# Information Security Management System

# G-Cloud 14

November 2024

# Table of Contents


1 Service Overview ..... 3
2 Business Need ..... 4
3 Our Approach ..... 4
4 Buyer Responsibilities ..... 5
5 Service Management ..... 6
6 Protection of Data ..... 6
7 On-boarding and Off-boarding ..... 6
8 Skills and Knowledge Transfer ..... 6
9 Vendor Accreditations/Awards ..... 7
10 Sub-contractors ..... 7
11 Business Continuity and Disaster Recovery ..... 7
12 Pricing ..... 8
13 Ordering and Invoicing ..... 8
14 Termination Terms ..... 8
15 Further Information ..... 8

# 1 Service Overview

Capgemini provides security consultancy, working with our clients to design and assist with Governance, Risk and Compliance (GRC) services through the delivery of Information Security Management System (ISMS) solutions. Through alignment with the ISO 27001 standard as a baseline and encompassing further assurance of hybridized Enterprise/Cloud environments against ISO27017 and ISO27018, the ISMS, taking a risk-based approach, supports the Confidentiality, Integrity and Availability (CIA) of the client's information systems in order to meet the standards required by Government and other public sector bodies.

The ISO27001 standard is used as a model for security management frameworks for public and private sector organisations to support establishment, management and continuous review of an ISMS. Capgemini's service helps to prepare clients for alignment, transformation and, if required, formal certification. Capgemini has qualified Lead Implementors and Auditors who can provide advice, guidance, security planning, change delivery and security policy/process management, undertaking audits of the client's ISMS and Statement of Applicability (SoA), ahead of a formal ISO27001 certification audit by an Accreditation Body.

Capgemini helps clients understand their information security requirements. Advice can consist of:

- Establishing policies and objectives for information security management;
- Implementing and operating security controls to manage information security risks in the context of the organisation's overall business risks;
- Monitoring and reviewing the performance and effectiveness of the ISMS, and
- Continuous improvement based on objective measurement.

ISMS management is important in *Service* environments where clients may have one or more third parties delivering key services, with multiple operational security interfaces and channels to manage, operate and assure.

Capgemini can help to design a solution that is simple to understand and aligns with the organisation's business priorities. Further support can be provided to enhance governance and security awareness through workshops and presentations.

Each solution is tailored to provide consultancy that addresses the specific needs of the client. Where required, knowledge transfer is included to enable the client to uplift capability and embed good governance over the ISMS for the longer term.

Risk assessment and mitigation are key elements in the establishment and maintenance of an effective ISMS. Capgemini consultants are skilled in undertaking assessments referencing the ISO27001 standard, both within the client's estate and at the premises of third-party suppliers and integrated service providers, assuring that security standards are being met and maintained throughout the supply chain.

Where specific changes or enhancements are recommended or required, Capgemini's security assurance consultants are engaged to identify, evaluate and respond to any changing security needs against NPSA Operational Requirements (OR). The impacts of these activities are reported into the ISMS accordingly.

Capgemini has a successful track record of delivering ISMS services to major UK Government organisations. This includes assisting some of them through their certification and re-certification against ISO27001.

This service supports both cloud and on-premises projects and services, integrating ISO27001 with ISO27017 and ISO27018 to create a hybrid ISMS spanning across Enterprise and Cloud Services.

# 2 Business Need

Implementation of an appropriate ISMS solution can enable the client to achieve business critical objectives, reduce risk and build confidence into transformation programmes. This approach ensures processes are robust, effective and repeatable with appropriate quality controls and records management.

Cloud and digital service adoption can provide clients with new business opportunities and the ability to reach more citizens or consumers. However, as more third parties and channels may be involved in delivering services, the dependency on external parties becomes greater and the associated risks must be carefully managed.

Capgemini's ISMS service is able to support the key principles of a robust information security management system.

The following are examples of key ISMS-related activities that can be provided with each service available as a stand-alone item or as a broader managed accreditation service:

1. Gap analysis, performed against the mandatory requirements of ISO27001 and selected controls reference;
2. Risk assessments. Where appropriate, Risk Management and Accreditation Documentation Set (RMADS) can be produced, our proportionate risk assessment methodology can also be employed where a 'lighter touch' assurance is warranted;
3. Identification of applicable information security controls, aligned with ISO27017/ISO2018 controls and the production of a Statement of Applicability (SoA), creating a hybrid ISMS whose scope spans across Enterprise and Cloud Services;
4. Third party assurance: A mandatory requirement across public (and some private sector) clients and their supplier chains;
5. Physical security reviews, utilising NPSA's Operational Requirements methodology where appropriate, in order to manage the risk of information loss as a result of unauthorised access to business premises;
6. Internal assessments of compliance with applicable security controls to evaluate their effectiveness.
7. Assessments against applicable Legislative and Regulatory requirements, such as DPA/GDPR, NIS or Smart Energy Code (SEC).

Depending on the option selected, Capgemini's ISMS consultancy provision can enable the following benefits:

1. Assurance around the Confidentiality, Integrity and Availability of the client's business systems;
2. Information risks are known, understood, owned, appropriately controlled and reported upon;
3. Client's systems can be demonstrated to be compliant with mandatory and legislative requirements.

In addition to ISMS consultancy, Capgemini can provide a range of cyber security services such as security management, security strategy and transformation, governance risk and compliance, architecture design & implementation, identity and access management, cyber analytics & protective monitoring, testing and employee education & awareness.

Capgemini has over 500 security professionals based in the UK whose expertise can be leveraged to provide our clients with cyber security services.

# 3 Our Approach

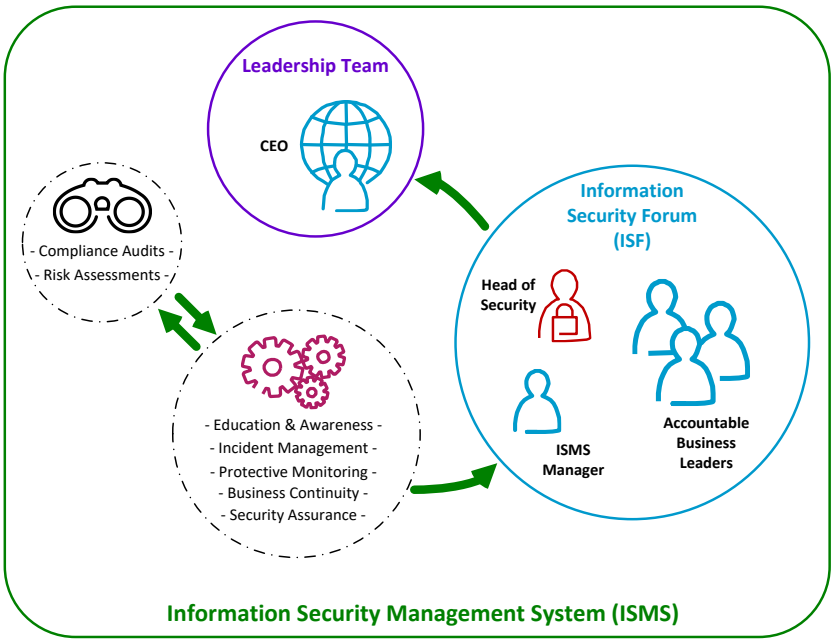
Capgemini's Governance, Risk and Compliance consultants are able to use their experience of ISO27001, Cloud Security Alliance (CSA), Payment Card Industry Data Security Standard (PCI DSS), MOD JSP440, NPSA Operational Requirements, NCSC advice and guidance, Government Security Secure by Design Principles, and

industry recognised risk assessment methodologies such as ISO 27005, IRAM and IS1/IS2 to address the client's challenges.

Capgemini can provide resources to help clients manage their ISMS for their cloud services, or work with the client's own cloud services providers as necessary.

In public sector accounts, the RMADS or alternative risk management processes are supported and used as a mechanism for the identification of applicable control objectives within the Statement of Applicability (SoA).

The ISMS would typically be governed through the establishment of an Information Security Forum (ISF), made up of senior business leaders and informed by key business areas delivering security operations as illustrated in the following diagram:




*This diagram is for illustration only and does not represent any obligation or responsibility of Capgemini.*

This ISMS service can be delivered by ISO27001 qualified Lead Implementors and Auditors.

# 4 Buyer Responsibilities

Please refer to the Supplier Terms listed with this service on the Platform. These may contain additional Buyer obligations/costs the Buyer is subject to that are not identified anywhere else in the Supplier's Application or on the Platform.

The following Buyer responsibilities will apply:

- The Buyer will provide a project/engagement manager to act as a single point of contact and an escalation route for the full duration of the project/engagement;
- The Buyer will make available appropriate subject matter experts (business and technical) as appropriate to support the project or delivery plan;
- The Buyer will be responsible for providing detailed requirements by the mutually agreed date;
- The Buyer will progress the introduction of the service through any internal service introduction/gating process, Enterprise Architecture processes and any other standard processes that are necessary;
- All internal and external user communications will be managed by the Buyer;
- The Buyer will make any network changes to their networks as required for the project;
- Any changes to existing environments required for the service will be Buyer's responsibilities;

- The Buyer will also provide any required test environments and test data reflective of the target implementation environment(s).
- Depending on the service model chosen, the Buyer may have other responsibilities which will be discussed, agreed and then described in the Order Form.
- If these responsibilities do not match your expectations, then please contact Capgemini in order that Capgemini can explore options to vary our approach.

# 5 Service Management

Capgemini's service can be consumed in the following deployment and delivery models, all fully managed by Capgemini. Please contact Capgemini to discuss which of these fits your requirements. These are:

- **Offshore resources**: Capgemini's consultants work from Capgemini's offshore locations. This provides a very cost-effective solution with access to a large pool of related skills.
- **Onshore resources:** Capgemini's consultants work from Capgemini's UK offices. This provides a cost-effective solution for buyers that require UK delivery.
- **Dedicated resources:** Capgemini's consultants work on your sites, embedded as part of your team. This provides a solution for buyers that require skills augmentation and a high degree of control over the work.

# 6 Protection of Data

This service is based on a security classification of 'Official', however should you have a requirement for a different security classification that you would like us to consider, please contact us to discuss.

# 7 On-boarding and Off-boarding

Capgemini shall undertake on-boarding and off-boarding activities agreed within the Order Form and an exit plan in line with the Call-Off Contract terms which will be charged for in accordance with the Pricing section for this service.

# 8 Skills and Knowledge Transfer

Capgemini recognises that skills and knowledge transfer is a critical element in the provision of G-Cloud services to public sector clients. Where possible and applicable, this forms part of the delivery plan for the service agreed at the start of the engagement. Our consultants and engineers are experienced in providing skills and knowledge transfer for major private and public sector clients.

Where appropriate, we may use a standard approach, tailored to topic, skills-gap and individual, to ensure consistency and effectiveness. The approach, Capgemini's Assess-Plan-Implement framework, has been used repeatedly by our teams to structure the work involved in transferring skills and creating new teams capable of driving and sustaining change long after the end of the formal programme. The framework can be applied throughout a project to understand knowledge transfer objectives, plan training delivery methods and materials, and deliver and evaluate success.

# 9 Vendor Accreditations/Awards


For the 12th year in a row, Capgemini has been recognized as one of the World's Most Ethical Companies® by the Ethisphere® Institute. This is an acknowledgment of our ethical culture that makes us an employer of choice and responsible player in the eyes of our clients, shareholders, and the wider community.

Capgemini can provide security delivery professionals with the following industry certifications:

- NIST Cybersecurity Framework (NCSF );
- Certified Information Privacy Professional/Europe (CIPP/E);
- Certified GDPR Practitioner;
- Certified ISO/IEC 27001 Lead Implementer;
- Certified ISO/IEC 27001 Lead Auditor;
- Certified Information Systems Security Professional (CISSP);
- Certified Cloud Security Professional (CCSP)
- Certificate of Cloud Security Knowledge (CCSK)
- Certified Information Security Manager (CISM);
- Certified Information Systems Auditor (CISA);
- Certified Ethical Hacker (CEH);
- TOGAF9, SABSA and other architectural methodologies including Capgemini's own;
- IT security specific MSc or PhD;
- Membership of the Chartered Institute of Information Security Professionals (CIISec)
- Certified in Risk and Information Systems Control (CRIS)
- Computer Hacking Forensics Investigator (CHFI)
- Capgemini delivery staff hold a wide range of vendor specific certifications for many types of cybersecurity tooling.

# 10 Sub-contractors

Capgemini can offer these services using either onshore UK resources or offshore resources. Should the Customer choose an offshore service from India, then Capgemini UK may use the following subcontractors to deliver this service:

- Capgemini Technology Services India Limited.

# 11 Business Continuity and Disaster Recovery

No disaster recovery plan is provided as part of these Services.

# 12 Pricing

This service is priced in accordance with the SFIA Rate Card attached. Capgemini can also provide offshore resources at reduced rates where appropriate. Projects can be priced either on a Time & Materials or Fixed Price basis.

# 13 Ordering and Invoicing

Please refer to the Supplier Terms for this service.

We would be pleased to arrange a call or meeting to discuss your requirements of our service in more detail.

# 14 Termination Terms

Please refer to the Supplier Terms for this service.

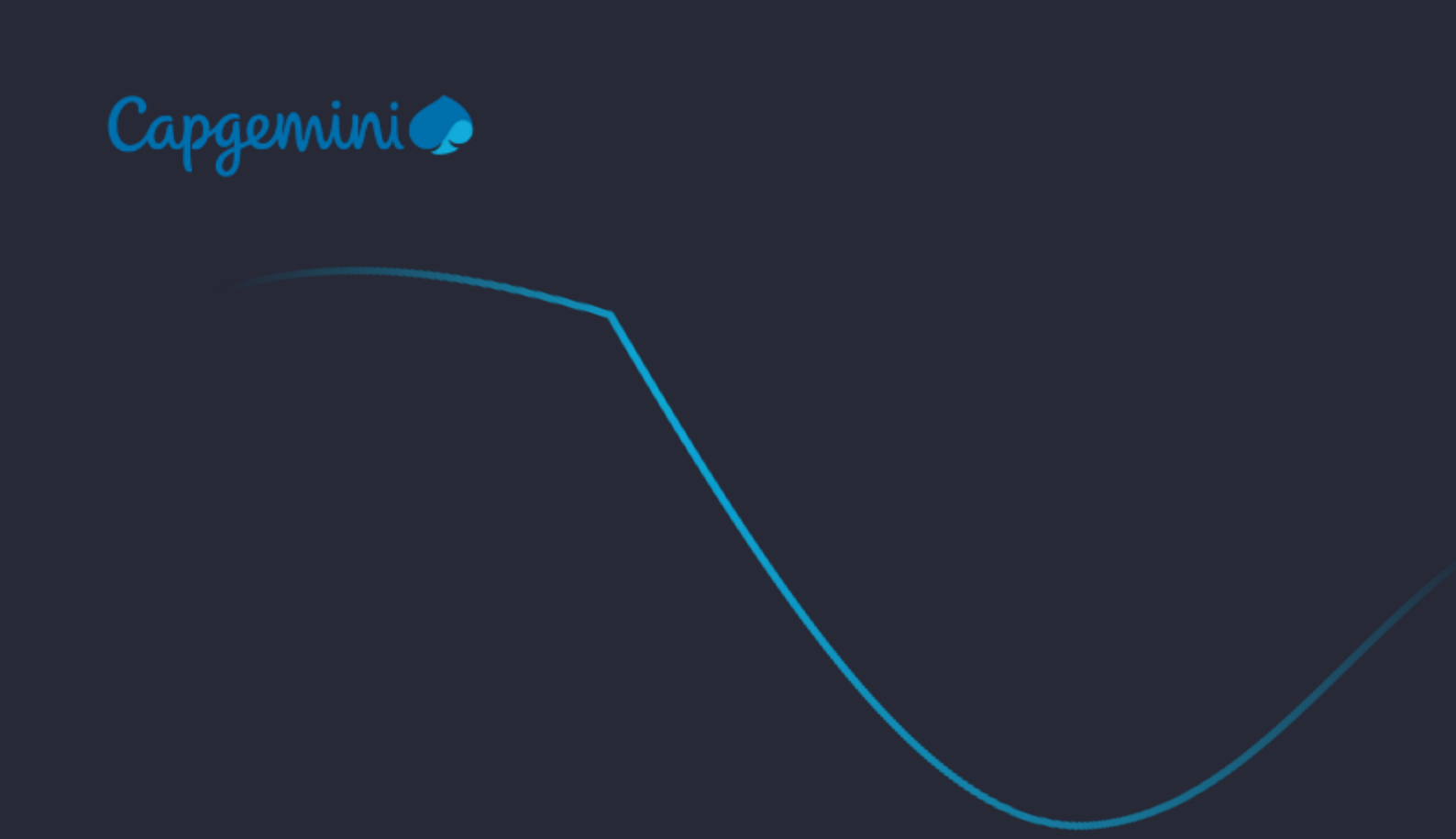
# 15 Further Information

For more information about this or any of our G-Cloud services, please contact our Public Sector Team.

**Phone**: 0370 904 4858

**Email**: publicsector.opps.uk@capgemini.com including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.



## About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the Future You Want | www.capgemini.com



C13AUG22