HEXAWARE

G-Cloud 15 (RM1557.15) Hexaware Ltd, Service Definitions

Cyber Security Risk Services

January 2026

Table of contents

1 Introduction

1.1 Document structure

This Service Definition document provides information about the Cyber Security Risk services offered by Hexaware under the G-Cloud 15 Framework. We have designed it to help public sector buyers understand the functionality, security, pricing and management of our services. This document will provide clarity on how to engage with us through the framework.

The document is divided into 3 core sections:

Service description	Operational delivery	Supplier information
Provides an overview of Cyber Security Risk services, including the delivery framework, key features and benefits, and service scope	Details how our services are delivered under the G-Cloud 15 framework, covering onboarding, service levels, business continuity, invoicing, termination and support.	Summarises our company background, mission, relevant experience and how to procure our services through G-Cloud

Each section is structured to allow buyers to quickly locate the information most relevant to their stage in the procurement process.

1.2 How to use this document

This document is intended to support buyers throughout their G-Cloud procurement process, from initial service evaluation through to contract award and delivery management. We have outlined this process below:

- To help determine alignment with organisational needs for early-stage evaluation, Section 2 (Service description) outlines our service scope, methodology and core benefits
- For due diligence and contract preparation, Section 3 (G-Cloud alignment information) provides the required detail on onboarding, service levels, data management, support and exit procedures
- To assure data protection and compliance, Section 4 (Security and data governance) outlines our information-security framework, data-handling standards and business-continuity measures
- For supplier verification, Section 5 (Supplier Information) includes background information on Hexaware, relevant accreditations and procurement routes

2 Service description

2.1 About our service

Our Cyber Security Risk services are designed to help public sector organisations protect critical digital services, sensitive citizen data and national interests across cloud and hybrid environments. The service supports organisations at every stage of cyber maturity, from establishing foundational controls and compliance assurance through to operating advanced, intelligence-led security at scale.
Our approach solves and responds to common public sector challenges, including:

- Fragmented security tooling
- Complex multi-agency environments
- Increasing regulatory pressure
- The need for rapid, auditable incident response

By combining governance, automation and continuous monitoring, we help organisations move from reactive security management to a proactive, resilient and continuously improving cyber posture.
Depending on customer needs, we can provide advisory, implementation and fully managed services, delivered through clearly defined scopes and Responsible, Accountable, Consulted, Informed (RACI) models. Our comprehensive service spans the full cybersecurity domain, including:

- Security Operations Centre (SOC) with managed detection and response
- Identity and Access Management
- Governance
- Risk and Compliance
- Cloud Security
- Application Security
- Data Protection
- Endpoint and Network Security

Designed specifically for regulated public sector environments, all security controls, reporting and operating models align with recognised standards, including ISO 27001, National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), Centre for Internet Security (CIS) Controls and UK regulatory requirements. Customer data always remains within customer-owned or customer-approved environments, ensuring data sovereignty, privacy compliance and full ownership.

Whether improving existing security operations or delivering structured, long-term cyber transformation, our Cyber Security Risk services are ideal for public sector organisations seeking to strengthen cyber resilience, reduce operational risk and maintain trust in digital public services.

2.2 Delivery framework

Supporting clients to upgrade their cyber security capabilities and reduce risks, we deliver our services through a structured, maturity-led framework. This framework is flexible by design and adapted based on the client's existing tooling, security maturity and the specific services included within the scope. Every stage of our delivery is underpinned by **Tensai® 360 Security Insights**, our proprietary platform, and Tensai® for SecOps, the accompanying methodology framework.

2.2.1 Tensai®

Tensai® 360 Security Insights is our proprietary, AI-powered security intelligence platform that underpins service delivery, governance and continuous improvement across the cybersecurity lifecycle. It:

- Provides centralised visibility across security operations, identity, cloud, data protection and compliance domains
- Aggregates data from existing customer tools to deliver real-time insights into risk posture, control effectiveness and regulatory alignment
- Offers persona-based dashboards tailored to the needs of different stakeholders, including security operations teams, risk and compliance functions, auditors and executive leadership
- Uses AI-driven analytics and automation to prioritise risks, highlight control gaps and support faster, evidence-based decision-making while maintaining continuous audit readiness

Tensai® for SecOps is our structured delivery methodology and maturity model that governs how cybersecurity services are assessed, implemented and optimised. Aligned to the NIST Cybersecurity Framework and Zero Trust principles, it evaluates security maturity across the **Predict, Prevent, Detect, Respond, Recover and Govern** stages of the security lifecycle. The framework facilitates:

- Benchmarking of current capabilities
- Identification of priority improvement areas
- Definition of a phased, risk-led roadmap aligned to organisational objectives and regulatory requirements

Together, **Tensai® 360 Security Insights** and Tensai® for SecOps ensure cyber security services are delivered in a consistent, measurable and outcome-driven manner. The methodology provides a structured approach to security transformation, while the platform delivers continuous visibility, governance and optimisation across cloud and hybrid environments.

2.2.2 Delivery methodology

Tailored to the client's needs, cyber security maturity, scope of services to be provided and required support demands, our delivery methodology is flexible. Typically, engagements follow the steps detailed below:

1. Baseline assessment

We begin by assessing the organisation's current cyber security posture using the Tensai for SecOps maturity model, aligned to the NIST Cybersecurity Framework and Zero Trust principles. This assessment establishes a clear baseline across the full security lifecycle and enables us to identify priority risk areas, control gaps and improvement opportunities across cloud, identity, data and operational security domains.

2. Scope definition

Based on the assessment outcomes, agreed objectives and the customer's existing tooling landscape, we define the exact security domains and services to be onboarded. This could be a single service, such as embedding identity and access management, or a full suite of improvements. Ensuring transparency across customer teams, technology vendors and our delivery teams, we clearly demarcate responsibilities through a RACI model embedded within the Statement of Work (SoW).

3. Security roadmap design

Clearly defining the outcome and journey towards it, we develop a phased, risk-prioritised Security Improvement Roadmap. Aligned to target maturity goals, this roadmap balances immediate risk reduction with longer-term resilience and optimisation, enabling customers to progress at a controlled pace while maintaining service continuity and compliance. Fostering transparency, we present the roadmap to clients for approval before commencing the implementation stage.

4. Implementation

We implement and operate security services incrementally in Agile sprints, through defined operating models and automation-led workflows. Enabling seamless integration of new upgrades, delivery integrates with existing customer platforms and security tooling. Leveraging automation, GenAI-driven analytics and pre-built playbooks, our implementations improve detection accuracy, response speed and operational efficiency across the full cybersecurity domain.

5. Continuous monitoring and optimisation

Using Tensai for SecOps, we track ongoing service performance and security maturity progression through dashboards, KPIs and periodic reassessments. Through continuous improvement cycles, we enable clients to move from reactive security to optimised, predictive and resilient security capabilities.

2.3 Scope of service

Delivering secure, resilient and compliant cloud environments, our Cyber Security Risk services provide a comprehensive security ecosystem spanning operations, identity, data, applications and infrastructure. Our service is designed to support public sector organisations across the full security lifecycle, enabling them to predict, prevent, detect, respond to and govern cyber risk in complex cloud and hybrid environments. Consequently, rather than addressing security challenges in isolation, our approach integrates multiple security domains into a single, cohesive service model encompassing the following capability domains:

Security Operations Centre (SOC):
Providing continuous protection, our 24/7 SOC delivers real-time monitoring, detection and incident response. Leveraging GenAI-driven threat detection, pre-built use cases and automated response playbooks, we provide a rapid, consistent and auditable response to security events. Integration with Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and threat intelligence platforms support proactive defence and threat-led operations.

Identity and Access Management (IAM):
Strengthening identity as a core security control, we deliver end-to-end identity lifecycle management aligned to Zero Trust principles. This includes role-based access control, multi-factor authentication and privileged access governance, integrated across cloud and on-premise environments to ensure secure and seamless user access.

Governance, Risk and Compliance (GRC):
Supporting regulatory assurance, our GRC capabilities align security operations to recognised standards including ISO 27001, NIST and relevant regulatory mandates. Through automated compliance reporting, risk scoring dashboards and advisory support, we enable organisations to demonstrate compliance, manage risk and prepare for audits with confidence.

Data security:
Protecting sensitive information, we deliver advanced data security controls including encryption, tokenisation and data loss prevention. Continuous monitoring supports the detection of insider threats and data exfiltration risks, while privacy controls align with GDPR and other applicable regulations.

Perimeter and endpoint security:
Providing robust frontline defence, we secure endpoints and network perimeters using next-generation firewalls, intrusion prevention and AI-driven endpoint detection and response. Patch management and vulnerability prioritisation further reduce exposure to known threats and attack vectors.

Cloud security:
Enabling secure cloud adoption at scale, we deliver cloud-native security across AWS, Microsoft Azure and Google Cloud. This includes cloud security posture management, cloud identity entitlement management and workload protection, alongside secure DevOps practices such as container security and automated policy enforcement.

Application security:
Embedding security into software delivery, we support secure software development lifecycle practices through application security testing, DevSecOps integration and runtime protection. Our services cover:

- Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) and Interactive Application Security Testing (IAST)
- API security
- Code review
- Remediation support for web and mobile applications

2.4 Service highlights

Identity-centric accelerators, such as IdentityXpress, Jarvic and StratoPAM, cut onboarding and migration timelines by 30-60% on average, reducing programme costs and risks

GenAI-enabled SOC, with 1,000+ use case repository, speed up triage and response, improving detection accuracy and reducing Mean Time to Repair

Framework-led approach enables standardisation of design, hardening and compliance for audit readiness

Platform-based delivery and shared SOC model for scalable, cost-effective operations across hybrid and multi-cloud platforms

Persona-based insights through Tensai 360 offer real-time visibility into risk and compliance for various roles, including executives, operational staff and auditors

2.5 Service features

As solutions and deliverables are tailored to each client, features can vary from engagement to engagement. However, typical features of our Cyber Security Risk services include:

✓ **Cyber security strategy and roadmap development**

Providing a clear and actionable plan for protecting systems, data and users, we work with clients to define a cyber security strategy aligned to organisational objectives, regulatory obligations and risk appetite. Through structured discovery and maturity assessments, we identify current gaps across people, process and technology, and prioritise initiatives based on risk reduction and business impact.

Supporting phased adoption and measurable improvement, we translate strategy into a practical, time-bound roadmap that enables organisations to strengthen security capabilities progressively while maintaining operational continuity.

✓ **Risk and compliance assessments against recognised standards**

For assurance and regulatory confidence, we conduct risk and compliance assessments aligned to recognised frameworks and standards, including:

- ISO 27001
- NIST Cybersecurity Framework
- GDPR
- Center for Internet Security (CIS) Controls
- Zero Trust principles

Using Tensai® for SecOps, we assess maturity across the Predict, Prevent, Detect, Respond, Recover and Govern stages of the security lifecycle. Delivering clear, evidence-based outputs, we identify control gaps, compliance risks and priority remediation actions, supporting informed decision-making and audit readiness.

✓ **24/7 SOC monitoring and incident response**

Providing continuous protection across cloud and hybrid environments, we deliver 24/7 SOC and managed services designed to detect, investigate and respond to threats in real time. Using SIEM-driven monitoring, Extended Detection & Response (XDR) and User and Entity Behaviour Analytics (UEBA), we identify suspicious activity across endpoints, users, workloads and networks.

Improving response speed and consistency, we combine automated detection with human-led investigation, supported by sandbox malware analysis, red teaming activities and structured incident response. Through SOAR, we reduce manual effort and ensure repeatable, auditable response actions.

✓ **Cloud security services across AWS, Microsoft Azure and Google Cloud**

Strengthening cloud security posture, we provide security services across AWS, Azure and Google Cloud environments. This includes continuous cloud compliance monitoring, workload protection and posture management to identify misconfigurations, vulnerabilities and policy breaches. Supporting secure cloud adoption and operation, we apply threat modelling to cloud and hybrid architectures, enabling organisations to understand attack paths, prioritise controls and reduce exposure as environments evolve.

- ✓ **Identity Governance & Administration (IGA) and Privileged Access Management (PAM)**

Reducing identity-based risk, we design and support IGA and PAM capabilities. This ensures that user access is appropriate, auditable and aligned to job roles, while privileged accounts are tightly controlled and monitored. To improve visibility and accountability, we help organisations manage access lifecycle events, enforce least privilege and reduce the risk of credential misuse or privilege escalation.

- ✓ **Zero Trust access design and enforcement**

Supporting modern security architectures, we design and implement Zero Trust access models aligned to organisational risk appetite. Through Zero Trust threat modelling, segmentation and attack-path analysis, we help clients minimise lateral movement and reduce blast radius in the event of compromise.

Helping organisations identify leaked credentials or malicious use of their digital identity, we support certificate and key management, as well as dark web monitoring and cyber brand protection.

2.6 Service benefits

Key benefits of our Cyber Security Risk service, integrations we implement through it, include:

Reduced cyber risk exposure through continuous monitoring and proactive controls

Accelerated cloud security maturity through phased, maturity-driven transformation journeys

Improved audit readiness through continuous compliance monitoring and evidence collection.

Reduced incident response time through automation-led detection and remediation workflows

Improved service availability through proactive resilience and recovery management

Reduced operational security costs through automation and scoped service activation

Improved governance through clearly defined RACI-based service responsibility models.

Enhanced data protection through Zero Trust and encryption enforcement controls.

Improved vulnerability remediation effectiveness through risk-based prioritisation and reporting

Measurable outcomes include:

Accelerated transformation: Identity accelerators, such as IdentityXpress, Jarvis and StratoPAM, reduce onboarding and migration timelines by **30–60%**, cutting program costs by **20–30%**	**Faster incident response:** Improving threat containment, GenAI-enabled SOC operations and automation bots reduce MTTD and Mean Time to Respond (MTTR) by **40–50%**	**Operational efficiency:** Library of automation bots lowers manual effort in remediation and compliance by **up to 40%,** freeing resources for strategic tasks
Improved compliance: Reducing regulatory risks, Identity and Access Management mirroring and Tensai 360 improve audit readiness and compliance scores by **25-30%**	**Cost optimisation:** A shared SOC delivery model, supported by our platform-based approach, lowers costs by circa **15-20%** compared to dedicated SOC set ups	

2.7 Service scope

2.7.1 User support/support levels

To ensure buyers can access help quickly, resolve issues efficiently and maintain continuity of operations, we provide a structured, responsive support service. Our service is tailored to the specific needs of each client. We conduct an initial, high-level assessment of our client's current infrastructure and goals, which informs our support plan. This ensures clients receive customised guidance that fits their specific needs. Support plans are based on a variety of factors, including project size.

2.7.2 Support details

We offer 24/7 user support and incident resolution using our multi-channel service desk, with 24/7 phone line, and email support, with the following response times:

- **Priority 1 (Critical):** Response within 30 minutes, resolution within 4 business hours
- **Priority 2 (High):** Response within 2 business hours, resolution within 1 business day
- **Priority 3 (Medium):** Response within 1 business day, resolution within 3 business days
- **Priority 4 (Low):** Response within 2 business days, resolution agreed with the client

Third-party contractors authorised by the buyer can access support channels upon request. For strategic engagements, a dedicated Technical Account Manager is available to support onboarding, change requests and service performance.

2.7.4 Service constraints

Our Cyber Security Risk service relies on client collaboration and access to information, including existing systems, workflows, IT architecture and current security solutions. Constraints may arise if clients are unable or unwilling to share this information or cannot dedicate sufficient time and resources to collaborative elements, such as workshops, assessments and reviews. Additionally, as data sharing must comply with GDPR and other applicable data protection requirements, this may influence the scope and pace of delivery.

3 G-Cloud alignment information

3.1 Section introduction

Ensuring quality and compliance, each phase of our onboarding/offboarding process is underpinned by our **ISO 9001** and **27001 accredited integrated management system** and supported by defined roles, responsibilities and service levels that align with G-Cloud 15 framework requirements. Our approach combines structured project controls with the flexibility needed for rapid iteration, ensuring clarity, accountability and consistent quality from mobilisation to completion.

This section explains how Hexaware and client teams will work together at each stage of delivery, from onboarding and configuration through to execution, support and secure offboarding.

3.2 Onboarding and offboarding processes

3.2.1 Onboarding

Ensuring all parties are aligned before delivery, our onboarding process is a structured engagement designed to align technical capabilities with business goals. Our typical onboarding timeline for standard engagements is 4 weeks.

An example of our typical onboarding steps is detailed below:

1. **Scope agreement:** Meeting with key representatives, we establish the Scope of Works (SoW). We seek to understand their pain points, mission, current operating model, constraints and risk appetite. Based on this, we confirm a set of opportunities, deliverables and client objectives to inform our Roadmap
2. **Stakeholder alignment and digital setup:** We ensure early alignment and clarity on expectations by establishing a digital onboarding system with the customer's key stakeholders. Integrating our activities with client priorities and ways of working, we collaborate with representatives to confirm role requirements, engagement expectations, and delivery context
3. **Role definition:** Our resource allocation process ensures the right skills and experience are mobilised by gathering detailed role requirements and evaluating internal standby candidates. We conduct initial profile screening to confirm suitability for the project before commencement
4. **Access provision:** The client provides access and appropriate permissions for environments, as well as information on existing systems, enterprise IT architecture, current security maturity level, solutions used and an overview of core platforms, current workflows, processes and documentation
5. **Delivery planning:** We agree on timelines and establish key milestones and review points in line with the agreed delivery lifecycle

3.2.2 Offboarding

To ensure a smooth transition and sustained value after delivery, every engagement concludes with a structured offboarding phase. Focusing on a secure, compliant and seamless handover of services, our process is as follows:

1. **Contract end/notice:** The client provides at least 30 days' notice for offloading resources, or the contract ends naturally
2. **Ramp-down planning:** We create a detailed ramp-down plan complete with timescales
3. **Knowledge transfer:** We begin our structured handover processes, where team members brief client teams on key aspects of the solution and how to operate it

4. **Documentation:** Ensuring all processes, methodologies, and project insights are documented and available to the client, we provide architecture diagrams, infrastructure-as-code, AI-specific artefacts and training materials, if relevant
5. **Account closure:** We revoke access to your systems, removing our accounts' permissions and returning stored data in line with our ISO 27001-accredited Information Security Management Framework

3.3 Service Management

Our delivery team manage services in accordance with ISO principles and scale management levels appropriately to the scope, expectations and requirements of each project. A dedicated Account Manager oversees delivery and acts as the single point of contact throughout the project lifecycle.

Our services are tailored to the unique needs of each client. We conduct an initial, high-level assessment of our client's current infrastructure and goals, which informs our support plan. This ensures clients receive customised guidance that fits their specific needs. Support plans are based on a variety of factors, including project size.

Providing proactive engagement and tailored solutions, we employ a **3-in-a-box** account management model, which includes:

- **An Account Manager:** The client's main point of contact, coordinating all activities and monitoring client satisfaction
- **A Delivery Manager:** Responsible for strategy development and ensuring deliverables are met and on time
- **A Talent Assurance Manager:** Ensuring appropriate skills are applied to relevant functions

Providing comprehensive oversight, this 3-tiered management system ensures alignment with client objectives and seamless coordination for effective support.

3.3.1 Customer alignment

Aligning with our clients' ways of working, existing systems and objectives, we provide a tailored, user-centric service. Allowing us to adjust based on project requirements, our delivery framework is flexible by design. During onboarding and early stages, we host co-creation workshops with business, IT, and compliance stakeholders to understand current maturity and define success criteria. Collaborating closely with client representatives, end-users and technical stakeholders, we seek to understand their:

- Concerns and sensitivities
- Objectives
- Current operating models
- Constraints (e.g. budget, technical literacy)

Based on these elements, we co-design a Security Improvement Roadmap. Fostering transparency, we present the roadmap to clients for approval before commencing the implementation stage.

3.3.2 Performance monitoring

To effectively measure ongoing compliance and goal alignment, we regularly review performance, assessing milestones, risks, dependencies and any required corrective actions. Our approach includes:

- **Performance alignment and reviews:** We ensure and measure adherence to SLAs through a structured and transparent performance framework designed to monitor, report, and continuously improve service delivery. At the outset of the engagement, we collaborate with the customer to define critical SLAs and KPIs, aligning them with business objectives and operational requirements. These SLAs are baselined during the transition phase and recalibrated post-stabilisation to reflect real-world conditions and ensure alignment with evolving business needs
- **Measuring compliance using performance dashboards:** To measure compliance with timescales and KPIs, we employ advanced tools such as the Tensai Insights dashboard, which provides real-time visibility into SLA performance and engagement metrics. This dashboard acts as a single source of truth, enabling role-based insights for informed decision-making and proactive issue resolution
- **Reporting:** Regular reporting is a cornerstone of our approach. During onboarding, we agree on a frequency and format for reports to be shared with clients. Typically, we provide detailed weekly, monthly, and annual performance review reports, including metrics such as response time, resolution time, uptime, and availability
- **Governance mechanisms:** We conduct periodic service reviews and governance interactions with stakeholders to address impediments and track corrective actions. Additionally, fostering a culture of accountability and continuous improvement, customer satisfaction scores and SLA metrics are linked to individual and team performance goals
- **Continuous improvement:** We actively address areas for improvement, leveraging performance metrics to identify gaps and implement corrective measures during engagements and across engagements. Initiatives such as automation, productivity enhancements, and value additions are implemented in collaboration with the customer to proactively address performance gaps.

Providing accountability, Account Managers will be responsible for embedding remedial actions if required. Operational reports can also be provided to buyers on request.

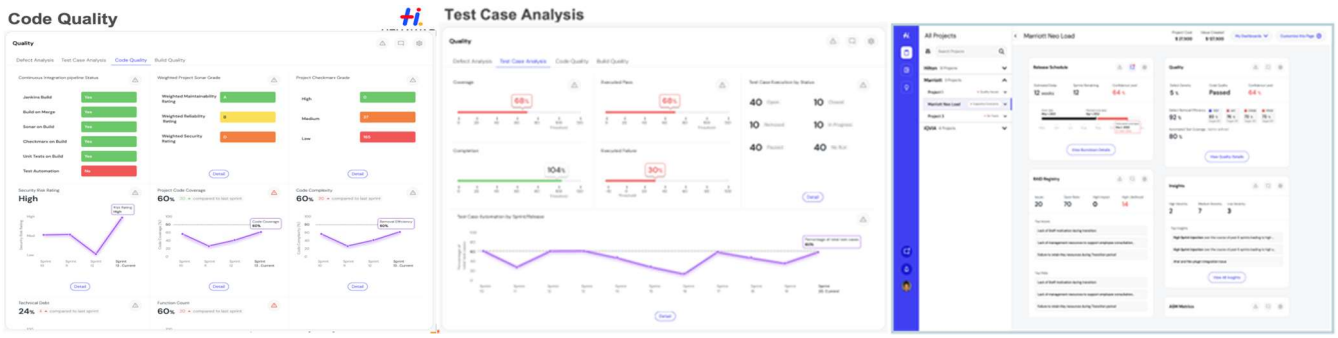

Figure 1: The Tensai Insights Dashboards

3.4 Backup, restore and disaster recovery

For our organisational data, Backups of critical systems and data are performed on daily, weekly, monthly and yearly cycles. Backups are maintained as immutable copies using the 3-2-1 backup principle to protect against data loss, corruption and ransomware.

Maximising security, we don't store within our environment and do not keep or backup customer data.

To safeguard all client and corporate information assets, we maintain comprehensive Data Protection, Business Continuity and Information Governance policies. Maintaining service continuity, data integrity and minimal disruption to client operations, business continuity and resilience processes are governed through a

formal Business Continuity Plans (BCP). This was designed to ensure that critical services and operations continue with minimal disruption during major incidents or disasters.

For each project we perform a **Business Impact Analysis (BIA)** to identify critical services, define acceptable **Recovery Time Objectives (RTO)** and align recovery strategies to contractual requirements. We maintain documented recovery strategies for critical systems and delivery functions and continuity plans are validated through structured testing and governance cycles.

3.4.1 Backup and data protection

Minimising potential disruption, we ensure data protection through redundant infrastructure and resilient design, including:

- Intra-office hub-and-spoke network connectivity
- Multiple Internet Service Providers (ISP) for internet resilience
- Active and passive server configurations for critical applications
- High availability network devices and load-balanced traffic
- Primary and fallback system mechanisms
- N+1 UPS power configurations and generator-backed power supply
- Regular immutable backups with offshore storage and restoration checks

Continuity readiness is validated through regular testing and simulations, including:

- 6-monthly BCP drills covering critical IT services, networks and applications
- Quarterly cyber crisis simulations and tabletop exercises
- Out-of-band (OOB) communication platforms for crisis coordination

These measures ensure that critical services can be recovered within agreed tolerances while maintaining information security and operational continuity.

3.4.2 Disaster recovery and restoration

In the event of disruption, our Disaster Recovery Plan sets out recovery priorities and escalation procedures. Our defined objectives are to:

- Restore essential systems within **24 hours**
- Limit potential data loss to less than one business day
- Maintain continuous communication with client contacts and stakeholders throughout recovery

Following every exercise or live incident, we complete a post-event review and integrate lessons learned into updated procedures.

3.5 Service pricing

To facilitate accessible, flexible service delivery, we offer a range of pricing models including:

- **Time and material (T&M):** Billing based on hourly rates, allowing flexibility for changes without contract amendments
- **Fixed capacity:** Set effort capacity reserved for a fixed period, pricing can be T&M fixed fee or adjusted based on story points

- **Fixed price:** The cost and deliverables are fixed with mutually agreed milestones and acceptance criteria
- **Managed services:** Outcome-based model used in development projects or application support, for projects managed by the vendor

3.6 Invoicing process

Providing a transparent, effective invoicing process, we are aligned with G-Cloud and client procurement terms. Invoices are issued monthly, unless otherwise specified in the SOW.

Each invoice includes:

- Purchase order number and reference
- Description of services delivered during the billing period
- Time or milestone breakdown
- Applicable VAT

Invoices are submitted electronically to the client's designated finance contact or portal, with standard payment terms of 30 days from the date of receipt. In line with best practice, disputes will be handled quickly and efficiently.

3.7 Termination terms

Termination of services is governed by the Crown Commercial Service G-Cloud 15 Call-Off Terms and Conditions and the specific call-off contract. Both parties may terminate the contract with appropriate notice: Usually 90 days, where such Agreement or SOW is terminated for convenience, or 30 days in the event of material breach or non-payment.
Upon early termination of the project for any reason, Hexaware and Customer shall mutually agree, and Customer shall be liable to pay Hexaware for costs associated, including any transition, transformation, tools, investment, outstanding invoices raised by Hexaware, such aggregate value of unrecovered services performed, or any third-party expenses committed by Hexaware, if any till the effective date of termination. If transition has been amortised/absorbed or licenses are used, then can give a schedule for the termination cost.

4 Security and data governance

4.1 Data protection and encryption

Ensuring confidentiality and protection against interception, customer information is protected through an enterprise-wide Information Security Management System (ISMS), Privacy and Business Continuity framework aligned with our **ISO 27001, ISO 27701** and **ISO 22301** accreditations**.** This governs the establishment, implementation, maintenance and continual improvement of security controls across people, process and technology domains, ensuring consistent protection of customer data and critical systems.

To maintain the security and integrity of data, we manage encryption keys through secure key-management systems with strong rotation and access controls. Continuous monitoring ensures any anomalous activity is detected and escalated in real time. Security is implemented using layered technical, physical and procedural controls aligned to defence-in-depth principles, including:

Physical controls	Logical controls	Procedural controls
• Controlled access to work areas through access cards • **24/7** security guards at entry and exit points • CCTV surveillance and visitor management • Restricted area approvals, door alarms and fire detection systems	• Role-based and need-to-know access models • Segregation of duties between production and non-production environments • Secure VPN-based access to client environments • Multi-factor authentication • Next-generation firewalls, IDS/IPS, NAC and DLP • Endpoint protection, patch management and encryption • SIEM-based continuous monitoring • Vulnerability assessments, penetration testing, malware sandboxing and application security reviews	• Formal change and incident management processes • Periodic access reviews and audit cycles • Secure data retention and destruction at engagement closure • Business continuity and disaster recovery governance

4.2 Compliance

Maintaining protection against unauthorised access, all data at rest is encrypted using **AES-256** and is stored exclusively within accredited **EEA data centres** that comply with **ISO 27001** and recognised security and resilience standards. Our approach leverages modern architectures, including Data Lakes, Enterprise Data Warehouses and Lakehouse patterns, to handle diverse workloads from batch reporting to real-time event stream processing.

Facilitating secure storing and processing, we maintain Cloud-based scalable infrastructure and data pods to accommodate a range on needs. Additionally, to support a flexible, hybrid data ecosystem, we accommodate both On-Premise and Cloud environments, which meet specific latency and residency needs. We provide scalable solutions across all major hyperscalers, including, AWS, Azure and Google Cloud and specialise in platforms like **Snowflake** and **Databricks** for high-performance analytics.

Compliance with UK/EU data regulations

Ensuring strict compliance with EU/UK standards, we tailor our storage and processing strategies to the client's specific data classification requirements. Our **Data Governance 10-point Frameworks** and **Data compliance and security strategies** are embedded directly into the solution design.

We also leverage Master Data Management (MDM) and Metadata Management to maintain control, using our Data Encryption and Access Control system to ensure that sovereignty and residency mandates are rigorously enforced.

4.3 Information security management and certifications

Providing effective oversight, Head of Information Security Governance, Peter Raj is our Chief Information Security Manager, with Maria Bellarmine supporting as Head of Information Security. Supporting secure service delivery, they are responsible for all security governance, risk management and compliance activities.

Operating within a formal information-security governance framework, our services are supported by the following certifications and independent assurance:

- ISO 27001:2022 – Information Security Management
- ISO
- SOC 2 / SOC 2+ Type II
- HITRUST (2024)
- ISO 14000 (2023)
- PCI-DSS (for selected customers)
- ISO 22301:2019 – Business Continuity Management
- Cyber Essentials Plus 27701 – Privacy Information Management
- SOC 1 Type II
- ISAE 3000 & GDPR Assessments

4.4 Identity and access management

Security access is governed through a comprehensive set of policies and controls aligned with our **ISO 27001** accreditation and the UK government's cloud security principles. The Project Manager oversees access and monitors adherence to our security policies.

All staff with access to systems or customer data undergo background screening. Access is granted on a strict least-privilege basis and protected through MFA and activity logging.

5 Supplier information

5.1 About us

At Hexaware, solving IT and business process challenges is our mission. Our ethos is deeply rooted in creating a meaningful impact on the world through the power of technology and people. We address complex problems across industries with innovative solutions:

- Transforming Data into Insights: Leveraging AI to uncover actionable insights.
- Enhancing Customer Experiences: Delivering innovative platforms to improve user engagement.
- Cloud Migration: Ensuring smooth and secure transitions to the cloud.
- Contact Center Management: Providing efficient and reliable solutions.

Our collaborative approach ensures exceptional outcomes at every step, turning your challenges into proven success stories. Together, we dream big, innovate relentlessly and create a brighter future.

5.1.1 Core Values

Guiding our decisions and shaping our culture, our values are based around our **5 core principles**:

1. **Put People First:** We prioritise the well-being and engagement of our employees, enabling them to create better solutions for our customers
2. **Create Customer Value:** As a trusted partner, we aim to surpass expectations and deliver value to help businesses grow and thrive
3. **Innovate Relentlessly:** We push boundaries, embrace change and continually find new ways to solve problems for our customers
4. **Be Sustainable:** Ensuring a better tomorrow for our stakeholders and the planet, sustainability is integrated into all our operations
5. **Come On In:** We foster an inclusive environment where everyone feels welcome, safe and valued

5.1.2 Our history

1990:	Hexaware was founded as Aptech Limited, focusing on training technology talent for the Indian IT industry.
1995:	We expanded operations to North America and Europe, establishing a strong reputation in application development and maintenance.
2001:	The training arm of Aptech was demerged and the company was renamed Hexaware Technologies Limited. This marked a strategic shift to focus solely on IT services.
2006:	Acquired Focus Frame, a testing services company in Mexico, which was later integrated into Hexaware.
2012-2013:	Launched SaaS offerings, mobile testing solutions and enterprise mobility services. Caliber Point, the BPO arm of Hexaware, was merged into the parent company.
2019:	Acquired Mobiquity, a digital service provider renowned for its innovative work in customer experience, mobile and cloud solutions.
2023:	Formed a joint venture in Qatar with Al-Balagh through QFC. Opened new delivery centers in Bhopal and Dehradun, India.

2024:	Acquired Softcrylic, a premier data consulting firm, to enhance data and analytics capabilities. Expanded operations with new delivery centers in Sri Lanka, Coimbatore and Mangalore, India and a 1000-seat facility in the Philippines.
2025:	Relisted on the NSE and BSE on February 19, marking a significant milestone. New delivery facilities opened in London, UK and Chicago, USA. In July, we acquired SMC Squared, a leader in Global Capability Centres, merging their build-operate GCC model with Hexaware's AI-powered IT delivery. This strategic integration launches GCC 2.0, unlocking long-term value through advanced, platform-driven operational excellence.

5.1.3 Hexaware in 2026

Hexaware is a purpose-driven global technology and business process services company operating in over **30 countries.** With a workforce of **over 31,000** professionals from **90+ nationalities**, we are committed to creating smiles through great people and technology. Our AI-first approach enables us to:

- Build great digital products that deliver frictionless customer experiences.
- Transform enterprises into cloud-native organisations.
- Optimise operations with AI-based platforms and a predominantly generative AI-trained workforce.

Revenue and Growth

Evidencing our successes, we have achieved an **18% CAGR** over the last decade, with a projected revenue of $1.5 billion for 2025.

5.2 Why choose us

We are uniquely positioned to deliver exceptional value through our innovative solutions, cultural alignment and proven track record. Our flexible, partner approach ensures access to senior leadership, tailored solutions and a partnership-oriented mindset that values continuity and trust. Below we have outlined the key differentiators that set us apart:

1. **Comprehensive delivery service across key areas:** Ensuring a seamless experience for clients, we offer integrated service delivery across all key areas, including:

    - **Cloud Services:** We improve strategy, migration, modernisation and managed cloud operations to deliver scalable, secure and resilient cloud foundations
    - **Data & Analytics:** We manage data modernisation, analytics and AI-driven insight frameworks to unlock value and accelerate decision-making
    - **Digital & Software Solutions:** We deliver product engineering, experience design and digital solutions that create differentiated customer and employee experiences
    - **Digital IT Operations:** We provide integrated infrastructure and digital workplace services, application management, testing/quality engineering, cybersecurity and intelligent automation
    - **Enterprise Platforms:** We support implementation and managed services to maximise ROI on platforms such as Oracle, SAP, Salesforce, Workday, ServiceNow, Adobe and Snowflake

- **Global Capability Centers (GCC):** We build and scale future-ready, AI-enabled capability centers to improve speed, quality and cost efficiency across enterprise functions
- **Generative AI:** We support end-to-end GenAI strategy, use-case acceleration and responsible AI enablement to enhance productivity and innovation.
- **Business Process Services (BPS):** We facilitate experience-led operations across customer support, content/marketing ops, finance and accounting and automation to drive efficiency and agility

2. **Proven methodologies and accelerators:** Our proprietary platforms, including Tensai, Amaze and RapidX, drive automation, efficiency and innovation
3. **Security and compliance embedded:** We embed security into our processes, aligning with our ISO 27001, ISO 20000, ISO 22301 and CMMI Level 5 certifications. Our services also align with NIST, SOC 2 and other regulatory standards critical to various industries
4. **Flexibility and scalability:** Ensuring scalability to meet fluctuating demands without compromising quality, we operate a Core-Flex Model, focusing on Outcome-Based Engagements and delivering measurable results.
5. **Innovation-driven approach:** Hexaware integrates advanced technologies such as AI, machine learning and process mining to drive continuous innovation
6. **Commitment to Sustainability:** Hexaware integrates sustainability into all operations, aligning with global focus on environmental and social responsibility. We collaborate with stakeholders to build a better tomorrow through innovative and sustainable solutions

Hexaware's unique combination of cultural alignment, innovative solutions and proven expertise makes us the ideal partner. By choosing Hexaware, you gain:

- **Localised Expertise:** Deep understanding of the UK market and public sector requirements.
- **Proven Track Record:** Demonstrated success in delivering measurable outcomes for UK clients.
- **Cost Efficiency:** Significant cost savings through automation and optimised delivery models.
- **Innovation and Agility:** Cutting-edge technologies and flexible engagement models tailored to your needs.

Hexaware is committed to empowering organisations to achieve their digital transformation goals, enhance user experiences and drive sustainable growth.

5.3 Relevant experience and testimonials

Case Study 1 – Leading UK Insurance Organisation

Overview

We delivered our Cyber Security Risk services for large UK-based insurance organisation delivering critical digital services to millions of customers. Operating complex cloud and hybrid IT environments with stringent regulatory and data protection obligations, the client sought to reduce intrusion attempts, improve compliance and enhance overall security.

Challenges

Key challenges the client faced included:

- High volume of intrusion attempts targeting cloud and perimeter environments
- Limited visibility and slow response times across distributed security tools

- Inconsistent privileged access governance and risk of unauthorised access
- Manual certificate management causing compliance and availability risks
- Difficulty maintaining consistent SLA performance across security operations

Solution

We designed and implemented a bespoke cyber security solution, with our full suite of services including:

- Implemented centralised 24×7 SOC operations with SIEM, XDR and automated response workflows
- Deployed unified perimeter security across next-generation firewalls, secure web gateways and cloud WAF platforms
- Implemented Identity Governance and Privileged Access Management for controlled access to critical systems
- Introduced PKI automation for certificate lifecycle management
- Established SLA-driven operational governance and reporting

Outcomes

Facing the client's challenges and meeting their objectives, our service delivered a variety of tangible outcomes, include:

- **38% reduction** in Mean Time to Resolve (MTTR)
- Blocked **1.67M+ intrusion attempts/month** via enhanced perimeter defense, cloud Flare Palo Alto, Cisco FTD, and Zscaler
- **82% reduction** in unauthorised access attempts
- **100% privileged access coverage** across critical systems
- **99.9% email threat interception** and uninterrupted availability during attack scenarios
- **97%+ SLA adherence** across security operations

Case Study 2 – UK & European Insurance Provider

We delivered this service for a UK and Europe-based pet-insurance provider delivering digital insurance services across multiple business units, operating hybrid cloud environments with strong regulatory, privacy and resilience requirements.

Challenges

Key challenges included:

- Limited centralised visibility across hybrid cloud environments
- Manual vulnerability handling and delayed remediation cycles
- Increasing regulatory and data privacy compliance requirements
- Lack of consistent SOC governance across multiple business units

Solution

Our tailored approach and solution comprised the following services:

- Implemented 24×7 SOC operations with SIEM-driven monitoring and response
- Deployed cloud security controls, identity governance and access management

- Implemented data protection, DLP and privacy management controls
- Standardised SOC processes and onboarding for multiple business units

Outcomes

Meeting the client's objectives, our support enabled the following measurable outcomes:

- **100% SLA adherence** across SOC operations
- **Improved regulatory compliance and privacy posture**
- **Centralised, scalable SOC delivery** across UK and European operations

"For us, Hexaware has been a key partner in allowing us to focus on the areas that are the highest value priorities. Given the limited number of resources we have, Hexaware can step in and assist with the important day-to-day work, allowing us to advance projects much more quickly with the resources we have."

- Bert Odinet, SVP and Chief Innovation Officer, Freeport-McMoRan

"Hexaware has been a great partner. We operate in 120 countries and have a lot of complex projects. We serve a large spectrum of clients, from large enterprises to small businesses. So, the breadth and depth of the businesses is wide and varied. Hexaware's engagement has been critical in enabling us to serve our customers better. They continue to play an important role in our 3X3 transformation."

- Abdul Razack, Global Head of Product and Engineering, Aon Plc

5.4 How to buy

Hexaware's services can be procured directly through the Crown Commercial Service (CCS) G-Cloud 15 Digital Marketplace. Buyers can search for Hexaware on the Digital Marketplace and select the required service listing. Once selected, the buyer and Hexaware will:

- Agree a Statement of Work (SOW) detailing scope, deliverables, timescales and pricing
- Raise a Call-Off Contract under the G-Cloud framework terms
- Issue a Purchase Order (PO) to confirm commencement

Ensuring transparency, quality and compliance with public-sector procurement regulations, all Engagements are delivered in line with G-Cloud framework conditions.

Enquiries or pre-contract discussions can be arranged through our central contact point:

Contact: Debabrata Dey
Telephone: 07432479231
Email: DebabrataD1@hexaware.com