalable, but this also brings new security challenges for the client.

BSI offers active, on-going management of information security to ensure information assets are appropriately protected and that legal and regulatory compliance requirements are met. We offer:

- Risk assessment, to identify the real risks faced by each organisation
- Advice and guidance on securing systems and services, proportionate to the risks
- Gap analysis or audit of compliance with recognised standards such as ISO 27001
- Advising on or producing a business case for introducing security controls
- Security incident prevention and management
- Production of risk management deliverables in a wide range of formats including conventional RMADS, lightweight RMADS used by several different departments and the cloud hosting providers

Features

- Supports compliance regimes including ISO27001, SPF, PSN, IRAR and PASF
- Risk assessment and management delivered by CCP SIRA
- Security architecture design and review by CCP IA Architects
- Operational Security Management including incident management and protective monitoring management
- Accreditation and certification deliverables produced and reviewed
- Internal audits undertaken to support certification and accreditation regimes
- Establish and facilitate Security Working Groups (SWG)
- Production and presentation of SIRO submissions and risk escalation cases
- Forensic investigation, incident management and incident response
- Delivering Business Impact Assessment (BIA) and Privacy Impact Assessment (PIA)

Benefits

- Service suitable for Public, Community, Hybrid and Private Cloud
- Experienced working with AWS, Azure, UK Cloud and Office 365
- Flexible engagement with client accreditors or business risk owners
- Experienced engaging with business stakeholders at IAO and SIRO level
- Resources certified at CCP Senior and Lead levels
- Resources certified as SIRA, IA Auditor and IA Architect
- Service supports knowledge transfer and transition to client staff
- Vendor agnostic supplier providing unbiased independent advice
- Can be resourced with HMG vetting at SC level

SOC 2 Type II Assessment and Attestation Report

A SOC 2 Type II attestation report is the gold standard for service organizations seeking to provide assurance to the enterprise marketplace that their organisations, products and services have appropriate information security and data privacy controls. BSI offers a variety of audit readiness services for clients who are pursuing a formal SOC report and attestation including protective monitoring strategy, implementation, operation and compliance assessments.

BSI will assist at every step of the way to ensure clients are fully prepared for formal audit activities. SOC 2 services include:

- **Scoping** – BSI will work closely with client management and stakeholders to properly identify all services/solutions to be considered in-scope for the SOC report. Additionally, we work with the service organization to identify all Trust Service Principles (TSPs) to be included in the SOC 2/3 report.

- **Planning** – BSI will work closely with your team to develop a customized project plan that takes into consideration all available resources (internal and external), competing initiatives, and organizational goals and objectives. This includes gap analysis covering technical, procedural, and physical aspects.
- **Implementation** – BSI will provide assistance and project management services as necessary to support all the activities defined above, with interim and operational security guidance and support. This includes development of accreditation materials, strategy, policy, remediation plans, and training plans.
- **Audit and reporting** – BSI will assist clients with pre-audit and audit activities. This includes coordination with the CPA firm that will perform the actual audit. This approach allows the auditor to be completely independent and provides a clear separation of duties.

BSI consultants hold CCP in multiple roles and have experience working with central government agencies, NHS, and Police forces.

Features

- Interim and operational security guidance and support
- Development and assurance of accreditation materials using client methods
- Development and implementation of strategy and policy
- Development of scopes and remediation plans
- Development, implementation and training for policy and procedures
- Protective monitoring strategy, implementation, operation and compliance assessments

Benefits

- Service suitable for public, private, community and composed cloud solutions
- Many consultants hold CCP in multiple roles
- Experience working with central government, NHS and Police forces
- Experience of pan-government/sector solutions (PSN, GCF, PNN)
- Experience of Office 365, Azure and Amazon Web Services (AWS)
- Experience of developing and implementing strategy and policy

Third Party Assurance Service

Organisations often rely on third parties to help support delivery of their services. The challenge is to ensure that these third parties safely process the organisation’s data, including personal and other sensitive information. BSI provides tailored assurance services to support organisations to obtain assurance of their third-party arrangements including partnerships, subcontractors, service providers, suppliers and supply chain contracts. BSI can support identification of relevant legislation, standards and best practice applicable to each outsourced service type.

BSI’s qualified consultants are certified cybersecurity professionals (CISSP, NCSC CCP, CISM, CIPPE), with extensive government, public sector, and wider industry experience, providing trusted advice. They can pragmatically assess third-party data processing risks (including residual risks) and advise on governance,

technical and organizational controls, and remediation measures, in order to drive compliance, enable innovation, support competitive advantage, improve security maturity, reduce reputation damage, and reduce regulatory fines. Third-party arrangements can be diverse and include partnerships, service providers, suppliers, supply chain and support contracts. Understanding the arrangements in place, especially data controller and data processor status, is crucial to ensuring that services are delivered with minimal risk. BSI can provide support for existing third-party arrangements as well as future procurement activity.

BSI can offer a range of services including support of compliance with applicable standards and legislation such as UK Government Supplier Assurance Framework, Data Protection Act 2018, General Data Protection Regulation, ISO 27001 etc. BSI can help to review, report and improve the maturity of third-party BAU services, as well as support the development or improvement of non-functional requirements, security policies, service provision model, remote access approach, training, and contract clauses.

Features

- Identification of existing third-party arrangements and their sub-contracts.
- Provide advice on applicable frameworks to manage third-party contracts.
- To support implementation of relevant frameworks, policies and processes.
- Residual risk assessment for each existing outsourced arrangement.
- Support development of non-functional requirements and contract clauses.
- Review of compliance against relevant legislation, standards and best practice.
- Identify appropriate and proportionate remediation activity to improve security maturity.
- Identify audit approach including independent third-party and self-assessment.
- Review and reporting of maturity of third-party BAU services.
- Identification of relevant legislation, standards, best practice for each service.

Benefits

- Improvement in third-party management maturity.
- Increased compliance reduces risks to reputation damage and regulatory fines.
- Specialist unbiased advice and pragmatic recommendations tailored to business context.
- Experienced professional risk advisors holding CISSP, NCSC CCP, CISM, CIPPE.
- UK-based consultants with extensive public sector and industry experience.
- Proven methodologies and templates to support early compliance activities.
- Scalable and available security cleared resources expedites successful project delivery.
- Significant experience using frameworks, methodologies and industry best practice approaches.
- Cross-domain security specialisms to support provision of holistic services.
- ISO 27001 and 9001 certified, with all reports independently reviewed.

Virtual CISO (vCISO)

The virtual CISO (vCISO) service option allows organisations to benefit from high quality, experienced, senior consultants and advisors who can assist with creating, developing, and operating their information and cybersecurity strategy. This offers a lower financial barrier to entry compared to hiring a full time CISO.

The vCISO role embeds senior security leadership into an organisation and brings the security lens to the organizations vision. The role hits the ground running whether in a small to medium size business or in a large enterprise with existing security functions in place. As the role is that of an external advisor, an objective view is always presented.

BSI have expert capability to supplement existing security teams in operationalising the culture of security into the Business As Usual operations and culture. Our approach to making the security journey successful is to work collaboratively with existing teams, ensuring that security is balanced in a meaningful way to facilitate delivery of business objectives, meet compliance obligations, and enable secure ways of working, without stifling innovation and rapid delivery.

The vCISO can deliver objective feedback on current risks and security maturity, as well as providing insight to the wider security landscape due to being involved in multiple industries and organizations. This will increase information security resilience and decreases the likelihood of a successful attack.

Features

- Minimum commitment, 1 day per month
- Time can be used flexibly within the month
- Rapid access to the team of BSI security professionals
- Benefit from BSI experience with many HMG departments
- Discuss questions by email, voice, video or site visit
- SIRA, IA Architect and other CCPs up to Lead level
- Access to PCI DSS QSA, DPO and CHECK qualified consultants
- Option for regular scheduled engagements and allocated consultant
- Named account manager

Benefits

- Rapid access to a range of specialist skills
- Experience working with MOD, Police and wider public sector
- Experience working with devolved administrations
- Risk Assessment and Management Advice
- Security Architecture Design and Design Review
- Product and Supplier evaluations, requirements development and review
- Data Privacy and PCI DSS QSA advice
- ITHC Scoping and Remediation advice
- Support with managing incidents
- Operational security and protective monitoring support