Public Sector

Dec.2025

Cloud Cyber Security, Data Protection, Data Privacy, and Data Ethics

Service Definition

V1.0

Cloud Cyber Security, Data Protection, Data Privacy, and Data Ethics

Service Definition

V1.0

Document owner

Chris Walker

Document Creation date

12-2025

Business Area/C.o.E./Area

Public Sector

Country

United Kingdom

Contents

1 Service Overview

BIP provides Cyber Security as a Service to help organisations protect critical systems, sensitive information, and essential services in an evolving threat landscape. The service brings together strategic advice, technical delivery, and ongoing assurance into a single, coherent offering that adapts to each client's business priorities, regulatory environment, and risk appetite.

Our approach is practical and collaborative. We work alongside client teams to embed cyber security into everyday decision making, system design, and operational delivery. Security is treated as an enabler of outcomes, not a barrier to progress.

The service is particularly well suited to complex and highly regulated environments where demonstrable assurance, strong governance, and evidence-based decision making are essential.

2 Secure by Design as a Foundation

Secure by Design is a core principle across all cyber security services delivered by BIP. Our teams apply these principles daily within central government and regulated sectors, supported by a detailed understanding of national cyber security guidance and department specific security policies.

BIP's cyber leadership includes an NCSC Head Consultant who holds Chartered status with the UK Cyber Security Council. This ensures senior oversight, technical credibility, and consistency across all Secure by Design activity.

Our teams are trained in the Cyber Assessment Framework, including Secure by Design considerations under Principle B4 System Security. This enables us to support both design assurance and formal assessment activity with confidence and clarity.

3 Secure by Design Engagement Model

BIP has developed a structured Secure by Design engagement and tracking approach aligned to the National Cyber Security Centre's five security design principles.

These principles guide how we support clients across the full lifecycle of systems and services.

- Establishing context before design begins, including users, threats, dependencies, and regulatory constraints
- Making compromise difficult through layered security controls and robust architecture

- Making disruption difficult by building resilience and recovery into design decisions
- Making compromise easier to detect through effective monitoring and response capability
- Reducing the impact of compromise through containment, segregation, and recovery planning

While grounded in recognised government best practice, the approach also incorporates wider perspectives drawn from standards such as ISO 27001 and NIST. This ensures solutions are proportionate, resilient, and aligned to international good practice.

4 Cyber Security Centre of Excellence

Cyber Security as a Service is delivered through BIP's internal Cyber Security Centre of Excellence, which brings together more than 500 skilled professionals.

The Centre of Excellence enables an integrated delivery model that combines expertise across:

- Cyber risk and assurance
- Legal and regulatory compliance
- Digital and cloud technologies
- Offensive and defensive security
- SOC, Incident response, and managed services

Clients benefit from coordinated expertise delivered through consistent methods, shared tooling, and strong governance, rather than fragmented or siloed services.

5 Our services

The services offered by BIP CyberSec are designed to support organisations at every stage of the cyber risk management process. Thanks to an integrated approach, proven methodologies, and advanced tools, we assist clients in identifying, assessing, and treating risks, providing effective, targeted solutions that are aligned with business objectives, **through the following areas of expertise:**

- Strategy Area
- Technology Area
- Cyber Defense Area
- Re@ck Security Center

5.1 BIP CyberSec – Strategy Area

The **Strategy** area of BIP CyberSec offers a diverse range of services, spanning **Business Continuity & Resilience**, **Cyber Risk Management**, **Compliance**, and **Data Protection & Privacy Advisory**.

Business Continuity & Resilience

BIP CyberSec supports organisations in implementing Business Continuity and Resilience programs to ensure operational continuity and effective response to critical cyber security events and threats.

Our approach combines business process analysis, continuity planning, and scenario-based testing to verify the effectiveness of measures in place, helping organisations maintain resilience over time. By following international best practices (ISO 31000) and industry standards (e.g., DORA Regulation), we deliver solutions that are both sustainable and aligned with business objectives.

Cyber Security Governance

Our team supports organisations in defining their Cyber Security Strategy, ensuring governance of security initiatives in alignment with business objectives and the company's digital strategy, while involving all relevant stakeholders. We also provide support in assessing the organisation's cyber security posture, leveraging key international standards, and in defining remediation roadmaps that include organisational and technological initiatives to protect corporate systems. We also assist clients in conducting maturity assessments for industrial environments, applying industry-specific standards.

Compliance

In order to ensure compliance with international and local regulations, organisations today must continuously evaluate their business and operational processes and align them with cyber security and resilience best practices. Our team supports clients in identifying regulatory requirements through an in-depth analysis of national and cross-border regulations, such as GDPR, CCPA, LGPD, HIPAA, NIS Directive, Cyber Security Act, NERC CIP, PCI DSS, PSD2, as well as major reference frameworks, including ISO 27001, NIST Cyber Security Framework, and COBIT. These frameworks and regulations are used to assess the maturity level of organisations in terms of regulatory compliance and to define remediation plans, providing a structured approach that is aligned with international standards.

Cyber Risk Management

BIP supports clients across the full cyber risk lifecycle. This includes the design of cyber risk management methodologies, execution of detailed risk assessments, and identification of targeted interventions to reduce exposure. Risks and recommended actions are prioritised based on business impact and presented clearly to senior leadership and boards. Where required, BIP also delivers the agreed interventions, ensuring recommendations translate into measurable outcomes rather than static reports. Our experience spans legacy, cloud, and hybrid environments, supporting complex organisations across multiple sectors.

Data Protection & Privacy Advisory

Personal information is an increasingly valuable – and increasingly risky – asset for organisations. In a context of rapidly evolving regulations and increasingly

sophisticated threats, it is essential to define appropriate measures involving key internal stakeholders with legal, technical, and cybersecurity expertise. Our team supports organisations in defining and implementing data protection and privacy programs, providing services such as audits and risk assessments, development of global policies, international data transfer strategies, management of data processing agreements, and other organisational and technological initiatives to ensure regulatory compliance. We assist clients in identifying regulatory requirements and assessing organisational maturity, leveraging international standards and guidelines (ISO/IEC 27701, ENISA, EDPB, CNIL, etc.) while considering national and regional laws, in order to implement effective measures and demonstrate compliance to supervisory authorities.

5.2 BIP CyberSec – Technology Area

Cloud Security & Strategy
Organisations today face continuous technological innovation and digital transformation, including the adoption of cloud services, in a context that requires safeguarding systems, data, and applications across complex and distributed environments. BIP's team supports organisations in implementing Cyber Security and Cloud Security programs, following a data-centric, security by design approach. This includes defining strategies and frameworks for cloud protection, designing secure systems, assessing process and technology maturity, and implementing solutions for data protection and encryption key management across multi-cloud and hybrid environments. Through proven methodologies and advanced tools, we help organisations manage systems, networks, APIs, and data securely, turning potential challenges into opportunities while ensuring operational continuity, regulatory compliance, and technological resilience.

Identity and Access Management (IAM)
BIP CyberSec supports organisations in modernising their Identity & Access Management (IAM) systems, reducing risks through a security-, automation-, and trust-based approach. We provide integrated services to protect critical data and access, covering Identity Management, Identity Governance, Access Management, and Secret & Key Management, enabling organisations to securely manage users, privileges, credentials, and policies while ensuring compliance, resilience, and data protection.

Data Protection
Data and information are among the most critical assets of any organisation. Uncontrolled handling of sensitive data poses significant risks, both in terms of regulatory compliance (e.g., GDPR, PCI-DSS, Data Privacy) and in terms of reputation, intellectual property protection, and competitiveness. BIP CyberSec supports organisations in defining and implementing Data Security strategies, adopting a security-by-design approach that integrates business enablement with data protection, ensuring safe collaboration across internal and external stakeholders. Our services cover the full data security journey, from information classification and mapping to the implementation of technical controls, including key areas such as Data Classification, Data Discovery, Data Governance, Data Masking, Data Protection, Cloud Data Protection, and Secure Collaboration. BIP CyberSec can support

organisations throughout the entire Data Security lifecycle or address specific needs, both from process and technology perspectives, reducing risk while ensuring operational continuity.

5.3 BIP CyberSec – Cyber Defence Area

Ethical Hacking
Evaluating defences from an attacker's perspective is one of the most effective ways to measure real security. BIP CyberSec supports organisations with Ethical Hacking and Red Team services, identifying vulnerabilities across networks, applications, cloud environments, and industrial systems. Our intelligence-driven approach combines penetration testing, social engineering, and scenario-based Red Team exercises, leveraging industry best practices and frameworks to simulate real attacks. Findings are prioritised by risk and delivered as a clear, actionable remediation roadmap, improving security posture and resilience across the organisation.

Blue Team
Building on our experience, BIP CyberSec offers the **Blue Team Service**, focused on **Prevention, Detection, and Response**. The service covers all aspects of cyber-attack management, including security monitoring, incident response, digital forensics, threat hunting, malware analysis, intelligence, brand protection, and cyber training. Our team of certified professionals, combining expertise in security architecture, incident management, threat intelligence, and training, delivers up-to-date and operationally effective solutions to continuously safeguard organisations.

Ransomware Simulation
In response to the rising number of ransomware attacks and the unpreparedness of many organisations, BIP CyberSec has developed the Ransomware Simulation service, which allows companies to simulate real attack scenarios before they occur. Leveraging in-depth knowledge of major ransomware families and active threat actors, the service enables organisations to test the effectiveness of existing security controls in a controlled environment and assess the potential impact of an attack, enhancing resilience and preparedness against real threats.

OT/IoT Security Testing
End-to-end IoT solutions encompass infrastructure, devices, mobile applications, and third-party services, tailored for environments such as Enterprise Smart Office, Smart Building, Industrial, and Healthcare. BIP CyberSec supports organisations in identifying and assessing cyber and physical vulnerabilities within their IoT infrastructure, detecting potential weaknesses that could be exploited by malicious actors. Our IoT Assessment service adopts a multidisciplinary approach, covering all critical security aspects—from devices and software to APIs and networks—providing a comprehensive evaluation of the resilience and security of IoT systems.

Digital Footprint
Organisations leave digital traces that, if analysed, can reveal insights into their overall cyber exposure. Proper management and control of this information is essential to reduce risk. The solution offered by BIP CyberSec, the Digital Footprint

service, enables organisations to analyse and reconstruct these digital traces, providing a clear view of their exposure and associated risks. This approach helps improve awareness, reduce attack surfaces, and strengthen overall security posture.

Vulnerability Management
In today's digital landscape, managing vulnerabilities is essential to reduce cyber risk and protect critical data and services. The solution offered by BIP CyberSec, the Vulnerability Management service, helps organisations identify, assess, and mitigate technical vulnerabilities through a comprehensive and tailored approach. The service manages the full vulnerability lifecycle—from detection to remediation—prioritising actions based on real risk, providing guidance on mitigation strategies, automating processes where possible, and ensuring scalable protection of digital assets while reducing costs associated with cyber incidents.

7 Our products

Our Risk Platform: Cyber Risk Dive
Cyber Risk DIVE is BIP's SaaS platform designed to provide a rapid, data driven view of cyber risk. The platform considers organisational context, threat exposure, and regulatory requirements to deliver a clear and actionable picture of cyber posture. This supports informed decision making, strengthens assurance, and helps focus investment where it delivers the greatest value.

Cyber Risk DIVE stands out as an all-in-one solution for the centralised management of cyber risk across multiple areas, from enterprise-wide risk management to third-party assessments and M&A activities. Thanks to advanced analytical models and a data-driven approach, the platform enables the identification of priority mitigation actions and the ongoing monitoring of the risk profile over time through intuitive dashboards. Cyber Risk DIVE can be deployed as a standalone assessment tool or integrated into a wider Cyber Security as a Service engagement.

Our Privacy Management Platform: Privacy Dive
Privacy DIVE is BIP CyberSec's smart and intuitive privacy management platform designed to simplify data protection compliance and turn regulatory obligations into a business enabler. Built to support organisations facing the complexity of GDPR and global privacy regulations, Privacy DIVE provides a centralised, cloud-based environment to map personal data, manage risks, and maintain full accountability. With guided workflows, automation, and clear dashboards, the solution helps companies embed privacy by design into everyday processes, strengthening trust, transparency, and governance while reducing operational effort.

Our Industrial Risk Platform: xDefense
xDefense™ is BIP CyberSec's advanced industrial cybersecurity visibility and risk platform designed to give organisations deep, actionable insight into their Operational Technology (OT) and industrial control environments. In today's Industry 4.0 landscape, where industrial systems are increasingly interconnected and exposed to cyber threats, knowing exactly what you have and how it communicates is the foundation for effective protection and resilience. xDefense™ builds detailed inventories of distributed OT assets, capturing hardware, software, and network

communications to centralise visibility across sites and support proactive risk management. With intuitive dashboards, scalable architecture, and comprehensive reporting, xDefense™ enables companies to identify vulnerabilities, prioritise remediation efforts, and strengthen security governance across complex industrial infrastructures, turning visibility into strategic defence.

8 Re@ck Security Services

The Re@ck Security Center by BIP CyberSec is a next-generation Security Operations Center designed to deliver continuous, 24/7 cyber protection for modern organisations. Combining BIP CyberSec's deep cybersecurity expertise with advanced cloud-based technologies, Re@ck enables real-time threat detection, rapid incident response, and proactive risk mitigation. The platform leverages automation, adaptive analytics, and integrated threat intelligence to reduce complexity and accelerate decision-making. Through tailored monitoring, operational playbooks, and actionable reporting, Re@ck supports organisations in protecting their critical assets and strengthening their overall cyber resilience. Built to scale and adapt to evolving business needs, the Re@ck Security Center empowers clients to confidently face an increasingly complex and dynamic threat landscape.

9 Specialist Cyber Capabilities

Offensive Securit
BIP's offensive security capability includes more than 50 specialists delivering ethical hacking, red teaming, adversary simulation, and phishing exercises.

Each year, the team tests more than 40,000 systems, identifies over ten zero-day vulnerabilities, and completes more than 100 successful engagements. Findings are prioritised clearly, with practical recommendations that support timely remediation and risk reduction.

Data and Identity Protection
Our data and identity protection specialists help organisations safeguard both structured and unstructured information across complex environments. The team brings experience from more than 50 consulting and system integration engagements, defining an end-to-end Data Security methodology from the mapping of information at process level to the implementation of technical controls.

Services include data classification design, data loss prevention strategy, definition of roles and responsibilities, and implementation of technical controls across productivity platforms, email services, and network infrastructure.

Cryptography and Application Security
BIP's cryptography and application security specialists provide deep expertise in encryption, digital certificates, cryptanalysis, and secure application development.

In emerging areas such as post-quantum cryptography (PQC), BIP works with leading technology vendors to assess exposure, understand potential impacts, and define practical and proportionate response strategies.

11 Secure Delivery & Assurance

BIP has extensive experience delivering complex digital products from early proof of concept through to live operation within regulated and high assurance environments.

Cyber security is embedded at every stage of delivery. Systems are designed to protect sensitive information, prevent unauthorised access, and maintain operational integrity from the outset.

Testing is structured, transparent, evidence based, and aligned to client assurance requirements. This includes penetration testing, vulnerability scanning, resilience testing, verification of encryption, identity management, and incident response scenarios.

All systems progress through defined test phases covering functionality, integration, performance, security, and user acceptance. Entry and exit criteria are clearly defined and supported by documented evidence. Test environments reflect live operational conditions to ensure confidence at release.

12 Client Assurance & Reporting

BIP provides clear and comprehensive documentation to support client assurance and governance needs. This includes test execution results, defect logs, remediation tracking, and signed assurance summaries.

Responsibilities are clearly defined across test managers, analysts, cyber specialists, and client stakeholders. This collaborative approach ensures systems are secure, compliant and operationally ready.

13 Value to Clients

Cyber Security as a Service from BIP gives clients confidence that security is built in, tested thoroughly, and managed continuously.

Clients benefit from:

- Reduced cyber risk and improved visibility of exposure
- Strong alignment to recognised national and international standards
- Practical delivery that balances assurance with pace
- Access to deep specialist expertise when required
- A trusted partner that works alongside internal teams

The service is designed to scale with client needs, providing assurance today while building lasting cyber resilience for the future.

14 Contacts

51 Moorgate
London
EC2R 6LL

Chris Walker
Partner

Office: 020 3141 8400
Mobile: +44 791 208 7462

15 About us

Who We Are

BIP is a fast-growing global management consultancy (backed by CVC Capital Partners), employing over 6,000 professionals across 27 offices in 12 countries.

We operate across Europe, the Americas, and the Middle East, including here in the UK, Italy, France, Germany, Spain, Portugal, Switzerland, Austria, Brazil, Chile, Colombia, the UAE, and the US.

We help organisations tackle complex challenges, outpace their competitors, and build a sustainable future through strategic insight, operational excellence, and technology innovation.

In the UK, BIP has been recognised by *The Times* and trusted by FTSE 100 companies, government departments, and industry leaders, establishing itself as one to watch in the consulting landscape.

Our Philosophy: Value, People and Technology

At the heart of everything we do lies a powerful combination: **value, people, and technology**. These three pillars enable us to deliver meaningful, scalable, and lasting outcomes for our clients.

We are value creators and business integrators, combining strategic insight with implementation excellence to help organisations move the dial at pace.

Our work is powered by deep expertise in digital transformation, AI, cloud, and technology-led change, ensuring every solution drives sustainable progress *and* measurable impact.

Our Approach: Design to Deliver

We are doers and makers, NOT just PowerPoint writers.

Everything we do is designed to deliver real, measurable change within defined timelines. We ideate, test, and learn, working closely with clients and partners in an open, collaborative way to ensure every solution is built to last.

Our goal is not only to deliver outcomes, but to transfer knowledge, and empower clients to continue their transformation independently.

This partnership model offers long-term value and enables us to focus on where we can make the next biggest impact.

Our Expertise

With deep sector experience across:

- Financial Services
- Government & Public Sector
- Defence & Industries
- Energy, Utilities & Resources
- Telecoms & Media
- Retail & Services
- Life Sciences
- Commercial Real Estate

We bring sharp insight, proven delivery experience, and technological edge to every engagement.

The recent integration of Verco and Riskcare into BIP UK further strengthens our offering, adding market-leading expertise in net zero strategy, sustainability advisory, and financial risk technology.

Here to Dare

“Here to dare” is more than a motto, it is our mindset.

We dare to think and act differently, to explore beyond limits, and to create opportunities through bold innovation and collaboration.

We believe in shared journeys, celebrating results, milestones, and even challenges, because true responsibility means growing together.

We imagine a future where business thrives through the synergy of technology, humanity, and sustainability.

The BIP World

BIP is a world of innovators, designers, data engineers, change managers, producers, and marketers, all working together, infusing each other with ideas, energy, and passion.

We want to leave a mark with what we do and share a journey with every company we work with.

We’re 6000 people, 47 nationalities, 12 countries, united by a drive to empower organisations through technology and passion.

Our people, the BIPers, are the heart of our success. They thrive in an environment that encourages self-expression, growth, and balance, inspiring them to engage clients with the values they live by.

12 Other Information

The scope of our G-Cloud Service

The scope of our G-Cloud service is defined in this document and the associated features and benefits. It covers the supply of professional services to support the evaluation, selection and deployment of cloud solutions and services for a range of public sector organisations.

Are we a reseller?

BIP is not a reseller, and we are totally independent of all product vendors and solution providers.

Support provided to buyers

When buyers have shortlisted one or more of our services, they may ask clarification questions prior to purchase. This helps them understand, in more detail, if we are the best supplier for them and how they can benefit from our service. We then use our knowledge of the cloud solution marketplace to advise and guide clients through the specification, selection and deployment process.

How users work with this G-Cloud service

Users can use this service to obtain professional advisory support for their GenAI needs. This can be on a short term, long term or ad-hoc basis using either selected specialists or a team approach.

Service onboarding and off-boarding process

When a client buys us using one of our G-cloud services, we typically undertake an initiation process at the start of the service to ensure the client's requirements are fully understood and that they are clear about what we will do, how we will do it and what we will deliver. We will also discuss and agree how any issues will be raised and managed from either side during the service operation.

At the end of the service, we will typically undertake a review with the client to ensure they are happy with what has been delivered and that their expectations have been met. We can also discuss and future support if this is appropriate.

Pricing

We provide services and our day rates are shown in the SFIA rate card for this service.

Service definition and how it will be delivered

The services defined in this document and the associated features and benefits will be delivered by one or more of our consultants with full management support and quality assurance from our public sector portfolio leadership. The service will be

delivered from our office, working remotely or at the client's offices, depending on which is most appropriate.

Our security certifications and standards

BIP has the Cyber Essentials Plus Certificate of Assurance which is renewed each year.

Our approach to personnel security

BIP's personnel checking process for new employees includes all components of the employment processes described on Gov.uk, including validating their right to work in the UK.

We cover checking original versions of the necessary documents with the new joiner and making and retaining copies of these documents.

The identity documents and other information gathered are sufficient to enable Government Security checks to be undertaken. BIP maintains an extensive pool of appropriately security cleared consultants.