DATA SECURITY
A UBDS GROUP COMPANY

INFORMATION SECURITY SERVICES

For G-Cloud 15

January 2026

Classification: Public

CONTENTS

1. INTRODUCTION

3B Data Security is one of the UK's only cyber security providers fully assured by the National Cyber Security Centre (NCSC) to deliver CHECK penetration testing, cyber incident response, cyber incident exercising, and cyber advisory services.

NCSC assured across the board, CREST accredited, and dual-approved by the PCI Security Standards Council as both a Qualified Security Assessor (QSA) and PCI Forensic Investigator (PFI), 3B Data Security is trusted by UK government, regulators, and critical national infrastructure organisations to deliver security assurance at the highest level.

Using the same reconnaissance techniques as threat actors and red teams, 3B Data Security's consultants uncover risks others miss, rigorously challenge assumptions, and deliver clear, action-oriented reporting that enables organisations to secure systems, data, and services that underpin the public sector. This approach is underpinned by **Check. Challenge. Secure.** 3B Data Security's proven method for ensuring defences hold under audit, attack, and public scrutiny.

Backed by over 20 years of real-world experience in digital forensics and incident response, 3B Data Security provides confidence that security controls operate effectively under real-world conditions - not just in theory.

CHECK

We uncover the risks others overlook, using deep expertise and the latest threat intelligence.

CHALLENGE

We rigorously test every control, critique every assumption, and simulate real attacker tactics so nothing is left to chance.

SECURE

We help you close every gap, validate every fix, and prove your defences hold under audit, attack, or public scrutiny.

CERTIFIED AT EVERY LEVEL THAT MATTERS.

You can get in touch with us via: 3bframeworks@3bdatasecurity.com

Website: www.3bdatasecurity.ccom

LinkedIn: https://www.linkedin.com/company/3b-data-security

2. ISO9001 QUALITY MANAGEMENT CONSULTING SERVICES (DESIGN, IMPLEMENTATION, AUDITS, SUPPORT).

Delivering ISO9001 quality management system design, implementation, auditing and ongoing support to help organisations achieve and maintain certification. The service includes expert guidance, audit readiness, continuous improvement support and tailored quality frameworks to enhance efficiency, reduce risk and ensure compliant quality management.

KEY FEATURES

- Certified and retained certification-body auditors
- Expert ISO9001 implementation support
- Internal and external audit readiness guidance
- UK Public Sector and industry-specific expertise
- Ongoing post-certification quality improvement support
- Compliance-as-a-Service quality management support
- Tailored documentation and process development
- Integration support for multi-standard management systems
- Specialist guidance reducing compliance complexity

KEY BENEFITS

- Proven expertise in ISO9001 design and implementation
- Access to retained certification body auditors
- Ongoing post-certification support services
- Reduced cost and complexity for integrated systems
- Added value integration with Cyber Essentials and CAF
- Dedicated certified Lead Implementers and Auditors
- Knowledge transfer and team training
- Extensive Public Sector experience
- Trusted consultants deployed by UKAS certification bodies

3. ISO20000 SERVICE MANAGEMENT CONSULTING SERVICES (DESIGN, IMPLEMENTATION, AUDITS, SUPPORT).

Delivering ISO20000 service management system design, implementation, auditing and ongoing support to help organisations achieve and maintain certification. The service includes expert guidance, audit readiness, continuous improvement support and tailored service management frameworks.

KEY FEATURES

- Certified and retained certification-body auditors
- Expert ISO20000 implementation support
- Internal and external audit readiness guidance
- UK Public Sector and industry-specific expertise
- Ongoing post-certification service improvement support
- Compliance-as-a-Service service management support
- Tailored documentation and process development
- Integration support for multi-standard management systems
- Specialist guidance reducing compliance complexity

KEY BENEFITS

- Proven ISO20000 implementation expertise
- Access to retained certification body auditors
- Ongoing post-certification support services
- Reduced cost and complexity for integrated systems
- Added value integration with Cyber Essentials and CAF
- Certified Lead Implementers and Auditors
- Knowledge transfer and team training
- Extensive Public Sector experience
- Trusted consultants deployed by UKAS certification bodies

4. ISO22301 BUSINESS CONTINUITY SERVICES (DESIGN, IMPLEMENTATION, AUDITS, TABLETOP-TESTING, SUPPORT).

Delivering ISO22301 business continuity end-to-end services including design, implementation, tabletop testing and ongoing support. Helping organisations identify critical risks, strengthen preparedness, ensure compliance and maintain resilient operations during incidents or major disruptions.

KEY FEATURES

- End-to-end ISO22301 business continuity design
- Expert implementation of continuity frameworks
- Internal and external audit readiness guidance
- Tabletop testing and exercise development
- Compliance-as-a-Service continuity support
- Risk assessment and business impact analysis
- Tailored documentation for certification success
- Integration across multi-standard resilience frameworks
- Cyber incident response and recovery support

KEY BENEFITS

- Proven BC and DR implementation expertise
- Reduced downtime through structured planning
- Specialist BC/DR and incident response support
- Reduced cost and complexity for integrated systems
- Certified Lead Implementers and Auditors
- Knowledge sharing and training
- Extensive Public Sector experience
- Trusted UKAS-deployed consultants

5. ISO27001 INFORMATION SECURITY MANAGEMENT CONSULTING SERVICES (DESIGN, IMPLEMENTATION, AUDITS, SUPPORT).

ISO27001 ISMS design, implementation, audit and ongoing support services delivering compliant information security management. The service strengthens governance, reduces security risk and supports organisations in maintaining effective ISO27001-certified controls.

KEY FEATURES

- ISO27001-aligned ISMS design
- UK Public Sector delivery by certified consultants
- Internal and external audit support
- Tailored information security documentation
- Multi-standard framework integration support
- Security governance framework optimisation
- Compliance-as-a-Service ISMS support
- UKAS-retained public sector security experts
- Comprehensive risk assessment and treatment

KEY BENEFITS

- Strengthened security resilience
- Accelerated ISO27001 certification
- Improved audit performance
- Reduced internal compliance workload
- Integration with wider security frameworks
- Knowledge sharing and training
- Increased stakeholder confidence
- Expert risk management assurance

6. ISO42001 ARTIFICIAL INTELLIGENCE (AI) AUDIT AND ASSURANCE SERVICES.

ISO42001 AI audit and assurance services supporting safe, compliant public-sector AI. Independent assessment of AI governance, risk, data integrity and operational safeguards to demonstrate responsible AI practices and regulatory compliance.

KEY FEATURES

- ISO42001 auditors retained by UKAS bodies
- Senior AI governance and risk specialists
- Comprehensive AI governance and risk assessment
- Data quality and model lifecycle evaluation
- Alignment testing against ISO42001 requirements
- EU AI Act governance expertise
- Detailed audit reporting and remediation guidance
- Ongoing AI assurance support
- Integration with security and ethics frameworks

KEY BENEFITS

- Improved AI transparency and accountability
- Reduced AI-related risk
- Support for emerging AI regulation compliance
- Actionable remediation guidance
- Ongoing AI assurance
- Proven Public Sector delivery
- Builds trust in AI decision-making
- Compliance-as-a-Service for AI governance

7. MULTI-FRAMEWORK GAP ANALYSIS AND INDEPENDENT AUDIT SERVICES.

Independent gap analysis and audit services across ISO27001, ISO22301, CAF, Cyber Essentials Plus, NIST CSF, DORA and other frameworks. Identifying control maturity, compliance gaps and remediation actions to strengthen security and regulatory alignment.

KEY FEATURES

- Multi-framework gap analysis delivery
- Control maturity assessments
- Independent audit services
- Cyber Essentials Plus and NIST CSF support
- Compliance-as-a-Service call-off
- DORA and emerging regulation coverage
- Public Sector aligned methodologies
- Independent assurance of controls
- Structured governance reporting

KEY BENEFITS

- Improved multi-framework compliance readiness
- Reduced organisational risk
- Enhanced audit performance
- Simplified multi-standard compliance
- Accelerated certification readiness
- Prioritised improvement planning
- Knowledge transfer to internal teams
- Improved stakeholder confidence

8. NHS DATA SECURITY PROTECTION TOOLKIT ASSURANCE SERVICES.

NHS DSPT assurance services supporting organisations to meet mandatory data security standards. Guidance on evidence gathering, governance reviews and improvement planning aligned to NHS DSPT requirements.

KEY FEATURES

- NHS DSPT compliance support
- DSPT self-assessment guidance
- Evidence collection and validation
- Data protection and cyber reviews
- Governance alignment with NHS standards
- Organisational readiness assessment
- Gap identification against DSPT controls
- Strengthened information handling practices

KEY BENEFITS

- Improved NHS data security compliance
- Stronger data governance
- Reduced organisational risk
- Improved audit readiness
- Enhanced handling of patient data
- Integration with wider security frameworks
- Improved compliance evidence quality

9. NIST CSF GAP ANALYSIS, RISK REVIEW AND ASSURANCE SERVICES.

Assessment of cybersecurity posture against the NIST Cybersecurity Framework. Identifying gaps, prioritising risks and providing assurance to strengthen security maturity and governance.

KEY FEATURES

- Expert-led NIST CSF gap analysis
- Control mapping to NIST functions
- Governance and risk reviews
- Actionable remediation planning
- Security maturity benchmarking
- Ongoing assurance support
- Independent expert delivery

KEY BENEFITS

- Improved cybersecurity maturity
- Reduced security risk
- Enhanced governance assurance
- Alignment with ISO27001 and other frameworks
- Proven Public Sector methodologies
- Structured reporting and progress tracking

10. ON-DEMAND VCISO AND VCSO SERVICES.

Virtual and fractional CISO / CSO services providing cybersecurity strategy, governance, risk management, compliance, incident response planning and board reporting. Flexible engagement models aligned to business outcomes and budgets.

KEY FEATURES

- Strategic cybersecurity leadership
- Risk assessment and continuous risk management
- Security governance framework design
- Compliance support (ISO27001, PCI DSS, NIST, GDPR)
- Policy and control development
- Vendor risk oversight
- Incident response planning
- Security metrics and board reporting
- Flexible fractional resourcing

KEY BENEFITS

- Stronger security posture
- Reduced organisational risk
- Improved governance
- Accelerated compliance
- Enhanced incident readiness
- Improved decision-making insights
- Cost-effective executive security leadership

11. PCI DSS CONSULTANCY AND COMPLIANCE – PCI QSAC AND PFI SERVICES.

PCI DSS consultancy, compliance assessment and breach investigation delivered by a PCI Qualified Security Assessor Company (QSAC) and PCI Forensic Investigator. Supporting compliance, incident response and strengthened payment card security.

KEY FEATURES

- PCI QSAC accredited consultancy
- PCI Forensic Investigator services
- PCI DSS gap analysis and audits
- Breach investigation and response
- Digital forensics for cardholder data
- Penetration testing aligned to PCI
- PCI training and awareness
- Tabletop exercises and playbooks

KEY BENEFITS

- Faster PCI DSS compliance
- Reduced breach impact
- Improved payment security
- Stronger audit assurance
- Enhanced staff readiness
- Proven Public Sector experience

12. POST QUANTUM CRYPTOGRAPHY READINESS ASSESSMENT, REMEDIATION PLANNING, IMPLEMENTATION, AND GOVERNANCE.

UBDS Digital's post-quantum cryptography readiness service helps organisations meet NCSC migration timelines. The service assesses cryptographic risk, delivers practical remediation planning, and provides governance and delivery management to support a controlled transition to quantum-resilient encryption.

KEY FEATURES

- Structured discovery defining scope, objectives and regulatory obligations
- End-to-end cryptographic asset and dependency mapping
- Automated discovery of encryption, keys and certificates
- Manual assessment of legacy and hard-to-discover cryptography
- Risk-based evaluation aligned to NCSC guidance
- Prioritised remediation roadmap based on exposure and impact
- Phased migration strategy using post-quantum architectures
- Practical remediation using application 6R framework
- Secure key and certificate lifecycle transformation
- Ongoing governance, monitoring, training and assurance

KEY BENEFITS

- Reduces long-term cyber risk from quantum threats
- Aligns early with NCSC post-quantum guidance
- Lowers remediation cost through phased planning
- Improves visibility of cryptographic risk
- Accelerates secure post-quantum transformation
- Reduces delivery friction with structured frameworks
- Simplifies complex encryption estates
- Improves efficiency through automated discovery
- Builds organisational capability and governance
- Supplier-independent, future-proof outcomes

13. TRUSTED SECURITY ADVISORY SERVICES SUPPORTING PUBLIC SECTOR ICT AND CYBER-RISK.

Delivery of trusted advisory services providing multi-framework gap analysis, control maturity assessments and independent audits. The service supports Cyber Essentials Plus, NIST CSF and emerging regulations using public-sector-aligned methodologies to strengthen security maturity and compliance readiness.

KEY FEATURES

- Multi-framework gap analysis across ISO, CAF and others
- Control maturity assessments
- Independent audit services
- Cyber Essentials Plus and NIST CSF support
- Compliance-as-a-Service call-off
- Coverage of DORA and emerging regulations
- Public-sector-aligned methodologies
- Independent assurance of controls
- Structured compliance reporting

KEY BENEFITS

- Improved compliance readiness across frameworks
- Reduced organisational cyber risk
- Enhanced audit outcomes
- Simplified multi-standard compliance
- Accelerated regulatory alignment
- Prioritised improvement planning
- Knowledge transfer to internal teams
- Increased stakeholder confidence

14. VIRTUAL DPO AND DATA PROTECTION EXPERTISE (COMPLIANCE, GOVERNANCE, OVERSIGHT, PRIVACY RISK).

Virtual Data Protection Officer services providing GDPR compliance, privacy governance, DPIAs, incident management, vendor risk oversight, regulatory liaison and ongoing monitoring. Flexible outsourced expertise supports robust privacy risk management and trusted data protection practices.

KEY FEATURES

- Expert GDPR guidance by qualified specialists
- Independent compliance oversight
- DPIA support for high-risk processing
- Policy, procedure and privacy notice development
- Ongoing data protection monitoring
- Incident and breach management advisory
- Third-party and vendor privacy risk assessments
- Staff privacy training and awareness
- Regulatory liaison support
- Flexible outsourced resourcing

KEY BENEFITS

- Stronger GDPR compliance
- Reduced privacy and regulatory risk
- Independent, unbiased oversight
- Improved breach readiness and response
- Enhanced staff awareness
- Streamlined vendor privacy assurance
- Consistent privacy governance
- Cost savings versus full-time DPO
- Sustained compliance monitoring
- Increased stakeholder trust

15. BS10008 SERVICES PROVISIONING, ENSURING INTEGRITY AND LEGAL ADMISSIBILITY OF DIGITAL RECORDS.

BS10008 services ensure electronic records are managed with controls protecting authenticity, integrity and reliability. The service supports assessment, framework design and assurance to demonstrate evidential weight and legal admissibility of digital records across public-sector environments.

KEY FEATURES

- UKAS-retained BS10008 audit specialists
- Bespoke governance and documentation controls
- Assurance of tamper-resistant digital records
- Internal and external BS10008 audits
- Legal admissibility framework design
- Integration with wider governance systems
- Remediation guidance for compliance gaps
- AI and digital records admissibility support
- Evidence trustworthiness validation

KEY BENEFITS

- Trustworthy, tamper-resistant digital records
- Maintained legal admissibility of information
- Controlled electronic record lifecycle
- Improved evidential integrity
- Regulatory confidence and assurance
- Secure digital information management

16. CYBER ESSENTIALS AND CYBER ESSENTIALS PLUS CONSULTANCY AND CERTIFICATION SERVICES.

Cyber Essentials and Cyber Essentials Plus services assess and strengthen core security controls, providing IASME-certified assurance. Expert guidance, remediation support and hands-on technical testing help organisations achieve and maintain UK government-backed certification.

KEY FEATURES

- IASME-licensed Certification Body
- Expert Cyber Essentials guidance
- Pre-assessment gap identification
- CE Plus technical testing
- Remediation advice and support
- Secure configuration reviews
- Patch management guidance
- Malware protection and firewall assessment
- Consultant support throughout certification

KEY BENEFITS

- Reduced cyber risk
- Improved baseline security controls
- Simplified certification journey
- Stronger cyber resilience
- Improved audit readiness
- Trusted IASME assurance

17. IASME CYBER ASSURANCE CERTIFICATION (INCLUDING IMPLEMENTATION, EVIDENCE AND CONTROLS).

Hands-on IASME Cyber Assurance consultancy supporting Levels 1 and 2 certification. The service covers risk management, training, policy development, resilience planning and incident response to support compliance and assurance.

KEY FEATURES

- IASME control implementation support
- Guided interpretation of IASME requirements
- Level-1 self-assessment completion support
- Preparation for Level-2 audited certification
- Cyber risk assessment and mitigation
- Training and awareness programme development
- Cybersecurity and data protection policy development
- Incident response and resilience planning
- Cyber Essentials prerequisite readiness

KEY BENEFITS

- Improved organisational resilience
- Stronger regulatory compliance
- Reduced cyber risk
- Enhanced staff capability
- Improved governance maturity
- Certification-ready assurance

18. ISO INTERNAL AUDIT SERVICES (ISO GAP ANALYSIS, AUDIT AND IMPLEMENTATION).

ISO gap analysis and internal audit services supporting readiness, remediation and assurance prior to certification or surveillance audits. Full implementation services support standalone or integrated ISO programmes with end-to-end delivery.

KEY FEATURES

- ISO9001 gap analysis and implementation
- ISO14001 gap analysis and implementation
- ISO20000 gap analysis and implementation
- ISO22301 gap analysis and implementation
- ISO27001 gap analysis and implementation
- ISO42001 gap analysis and implementation
- BS10008 evidential admissibility audits
- Integrated management system audits
- Impartial internal audit delivery

KEY BENEFITS

- Proven ISO implementation expertise
- Reduced audit risk
- Lower cost and complexity
- Integrated framework alignment
- Certified lead auditors and implementers
- Public Sector delivery experience

19. ISO14001 ENVIRONMENTAL MANAGEMENT CONSULTING SERVICES (DESIGN, IMPLEMENTATION, AUDITS, SUPPORT).

Delivering ISO14001 environmental management system design, implementation, auditing and ongoing support. The service enhances compliance, efficiency and continual improvement through expert guidance and tailored environmental management frameworks.

KEY FEATURES

- Certified and retained certification-body auditors
- Expert ISO14001 implementation support
- Internal and external audit readiness guidance
- Public Sector and industry expertise
- Ongoing post-certification support
- Compliance-as-a-Service delivery
- Tailored documentation development
- Multi-standard integration support
- Specialist efficiency and compliance guidance

KEY BENEFITS

- Proven ISO14001 delivery expertise
- Reduced compliance complexity
- Ongoing post-certification assurance
- Integrated management systems
- Certified lead implementers and auditors
- Public Sector experience

20. CYBER SECURITY MATURITY REVIEW AND ASSESSMENT SERVICES.

Cyber security maturity review and assessment services covering capability assessment, gap analysis, risk identification, benchmarking and remediation planning. The service supports ISO27001, NIST CSF, CIS v8 and Cyber Essentials, helping organisations understand cyber posture, strengthen governance and prioritise security improvements.

KEY FEATURES

- Assess current cyber security maturity capability
- Identify gaps in security controls and processes
- Benchmark against recognised cyber security frameworks
- Conduct cyber risk assessments and threat analysis
- Evaluate governance, policies and procedures
- Provide actionable remediation recommendations
- Review people, process and technology effectiveness
- Support ISO27001, NIST and Cyber Essentials compliance
- Prioritise improvements based on risk and impact
- Advise on cyber security strategy and objectives

KEY BENEFITS

- Clear understanding of cyber security strengths and weaknesses
- Reduced risk through targeted remediation
- Better informed system and vendor decisions
- Improved compliance with recognised standards
- Prioritised improvements aligned to business risk
- Increased confidence in cyber resilience
- Stronger cyber governance
- Continuous security improvement
- Smoother implementation of security initiatives
- Improved coordination across IT and risk teams

21. DATA PROTECTION SERVICES TO HELP UNDERSTAND AND COMPLY WITH DATA PROTECTION REGULATIONS.

Data protection and GDPR compliance services supporting legal obligations, privacy governance and risk management. The service covers DPIAs, policy development, breach response and ongoing advisory support for UK GDPR, Data Protection Act 2018 and international privacy requirements.

KEY FEATURES

- Data protection advice and implementation support
- Data Protection Impact Assessments (DPIAs)
- Privacy by design and system assurance
- Data protection policies and procedures development
- Vendor and system selection oversight
- Records of Processing Activities (ROPA) support
- Data breach response and incident management
- Ongoing data protection advisory services
- Data protection risk assessments and mitigation
- Compliance support for GDPR and DPA 2018

KEY BENEFITS

- Clear data protection roles and responsibilities
- Reduced compliance and organisational risk
- Faster project approvals with embedded privacy controls
- Improved decision making for systems and suppliers
- Better information handling practices
- Increased confidence in GDPR compliance
- Stronger governance for personal data use
- Increased assurance for senior stakeholders
- Reduced delivery delays caused by privacy risk
- Improved coordination across delivery and governance teams

22. NCSC CYBER ASSESSMENT FRAMEWORK (CAF) SERVICES SUPPORTING COMPLIANCE, RISK AND SECURITY.

NCSC CAF services assessing cyber risk, verifying compliance and strengthening controls across public sector IT systems. The service supports continuous improvement, secure and resilient operations, and protection of critical services through structured CAF-aligned assurance.

KEY FEATURES

- Assess cyber risks across public sector IT systems
- Evaluate vulnerabilities and security controls
- Verify compliance with NCSC CAF requirements
- Conduct IT security audits and assessments
- Provide actionable risk mitigation recommendations
- Identify gaps in cyber resilience and protection
- Assess IT system security and resilience
- Data protection and governance framework review
- Public sector cyber compliance assurance
- Continuous improvement of cyber security posture

KEY BENEFITS

- Reduced cyber risk and fewer security incidents
- Compliance with NCSC CAF standards
- Stronger system resilience and reliability
- Protection of critical public sector services
- Better security decision making
- Improved business continuity
- Proactive cyber risk management
- Increased confidence in security controls
- Continuous cyber improvement
- Regulatory alignment of IT systems

23. SUPPLY CHAIN RISK AND ASSURANCE REVIEW SERVICES.

Supply chain assurance services identifying and managing supplier risk through reviews, compliance checks and performance monitoring. The service supports resilience, continuity and risk mitigation across global and local supply chains in public sector environments.

KEY FEATURES

- Supply chain risk management and mitigation
- Supplier compliance verification and monitoring
- Quality assurance of products and services
- Supplier delivery and performance tracking
- Regulatory compliance audits and assessments
- Continuous improvement of supply chain operations
- Transparent reporting and tracking
- Third-party risk management oversight
- Business continuity and disruption planning
- Public sector supply chain assurance

KEY BENEFITS

- Reduced supply chain delays
- Lower supplier and operational risk
- Improved procurement efficiency
- Consistent quality across suppliers
- Stronger regulatory compliance
- Streamlined vendor management
- Improved supplier visibility and transparency
- Better decision making with accurate insights
- Increased trust and accountability
- Maintained continuity during disruptions

24. ACTIVE DIRECTORY CONFIGURATION AND REVIEW.

Delivering comprehensive Active Directory security services, including gap analysis, configuration assessment and hardening tailored to organisational needs. Certified specialists align AD environments to best practice, improve resilience, minimise cyber risk exposure and provide actionable remediation guidance across authentication, Group Policy and identity controls.

KEY FEATURES

- Active Directory gap analysis identifying critical security weaknesses
- Configuration reviews aligned to security best practices
- Security hardening of authentication and identity controls
- Expert recommendations improving Active Directory security posture
- Group Policy assessments detecting misconfigurations
- Tailored remediation guidance to enhance AD resilience
- Delivery by certified Microsoft Active Directory specialists
- Comprehensive audits aligned to industry standards
- Review of authentication, directory browsing and SSO
- Hands-on support implementing recommended improvements

KEY BENEFITS

- Improved Active Directory security posture and assurance
- Early identification of exploitable configuration weaknesses
- Stronger authentication and access controls
- Reduced risk of AD-related outages
- Improved resilience against cyber threats
- Group Policy alignment with multi-framework standards
- Practical remediation support
- Alignment with industry best practice
- Secure Microsoft 365 and AD integration
- Expert-led delivery and implementation support

25. CYBER-HARDENED PII AND PAYMENT DATA DISCOVERY AND PROTECTION SERVICES.

Delivering expert cardholder and PII data discovery across networks, databases and storage systems. The service identifies unencrypted payment data, supports secure erasure and redaction, ensures PCI DSS and DPA compliance, reduces breach risk and protects sensitive personal and cardholder information.

KEY FEATURES

- Detection of unencrypted cardholder data across systems
- Discovery across databases, files, spreadsheets and recordings
- Identification of sensitive PII and payment data
- Secure verification and erasure of cardholder information
- Redaction of voice recordings for PCI compliance
- Process improvements preventing future unauthorised data storage
- Support for PCI DSS and DPA compliance
- Risk mitigation for sensitive data retention
- Expertise informed by breach investigation experience
- Strengthening of organisational security posture

KEY BENEFITS

- Elimination of hidden payment data risks
- Full visibility of potential data leakage locations
- Reduced exposure to breaches and compliance penalties
- Prevention of unnecessary data retention
- Improved PCI DSS and regulatory adherence
- Reduced repeat compliance risk
- Protection of brand reputation
- Trusted insights from experienced specialists
- Improved organisational confidence
- Stronger customer trust

26. IASME CYBER ADVISORY SERVICES – PREMIUM SECURITY ASSURANCE.

IASME Cyber Advisory services provide expert, accredited guidance to strengthen security, achieve IASME and Cyber Essentials compliance and reduce cyber risk. Advisors deliver tailored assessments, hands-on remediation support and trusted assurance to improve resilience and protect critical systems.

KEY FEATURES

- Expert support implementing Cyber Essentials technical controls
- Named consultants providing tailored hands-on guidance
- Risk identification with prioritised remediation advice
- Cost-effective security improvement pathways
- Preparation support for Cyber Essentials certification
- Baseline security measures reducing common attack risks
- Delivery by IASME-certified consultants
- Enhanced assurance backed by IASME and NCSC
- Additional consultancy beyond baseline requirements
- Integration with wider security frameworks

KEY BENEFITS

- Named, certified advisors providing trusted support
- Improved implementation of IASME and Cyber Essentials controls
- Practical, SME-led cyber security support
- Comprehensive risk and remediation insight
- Broader expertise across incident response, PCI, ISO and NIST
- Cost-effective security improvement
- Strong public sector credibility
- Trusted advisory relationships
- Improved organisational cyber resilience

27. ISO31000 CYBER RISK MANAGEMENT, THREAT DETECTION AND RESPONSE STRATEGIES.

Cyber risk modelling and management services helping public sector organisations identify, quantify and mitigate cyber threats. Integrating ISO31000, NCSC guidance, Cyber Essentials, ISO27001 and NIST, the service delivers data-driven insights that strengthen resilience, compliance and operational security.

KEY FEATURES

- ISO31000-aligned cyber risk management delivery
- Certified Cyber Risk Management Professional (CCRMP) consultants
- Multi-framework control assessments
- Scenario-based impact modelling
- Centralised cyber risk dashboards
- Strategic and tactical risk management programmes
- Integrated remediation planning with measurable outcomes
- Independent review of risk posture and governance
- Mapping across NCSC, ISO, NIST and Cyber Essentials
- Risk mitigation and containment guidance

KEY BENEFITS

- Independent assessment revealing unseen risk blind spots
- On-demand access to specialist cyber expertise
- Delivery by certified technical and risk professionals
- Up-to-date threat intelligence and best practice
- Reduced bias in risk decision-making
- Faster cyber maturity improvement
- Objective validation of governance and controls
- Scalable support for major initiatives
- Frees internal teams for strategic priorities

28. MICROSOFT 365 SECURITY CONSULTANCY.

Comprehensive Microsoft 365 security assessment and hardening covering Exchange Online, Teams, SharePoint, OneDrive and Intune. The service identifies configuration gaps, strengthens global settings and enhances protection for high-risk users, delivered by specialists experienced in Microsoft 365 security incidents.

KEY FEATURES

- Microsoft 365 security gap analysis across core services
- Expert review of email, Teams, SharePoint, OneDrive and Intune
- Hardening of global security configurations
- Role-based security controls for user risk profiles
- Protection for privileged and high-risk accounts
- Detailed remediation guidance
- Hands-on implementation support
- Specialists experienced in M365 breach investigations
- Custom security policies aligned to operations
- End-to-end assessment and continuous improvement

KEY BENEFITS

- Early identification of Microsoft 365 security weaknesses
- Strengthened security across collaboration services
- Reduced risk from misconfiguration
- Improved protection of high-risk users
- Clear, actionable security improvements
- Effective delivery of recommended changes
- Real-world breach-informed expertise
- Better alignment of security and business workflows
- Improved endpoint protection and compliance
- Secure, compliant Microsoft 365 environments