



Service Delivery Approach: Cyber as a Service

Executive Overview

Redbay “Cyber as a Service” (CyaaS) is designed to support your digital transformation and cyber resilience objectives. The service provides:

- Risk Management – embedding cyber security in risk management to inform business decision making and active risk management of the top cyber security risks to improve your cyber resilience.
- Governance and Compliance – compliance against legal and industry frameworks to demonstrate business maturity and drive continuous improvement.
- Security Design – embedding security in the architecture and design process to create lowest cost secure outcomes.
- Incident Management – We will embed leading practices of cyber security incident management and provide leadership of critical incidents to provide a swift resolution to any incidents.

The service delivery model is built on deep operational experience, industry best practices, and a commitment to continuous improvement. This approach ensures that all stakeholders are consulted, trained, and supported, enabling you to make smarter, data-driven decisions and maintain resilience against cyber threats.

Service Structure

Thematic Integration

Service delivery is organized around themes identified with you, each mapped to specific outputs and deliverables. This thematic approach ensures optimal integration and avoids siloed operations, delivering best value and benefits from the service. Monthly face-to-face meetings, such as the CyaaS all-hands call, foster knowledge transfer, challenge, and innovation in a psychologically safe environment.

Stakeholder Alignment

Outputs and themes are aligned to two key stakeholder groups:

- **Contract Managers and Board members**



- **Users of Outputs:** CISO, Senior Responsible Officers, System Owners, Delivery Team Security Leads, IT Security Officers, Capability Managers, Risk Managers, Information Asset Owners

Regular meetings and reporting cycles ensure that all parties are informed and engaged in service delivery.

Service Reporting and Innovation

- **Monthly Reporting:** All outputs are summarized monthly for the Risk Management lead, who provides overarching reports to contract managers. Output leads maintain regular contact with their associated users onsite.
- **Innovation and Value for Money (VFM):** Redbay leverages monthly all-hands meetings, KANBAN methodology, and cross-sector best practices to drive innovation. Cyber security is embedded as business-as-usual (BAU) in your processes.

Skills and Experience

Service delivery is supported by a team of consultants, each bringing specialized skills and extensive experience of commercial and Government networks and frameworks. Full biographies are available.

Methodology

Risk Management

The central approach is to create an efficient risk information flow, providing a comprehensive understanding of cyber security risks across the client's enterprise. The methodology is based on the ISO Risk Management Framework and the NIST Cyber Security Framework (CSF), tailored to your needs. This ensures that risk owners and managers have clear benchmarks and standards, enabling informed decision-making and prioritization of mitigation activities.

Governance and Compliance

Governance, risk, and compliance (GRC) activities are coherently integrated using NIST CSF and NCSC CAF. Audits are risk-led, providing independent scrutiny and actionable recommendations. Governance drives completion of actions and continuous improvement.

Security Design



Using a secure by design approach, Redbay will assist you with understanding your network requirements and how they might best be delivered, mitigating security risks and providing knowledge of control measures to adopt using industry best practice.

Security Incident Management

Redbay has the necessary skills and experience to assist you in the management of cyber security incidents. Understanding the impact and priority of the incident, having worked with you during the design and implementation process and providing the risk oversight and management, allows us to quickly recommend the remediation and recovery plans required for bringing a service back online.

Continuous Improvement

Redbay's service delivery model emphasizes continuous improvement through:

- Regular evaluation of processes and outcomes
- Adoption of industry standards and best practices and continuous training
- Stakeholder engagement and feedback
- Attendance at industry conferences and workshops to stay ahead of evolving cyber threats



Conclusion

Redbay's "Cyber as a Service" delivers a robust, integrated, and innovative approach to cyber security for you. The service structure, reporting, continuity measures, and methodology are all designed to meet the client's operational outcomes and digital vision statements, ensuring resilience, efficiency, and ongoing improvement