Advisory

G-Cloud 14 Service Definition

Author: Ian Marlow

Version: 1.0
Date: April 19, 2024
Document: EKCO-GEN-447

Table of Contents

Advisory

Service Overview

Our Advisory team assists clients in safeguarding their brand, people, assets, intellectual property, and profits by providing high-quality information security and data protection services for their cloud-based infrastructure and services. We identify risks and implement industry best practices like ISO27001:2022 to manage them effectively.

As trusted cyber security advisors, we collaborate with your internal team to drive cultural change in cyber risk management throughout your organization. With our expertise, certifications, and experience, we support your entire cyber security governance lifecycle, helping you achieve your cybersecurity goals.

Features

The key features of the Advisory Service are:

- Chief Information Security Officer (CISO) as a Service
- Executive and Technical Cyber Crisis Simulation
- Cyber Resilience and Business Continuity Planning (BCP) including DRP
- Cyber Security Risk and Maturity Assessment
- Data Protection Consultancy for General Data Protection Regulation (GDPR)
- Digital Operational Resilience Act (DORA) Compliance Consultancy
- Data Protection Officer (DPO) as a Service
- ISO27001:2022 (ISO27K) Consultancy
- NIS 2 / PCI / SOC 2 Compliance Consultancy
- Supply Chain Governance

Benefits

The key benefits of the Advisory Service are:

- CISM, CRISC, CISA, CIPP/E, CISSP, ISO27001:2022 certified experts
- Access to the extensive combined cybersecurity knowledge of our team
- Access to real world Incident Management knowledge and experience
- Cyber Resilience, Business Impact Analysis (BIA), RPO/RTO and DR review
- Cyber Maturity Assessment against all frameworks ISO27001:2022, NISTCSF2.0 etc
- Achieve GDPR compliance through Gap analysis, ROPA and policy development
- Access to certified and experienced GDPR Data Protection Officers
- Achieve ISO27001:2022 accreditation with our Lead Implementer /auditor support

- Development of strategic cyber roadmaps to support your digital transformation
- Implement supply chain management process to monitor and mitigate risks

Service Outline

CISO as a Service

Ekco's CISO as a Service (vCISO) is delivered by our advisory team. The service presents a cost-effective resourcing model for your CISO requirements. Our senior information security consultants are industry certified (CISM, CISA, CIPP/E, CISSP, CRISC, ISO27001:2022 lead auditor) and have the knowledge and experience to deliver all your information security requirements. You will have the benefit of having access all the resources and expertise available within Ekco and not have to rely on the personal experience of a single CISO FTE.

Our Chief Information Security Officer will become your trusted advisor and a key component of your internal team. The CISO will ensure that your Information Security risk management program is managed effectively and aligned to both industry best practices and internationally recognised standards. The central responsibility of the CISO role is to reduce the overall level of cyber risk within the organisation to an acceptable level. The CISO will also accurately determine and measure your organisation's cyber security posture and present results and recommendations to your executive board.

The key benefits of using this CISO resourcing model are:

- **Cost Effective:** Avoid the difficulties and cost of hiring a dedicated CISO
- **Trusted Advisor:** Embeds with your internal team acting as their Trusted Advisor
- **Support:** Access to all the resources and expertise available within Ekco
- **Flexibility:** Used to deliver a wide range of projects typically between one to five days per week
- **Experience:** Our consultants have extensive experience delivering across all sectors
- **Mentoring:** Ability to develop the internal team's cyber security expertise
- **Unbiased:** Unbiased insights into your business, acting as a trusted third-party expert

Service Offering:

- Responsible for reducing the overall level of cyber risk within the organisation to an acceptable level
- Act as your trusted advisor on all information security and cyber risk related topics
- Understanding your legal, regulatory and compliance requirements and work with your internal team to manage your compliance requirements
- Embed with your internal team to support them as an information security mentor
- Establishing direct communication channels with key stakeholders, including the board of directors, senior executives, and relevant department heads to provide updates, seek support, and raise any concerns

Cyber Crisis Simulation

Ekco's cyber crisis simulation engagements are delivered by our advisory team. Our senior information security consultants are industry certified (CISM, CRISC, CISA, CIPP/E, CISSP, ISO27001:2022 lead

auditor / implementer). Several have responded to have managed live cyber security incidents for our customers. These events have provided them with the knowledge and experience required to efficiently deliver an effective cyber crisis simulation workshop.

Our assigned consultant will collaborate with your key stakeholders to gain an understanding of your business and its operational environment. We will identify your key systems and processes and propose these as targets when creating the simulation scenario to make it as real as possible for all participants. The objective of this simulation is to ensure that your key stakeholders are prepared to react efficiently when an incident occurs and have the necessary expertise available to mitigate its impact. To remain effective, they should be run frequently and focused on both your executive and technical response teams. We recommend the following sequence of simulations should be run annually.

- **Crisis Simulation (Executive)** - Focus on understanding and verifying the current incident response management procedures and policies
- **Crisis Simulation (Technical Internal)** - Focus on understanding and verifying the current internal technical incident response procedures, policies, and capabilities
- **Crisis Simulation Three (Technical Internal/External)** - Focus on understanding and verifying the current internal/external technical incident response procedures, policies, and capabilities
- **Crisis Simulation One (Executive - Technical)** - Focus on understanding and verifying the current incident response management procedures and policies relating how the Executive and Technical teams mutually support each other during an incident

Service Offering:

- We will gain an understanding of your core business, key systems and processes and your operational environment, including all legal, regulatory compliance requirements
- Conduct a review of your current incident management policy, runbooks, and incident response procedures
- Create a bespoke scenario based cyber crisis simulation scenario which will focus on your key systems and processes
- Deliver the crisis simulation workshops to the staff groupings agreed upon and within the timeframe agreed
- Create a lesson learned report with input from all participants to identify all gaps in your current incident response procedures

Cyber Resilience and Business Continuity

Ekco's cyber resilience and business continuity engagements are delivered by our advisory team. Our senior information security consultants are industry certified (CISM, CISA, CIPP/E, CISSP, CRISC, ISO27001:2022 lead auditor / implementer) and have the knowledge and experience required to efficiently deliver all your cyber resilience and business continuity requirements. Cyber resilience is a key theme within recent EU regulations and directives including DORA, MICA, and NIS 2. Planned cyber resilience and business continuity will enable you to continue to deliver your business products and services in a time of crisis. Comprehensive cyber resilience and business continuity planning is an

essential foundation of effective Incident response management. The mission critical business functions (MCBF) identified during this process will form a vital component of your incident response plan.

Our assigned consultant will collaborate with your key stakeholders to gain an understanding of your business and its operational environment. The first step in this process is the delivering an awareness workshop attended by all key stakeholders where we discuss your core business, our approach to the engagement is discussed, and the input required from the participants are detailed. We issue a business impact analysis (BIA) questionnaire for completion by these stakeholders and through this process we identify all the mission critical business functions and assign an appropriate recovery time objective (RTO) and recovery point objective (RPO). The collected BIA data is analysed to identify the corporate MCBFs. These business functions will inform your disaster recovery planning and are key to effective incident response.

Service Offering:

- We will gain an understanding of your core business, its operational environment, and legal and regulatory compliance requirements
- Conduct a business impact assessment across all your departments in collaboration with your key stakeholders
- Deliver a consolidated, prioritized of your mission critical business functions together with associated RTP/RPO and dependencies
- Create a business continuity plan (BCP) centred around these business functions which details the procedural requirements for invoking your BCP in the event of a critical incident
- Ensure your disaster recovery plan (DRP) is fully aligned with the requirements of your BCP
- Ensure your incident response management procedures are aligned with your MCBF, BCP and DRP
- Perform a knowledge transfer with the client's project team to discuss the results obtained and provide clarifications on any recommendations made

Cyber Security Risk and Maturity Assessment

Ekco's cyber security risk and maturity assessments are delivered by our advisory team. Our senior information security consultants are industry certified (CISM, CISA, CIPP/E, CISSP, ISO27001:2022 lead auditor) and have the knowledge and experience required to deliver a comprehensive assessment of your true cyber security posture. Our cyber risk and maturity assessment delivers two distinct outcomes, a comprehensive report detailing all vulnerabilities identified within your physical, people, organizational and technological controls based on the ISO27001:2022 control set, and a measure of your cyber security maturity against the requirements of international standards such as NIST CSF 2.0 or ISO27001:2022.

The measurement of your organisations cyber security posture provides a baseline with which you can measure your cybersecurity posture improvements periodically over time, typically annually. Your current security posture and maturity levels are assessed through documentation review and interviews with key stakeholders typically using the control requirements of the NIST Cyber Security Framework version 2.0 as a baseline.

The operational risk assessment identifies vulnerabilities and associated business risks. These risks are prioritised, and SMART recommendations identified to mitigate them to an acceptable level. The reported output risks can then be added directly to the organisations corporate risk register and form the basis of a cybersecurity roadmap for risk mitigation, resourcing, and budgeting purposes.

Service Offering:

- We will provide a detailed measurement of your cyber security posture which is aligned to international frameworks, and which describes both your current and target cyber security posture
- The measurement methodology used is the capability maturity model which is an internationally recognised methodology
- We will deliver a comprehensive report detailing all vulnerabilities identified within your physical, people, organizational and technological controls based on the ISO27001:2022 control set
- Identify, document, and report SMART recommendations to mitigate these risks
- Perform a knowledge transfer with the client's project team to discuss the results obtained and provide clarifications on any recommendations made
- The cyber risks identified should be managed in your corporate risk register and will form the basis of a cybersecurity roadmap for risk mitigation, resourcing, and budgeting purposes

Data Protection Consultancy

Ekco's data protection consultancy engagements are delivered by our advisory team. Our senior information security consultants are industry certified (CIPP/E, Law Society Certificate in Data Protection Practice). They delivered a range of data protection services to our enterprise customers including the delivery of General Data Protection Regulation (GDPR) gap analysis, GDPR awareness workshops, creation of record of processing activities (ROPA), Data privacy impact assessments and assistance with their response to data subject access requests (DSAR). This experience uniquely equips them with the knowledge to efficiently deliver your data protection consultancy requirements.

An integral control under Article 32 of the GDPR is to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk". The first step in determining what controls are appropriate is to gain a full understanding of and document the business processes conducted within your organisation which generates personal data records. This is the foundation of all Data Protection efforts and is itself a requirement under GDPR under Article 30 of the GDPR "Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility". Ensuring your ROPA is up to date and appropriate provides our initial focus on all data protection consultancy engagements.

Service Offering:

- We will gain an understanding of your core business, key systems and processes and your operational environment, including all legal, regulatory compliance requirements
- Create/Review your article 30 ROPA to ensure it is up to date and is compliant with the requirements of GDPR

- Conduct a gap analysis of your compliance with the control requirements of the GDPR
- Review all available Data protection Policies and documentation to identify GDPR compliance gaps
- Conduct interviews with key staff to identify GDPR compliance gaps
- Conduct a risk assessment (on a sampling basis) of your operational Data Protection procedures
- Identify, document, and report SMART recommendations to mitigate these risks
- Perform a knowledge transfer with the client's project team to discuss the results obtained and provide clarifications on any recommendations made

DORA Compliance Consultancy

Ekco's Digital Operational Resilience Act (DORA) compliance engagements are delivered by our advisory team. Our senior information security consultants are industry certified (CISM, CISA, CIPP/E, CISSP). They delivered a range of cyber compliance audits to our enterprise customers, (including the financial sector) based on international standards and frameworks such as NIST 800, ISO27001:2022, IEC62443 PCI, GDPR and SOC 2. This experience uniquely equips them with the knowledge to efficiently deliver your DORA compliance consultancy requirements. DORA details five compliance pillars which combine a series of control requirements listed under articles 5 to 45 of the regulation. These will form the focus of our initial compliance gap assessment. Where control gaps are identified during this assessment, we will create a roadmap to green and work with your key stakeholders to close these gaps.

Service Offering:

- We will gain an understanding of your core business, key systems and processes and your operational environment, including all legal, regulatory compliance requirements
- Conduct a gap analysis of your compliance with the control requirements of the relevant articles described under the five pillars of DORA
- Where gaps are identified we will provide SMART recommendations to close these gaps
- Create a roadmap to green to assist your internal team in managing your DORA compliance program
- Collaborate with your internal team to deliver this compliance program and close out all control compliance gaps
- Perform a knowledge transfer with the client's project team to discuss the results obtained and provide clarifications on any recommendations made
- Deliver annual audits to ensure your organization maintains its compliance with the requirements of DORA

DPO as a Service

Ekco's DPO as a Service (vDPO) is delivered by our advisory team. The service presents a cost-effective resourcing model for your DPO requirements. Our senior information security consultants are industry certified (CIPP/E, Law Society of Ireland Certificate in Data Protection Practice) and have the knowledge and experience to deliver all your data protection requirements. In addition, our consultants have a wide range of information security certifications (CISM, CISSP, CISA, CRISC, ISO27001:2022 lead auditor) and

cyber security experience which they can leverage when delivering advice and recommendations on how personal data should be protected in your unique environment. You will have the benefit of having access all the resources and expertise available within Ekco and not have to rely on the personal experience of a single DPO FTE.

Our Data Protection Officer will become your trusted advisor and a key component of your internal team. The DPO will ensure that your data protection program is managed effectively and aligned to both industry best practices and internationally recognised standards. The central responsibility of the DPO role is to ensure your organisation maintains compliance with GDPR and all other data protection regulations and directives. The DPO will also accurately determine and measure your organisation's GDPR compliance posture and present results and recommendations to your executive board.

The key benefits of using this DPO resourcing model are:

- **Cost Effective:** Avoid the difficulties and cost of hiring a dedicated DPO
- **Trusted Advisor:** Embeds with your internal team acting as their data protection trusted advisor
- **Support:** Access to all the resources and expertise available within Ekco
- **Flexibility:** Used to deliver a wide range of projects typically between one to five days per week
- **Experience:** Our consultants have extensive data protection experience delivering across all sectors
- **Mentoring:** Ability to develop the internal team's data protection expertise
- **Unbiased:** Unbiased insights into your business, acting as a trusted third-party data protection expert

Service Offering:

- Responsible for maintaining compliance with GDPR and all other data protection regulations and directives
- Act as your trusted advisor on all data protection related topics
- Understanding your legal, regulatory and compliance requirements and work with your internal team to manage your compliance requirements
- Embed with your internal team to support them as a data protection mentor
- Establishing direct communication channels with key stakeholders, including the board of directors, senior executives, and relevant department heads to provide updates, seek support, and raise any concerns

ISO27001:2022 Consultancy

Ekco's ISO27001:2022 consultancy engagements are delivered by our advisory team. The advisory team has extensive knowledge and practical experience in implementing all common information security frameworks including ISO27001:2022 across all verticals. The consultants hold specific audit certifications such as ISO27001:2022 lead auditor and implementer, in addition to numerous academic qualifications and industry certifications. They also typically hold several industry certifications including CISM, CISA, CIPP/E, CISSP, CRISC. This uniquely equips them with the experience and knowledge to deliver all your ISO27001:2022 requirements.

The advisory team successfully implemented and assisted numerous customers on their journey to achieve accredited to the ISO27001:2022 standard. During these engagements, we typically deliver a range of guidance, advice and assistance including pre-certification audits and support at the formal accreditation audit. Once accredited we periodically assist these clients with the maintenance of their accreditation by delivering pre-surveillance audits in advance of their formal surveillance audits. Our approach to delivering this is fully aligned with the requirements of:

- ISO/IEC 27007: Guidelines for information security management systems auditing
- ISO/IEC 27004: ISMS monitoring, measurement, analysis, and evaluation
- ISO/IEC 27005: Information security risk management
- ISO/IEC 27007: Guidelines for information security management systems auditing
- ISO/IEC TR 27008: Guidance for auditors on ISMS controls
- ISO/IEC 27001: Information security management systems requirements

Service Offering:

- We will gain an understanding of your core business and operational environment, including all legal, regulatory compliance requirements
- Review all available ISMS documentation and conduct interviews with key stakeholders to deliver a gap analysis of your alignment with the control requirements of ISO27001:2022
- Where gaps are identified we will provide SMART recommendations to close these gaps
- Create a roadmap to green to assist your internal team in delivering your ISO27001:2022 accreditation program efficiently
- Collaborate with your internal team to deliver this program, build, and operationalize your ISMS and close out all control compliance gaps
- Support your internal team at your initial ISO27001:2022 accreditation audit
- Deliver ongoing assistance at scheduled supervisory audits to ensure your organization maintains its compliance with the requirements of ISO27001:2022

NIS 2 Compliance Consultancy

Ekco's Network and Information Systems 2 (NIS 2) directive engagements are delivered by our advisory team. Our senior information security consultants are industry certified (CISM, CISA, CIPP/E, CISSP, ISO27001:2022 lead auditor / implementer). They delivered a range of cyber compliance audits to our enterprise customers, (including to operators of essential services (OES) and digital service providers (DSP) under NISD). These compliance audits were based on international standards and frameworks such as NIST 800, ISO27001:2022, IEC62443 PCI, GDPR and SOC 2. This experience uniquely equips them with the knowledge to efficiently deliver your NIS 2 compliance consultancy requirements.

NIS 2 mandates ten specific risk management measures which form the core compliance controls detailed under the directive. The Ekco NIS 2 compliance gap analysis assessment will help you identify your level of compliance maturity against the requirements of NIS 2 and specifically against the ten

mandated risk management measures detailed in the directive. We will identify all compliance gaps with NIS 2 and report SMART recommendations that will mitigate these compliance gaps. Where control gaps are identified during this assessment, we will create a roadmap to green and work with your key stakeholders to close these gaps by delivering on this roadmap.

Service Offering:

- We will gain an understanding of your core business, key systems and processes and your operational environment, including all legal, regulatory compliance requirements
- Conduct a gap analysis of your compliance with the control requirements of the ten mandated risk management measures detailed in the NIS 2 directive
- Where gaps are identified we will provide SMART recommendations to close these gaps
- Create a roadmap to green to assist your internal team in managing your NIS 2 compliance program
- Collaborate with your internal team to deliver this compliance program and close out all control compliance gaps
- Identify, document, and report SMART recommendations to mitigate all identified risks
- Perform a knowledge transfer with the client's project team to discuss the results obtained and provide clarifications on any recommendations made
- Deliver annual audits to ensure your organization maintains its compliance with the requirements of NIS 2

PCI Compliance Consultancy

Ekco's Payment Card Industry Data Security Standard (PCI-DSS) engagements are delivered by our advisory team. Our senior information security consultants are industry certified (CISM, CISA, CRISC CIPP/E, CISSP). They delivered a wide range of cyber compliance audits to our enterprise customers (including the financial sector). These compliance audits were based on international standards and frameworks such as NIST 800, ISO27001:2022, IEC62443, PCI, GDPR and SOC 2. This experience uniquely equips them with the knowledge to efficiently deliver your PCI-DSS compliance consultancy requirements. The PCI DSS (Payment Card Industry Data Security Standard) is an information security standard designed to reduce payment card fraud by increasing security controls around cardholder data.

The latest iteration of the PCI DSS – version 4.0 – was released at the end of March 2022. All merchants and service providers that process, transmit or store cardholder data must comply with the PCI DSS.

Compliance requirements are dependent on the number of annual card transactions, which sets the merchant level, and the way card data is processed, which determines which SAQ must be completed or where a report on compliance (ROC) is required. The main objective is to set appropriate controls on your card data environment (CDE) to protect the card data processed there.

The Ekco PCI-DSS compliance gap analysis assessment will help you identify your level of compliance maturity against the requirements of PCI and specifically against the controls identified on the appropriate SAQ for your merchant level. We will identify all PCI compliance gaps within your CDE and report SMART recommendations that will mitigate these gaps. Where control gaps are identified during

this assessment, we will create a roadmap to green and work with your key stakeholders to close these gaps by delivering on this roadmap.

Service Offering:

- We will gain an understanding of your core business, key systems and processes, your operational and card data environment, including all legal, regulatory compliance requirements
- Conduct a gap analysis of your compliance with the control requirements of all appropriate SAQ's
- Where gaps are identified we will provide SMART recommendations to close these gaps
- Create a roadmap to green to assist your internal team in managing your PCI-DSS compliance program
- Collaborate with your internal team to deliver this compliance program, complete the relevant SQA's and close out all control compliance gaps
- Deliver periodic ASV vulnerability scanning services of your card data environment
- Identify, document, and report SMART recommendations to mitigate all identified risks
- Perform a knowledge transfer with the client's project team to discuss the results obtained and provide clarifications on any recommendations made
- Deliver annual audits to ensure your organization maintains its compliance with the requirements of PCI-DSS

SOC 2 Compliance Consultancy

Ekco's Service Organization Control Type 2 (SOC 2) engagements are delivered by our advisory team. Our senior information security consultants are industry certified (CISM, CISA, CIPP/E, CISSP). They delivered a wide range of cyber compliance audits to our enterprise customers. These compliance audits were based on international standards and frameworks such as NIST 800, ISO27001:2022, IEC62443 PCI, GDPR and SOC 2. This experience uniquely equips them with the knowledge to efficiently deliver your SOC 2 compliance consultancy requirements. A SOC 2 audit report provides detailed information and assurance about a service organisation's security, availability, processing integrity, confidentiality and/or privacy controls, based on their compliance with the AICPA's (American Institute of Certified Public Accountants) TSC (Trust Services Criteria). These trusted services criteria will form the basis of our gap assessment.

The Ekco SOC 2 compliance gap analysis assessment will help you identify your level of compliance maturity against the requirements of SOC 2 and specifically against the appropriate trusted services detailed in the standard. We will identify all compliance gaps with SOC 2 and report SMART recommendations that will mitigate these compliance gaps. Where control gaps are identified during this assessment, we will create a roadmap to green and work with your key stakeholders to close these gaps by delivering on this roadmap.

Service Offering:

- We will gain an understanding of your core business, key systems and processes and your operational environment, including all legal, regulatory compliance requirements

- Conduct a gap analysis of your compliance with the control requirements of all appropriate trusted services controls detailed in SOC 2
- Where gaps are identified we will provide SMART recommendations to close these gaps
- Create a roadmap to green to assist your internal team in managing your SOC 2 compliance program
- Collaborate with your internal team to deliver this compliance program and close out all control compliance gaps
- Identify, document, and report SMART recommendations to mitigate all identified risks
- Perform a knowledge transfer with the client's project team to discuss the results obtained and provide clarifications on any recommendations made
- Deliver annual audits to ensure your organization maintains its compliance with the requirements of SOC 2

Supply Chain Governance

Ekco's supply chain governance engagements are delivered by our advisory team. Our senior information security consultants are industry certified (CISM, CISA, CIPP/E, CISSP, CRISC, ISO27001:2022 lead auditor / implementer) and have the knowledge and experience required to efficiently deliver all your supply chain governance requirements. Supply chain cyber security governance is a key theme within recent EU regulations and directives including DORA, MICA, and NIS 2. Securing your supply chain will assist in enabling you to continue to deliver your business products and services in a time of crisis and is a vital component of your organisational cyber security posture.

Our assigned consultant will collaborate with your key stakeholders to gain an understanding of your business, its operational environment and identify your key vendors. We will review your vendor management policy and procedures and ensure they are appropriate and aligned to industry best practice and international standards. We will perform a cyber security risk assessment of your supply chain to identify your key vendors. This will include a review of the processes and procedures for selecting, evaluating, and monitoring third-party vendors who provide products or services critical to your organisation's security posture.

Service Offering:

- We will gain an understanding of your core business, its operational environment, and legal, regulatory compliance requirements and your supply chain management process
- Implement a supply chain management process which will include Identifying and assessing potential vendors based on their capabilities, reputation, and alignment with the organization's security requirements
- Ensure the supply chain management includes a process for evaluating the potential risks associated with engaging a vendor, including assessing their security practices, compliance with regulations, and potential impact on the organisation's security posture
- Ensure that when negotiating and establishing contractual agreements the cyber security and data protection expectations, responsibilities, and liabilities are defined

- Implement a process of continuously monitoring vendor performance and security practices to ensure they meet the organisation's standards and address any emerging risks
- Ensure that procedures for responding to security incidents involving third party vendors, including communication protocols, investigation processes, and remediation actions
- Identify, document, and report SMART recommendations to mitigate all risks identified
- Perform a knowledge transfer with the client’s project team to discuss the results obtained and provide clarifications on any recommendations made