CIRRO

Lot 3 Cloud Support Services – Cirro Professional Services

Security Strategy, Risk Management and Design 3
Security Strategy and Governance 3
Risk Management and Assurance 3
Secure Design and Architecture 3
Delivery Support and Integration 4
Technology & Cloud Strategy, Business Case and Project Planning 5
Technology and Cloud Strategy 5
Business Case Development 5
Risk, dependency, and sensitivity analysis 5
Project and Programme Planning 5
Integration with Delivery and Assurance 6
Disaster Recovery & Restoration Strategy - Cyber Security 7
Cyber-Focused Resilience Strategy 7
Recovery Objectives and Architecture 7
Planning and Playbooks 7
Testing and Assurance 8
Outcomes for Buyers 8
Security - Baseline Health Check 9
Purpose and Scope 9
Assessment Approach 9
Evidence-Based Findings 9
Recommendations and Roadmap 10
Reporting and Stakeholder Engagement 10
Outcomes for Buyers 10
Cyber Security – External Vulnerability (Penetration) Testing 11
Purpose and Objectives 11
Testing Approach and Methodology 11
Risk-Based Focus 11
Reporting and Remediation Support 12
Integration with Wider Security Activities 12
Outcomes for Buyers 12

Security Strategy, Risk Management and Design

Our Security Strategy, Risk Management and Design service supports UK public sector organisations to design, assure and operate secure digital and cloud services that are proportionate to risk, compliant with policy, and aligned to organisational objectives. The service provides expert security leadership across strategy, architecture, and delivery, ensuring security is embedded from the outset rather than applied retrospectively.

Security Strategy and Governance

We work with buyers to define a clear, outcome-focused security strategy aligned to business priorities, regulatory obligations, and UK government policy. This includes assessing current security maturity, identifying gaps, and defining a pragmatic roadmap for improvement. Strategies are designed to be proportionate, avoiding unnecessary controls while ensuring risks are appropriately managed.

Our approach aligns with recognised standards and guidance, including NCSC Cloud Security Principles, ISO 27001, and government risk management frameworks. We support the development of security policies, operating models, and governance structures that enable consistent decision-making and accountability across programmes and suppliers.

Risk Management and Assurance

We provide structured, evidence-based risk management throughout the service lifecycle. This includes identifying and assessing information, cyber, operational, and supply chain risks, and supporting buyers to make informed, defensible risk decisions.

Risk activities include:

- Threat modelling and risk identification
- Risk assessment and prioritisation
- Definition of mitigations and control selection
- Support for risk acceptance and escalation
- Ongoing risk tracking and reporting

We support buyers through assurance activities such as architecture reviews, supplier assurance, and security risk assessments, providing clear recommendations and actionable outputs. Our approach ensures security risks are visible, owned, and managed rather than hidden within technical detail.

Secure Design and Architecture

We embed security into service and system design, ensuring solutions are secure by design and by default. This includes developing security architectures that support modern cloud and hybrid environments while maintaining compliance with government expectations.

Design services include:

- Secure cloud and platform architecture
- Identity and access management design
- Data protection and encryption design
- Network and segmentation models
- Logging, monitoring, and incident response design

Design outputs are documented clearly and are suitable for use in delivery, accreditation, and audit activities. We ensure designs are practical to implement and support future scalability and change.

Delivery Support and Integration

We work collaboratively with delivery teams, architects, and suppliers to ensure security requirements are implemented effectively and do not create unnecessary delivery friction. Security is integrated into agile and iterative delivery models, supporting continuous improvement and early risk reduction.

Outcomes for Buyers

- By using this service, buyers gain:
- A clear and proportionate security strategy
- Improved visibility and control of security risk
- Secure, compliant service designs
- Reduced likelihood of late-stage security issues
- Greater confidence in supplier and service assurance

This service enables buyers to make confident security decisions while delivering digital and cloud services at pace and with reduced risk.

Technology & Cloud Strategy, Business Case and Project Planning

Our Technology & Cloud Strategy, Business Case and Project Planning service supports UK public sector organisations to define, justify, and deliver technology and cloud programmes that are aligned to organisational objectives, policy requirements, and value-for-money expectations. The service provides structured support from early strategic intent through to delivery-ready plans, enabling confident decision-making and successful outcomes.

Technology and Cloud Strategy

We work with buyers to develop clear, actionable technology and cloud strategies that align digital ambition with operational reality. Strategies are rooted in business need and policy context, including Cloud First, Technology Code of Practice, and service standard expectations. We assess the current technology landscape, identify constraints and opportunities, and define a target state that supports improved service delivery, resilience, and scalability.

Our approach ensures strategies are pragmatic and prioritised, providing a roadmap that balances modernisation, risk reduction, and affordability. We explicitly consider legacy transition, skills, security, data, and supplier dependencies to ensure strategies are deliverable and sustainable.

Business Case Development

We support the development of robust business cases that enable buyers to secure funding, approvals, and stakeholder confidence. Business cases are structured in line with HM Treasury and public sector best practice, ensuring clarity of benefits, costs, risks, and delivery approach.

Business case activities include:

- Definition of strategic need and objectives
- Options appraisal and recommended approach
- Cost modelling and affordability analysis
- Benefits identification and realisation planning

Risk, dependency, and sensitivity analysis

We ensure business cases are evidence-based, proportionate, and aligned to the scale and complexity of the initiative. Outputs are suitable for internal governance, investment boards, and external assurance where required.

Project and Programme Planning

We translate strategy and business cases into clear, delivery-ready project and programme plans. This includes defining delivery models, governance structures, and realistic timelines that reflect public sector constraints and assurance requirements.

- Planning services include:
- Delivery model and sourcing strategy definition

- Phased delivery and milestone planning
- Governance and decision-making structures
- Resource and capability planning
- Risk and dependency management

Plans are designed to support iterative and agile delivery approaches while maintaining appropriate controls and transparency. We ensure plans are adaptable, enabling buyers to respond to change without losing sight of strategic outcomes.

Integration with Delivery and Assurance

We work closely with delivery teams, commercial leads, and assurance functions to ensure strategic intent is maintained throughout delivery. Our approach supports alignment between strategy, procurement, security, and delivery, reducing the risk of misalignment or rework.

Outcomes for Buyers

- By using this service, buyers benefit from:
- Clear and coherent technology and cloud strategies
- Well-evidenced business cases that support approval
- Delivery-ready plans with realistic timescales
- Improved confidence in investment and delivery decisions
- Reduced delivery risk and stronger governance

This service enables public sector organisations to move from ambition to execution with clarity, control, and confidence.

Disaster Recovery & Restoration Strategy - Cyber Security

Our Disaster Recovery & Restoration Strategy – Cyber Security service supports UK public sector organisations to design, validate, and implement cyber-resilient recovery capabilities that ensure critical services can be restored safely and effectively following cyber incidents, system failures, or major disruptions. The service focuses on resilience by design, ensuring recovery arrangements are secure, tested, and aligned to organisational risk appetite and policy obligations.

Cyber-Focused Resilience Strategy

We work with buyers to define a clear disaster recovery and restoration strategy that explicitly addresses cyber threats such as ransomware, destructive attacks, insider compromise, and supply chain incidents. Strategies are aligned to organisational priorities, service criticality, and tolerance for disruption, ensuring recovery objectives are realistic and achievable.

Our approach aligns with NCSC guidance, government resilience expectations, and recognised standards, supporting buyers to demonstrate appropriate preparedness and assurance. We consider both technical and operational dependencies, ensuring recovery strategies extend beyond infrastructure to people, processes, and third-party services.

Recovery Objectives and Architecture

We support the definition of recovery objectives, including Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), based on business impact and risk. These objectives inform the design of secure recovery architectures that prioritise integrity and assurance over speed alone.

Design activities include:

- Cyber-resilient backup and recovery models
- Segregated and immutable backup strategies
- Clean-environment restoration approaches
- Identity, access, and privilege recovery
- Secure configuration and baseline restoration

We ensure recovery designs account for the need to verify system integrity before restoration, reducing the risk of reinfection or repeated compromise.

Planning and Playbooks

We develop practical, role-based disaster recovery and cyber restoration plans that enable coordinated and controlled response during incidents. Plans clearly define responsibilities, decision points, escalation paths, and communications, supporting effective execution under pressure.

Deliverables may include:

- Cyber-specific disaster recovery strategies
- Restoration and rebuild playbooks
- Incident-driven recovery decision frameworks

- Third-party and supplier recovery coordination
- Alignment with wider business continuity plans

Plans are designed to be usable, tested, and regularly reviewed, rather than static documents.

Testing and Assurance

We support buyers to validate recovery strategies through structured testing and assurance activities. This includes tabletop exercises, scenario-based testing, and technical recovery validation, ensuring plans work in practice and gaps are identified early.

Testing focuses on:

- Cyber incident scenarios
- Decision-making and governance under stress
- Recovery sequencing and dependencies
- Communication and stakeholder coordination

Findings are documented with clear recommendations and prioritised improvement actions.

Outcomes for Buyers

By using this service, buyers gain:

- A cyber-resilient disaster recovery and restoration strategy
- Clear, tested recovery objectives and plans
- Reduced risk of prolonged or unsafe recovery
- Improved confidence in cyber incident response
- Stronger assurance for regulators and stakeholders

This service enables public sector organisations to recover from cyber disruption safely, decisively, and with confidence.

Security - Baseline Health Check

Our Security – Baseline Health Check service provides UK public sector organisations with a clear, evidence-based assessment of their current cyber and information security posture. The service establishes a practical baseline of security maturity, identifies priority risks and gaps, and provides actionable recommendations to improve resilience, compliance, and operational assurance.

Purpose and Scope

The Baseline Health Check is designed to give buyers rapid visibility of their security strengths and weaknesses across people, process, and technology. It is suitable for organisations at any stage of maturity and can be applied to cloud platforms, on-premise environments, hybrid services, or specific programmes and suppliers.

The service is proportionate and risk-based, avoiding unnecessary complexity while ensuring meaningful assurance. It is commonly used to support strategic planning, investment decisions, audit preparation, supplier assurance, or as a precursor to cloud migration or service transformation.

Assessment Approach

We conduct the health check using a structured, repeatable methodology aligned to recognised standards and UK government guidance, including NCSC principles and ISO-aligned controls. The assessment combines documentation review, stakeholder interviews, and targeted technical validation where appropriate.

Key assessment areas typically include:

- Security governance, policies, and accountability
- Risk management and risk ownership
- Identity and access management
- Data protection and information handling
- Logging, monitoring, and incident management
- Vulnerability management and patching
- Third-party and supply chain risk

The scope can be tailored to focus on specific systems, services, or risk areas, ensuring relevance and value.

Evidence-Based Findings

Findings are evidence-led and clearly documented. We distinguish between design gaps, implementation weaknesses, and operational issues, enabling buyers to understand root causes rather than symptoms.

Each finding is:

- Mapped to recognised good practice

- Assessed for likelihood and impact
- Prioritised based on risk and business criticality
- Clearly explained in plain language

This ensures outputs are accessible to both technical and non-technical stakeholders.

Recommendations and Roadmap

We provide practical, prioritised recommendations that are realistic within public sector constraints. Recommendations focus on achievable improvements rather than theoretical best practice, balancing security, cost, and delivery effort.

Outputs include:

- A clear security maturity baseline
- A prioritised risk register
- Short-, medium-, and long-term improvement actions
- Dependencies and quick wins

Where required, we can also provide indicative effort estimates or link recommendations to wider strategy, architecture, or delivery plans.

Reporting and Stakeholder Engagement

Results are presented in a concise report suitable for senior stakeholders, audit teams, and delivery leads. We provide clear summaries and visual indicators to support decision-making and governance.

We also offer walkthrough sessions to explain findings, validate understanding, and support next-step planning.

Outcomes for Buyers

By using this service, buyers gain:

- Clear visibility of their current security posture
- A defensible security baseline for assurance and audit
- Prioritised actions aligned to real risk
- Improved confidence in security decision-making
- A foundation for continuous security improvement

The Security – Baseline Health Check enables organisations to move forward with clarity, confidence, and control.

Cyber Security – External Vulnerability (Penetration) Testing

Our Cyber Security – External Vulnerability (Penetration) Testing service provides UK public sector organisations with an independent, controlled assessment of the security of their externally exposed systems and services. The service identifies vulnerabilities that could be exploited by real-world attackers and provides clear, actionable insight to reduce cyber risk and improve overall security posture.

Purpose and Objectives

The service is designed to help buyers understand how their internet-facing infrastructure, applications, and services would withstand attack from an external threat actor. It supports assurance, compliance, and risk management objectives by identifying weaknesses before they can be exploited, enabling timely remediation and informed risk decisions.

External testing is suitable for cloud platforms, web applications, APIs, remote access services, and supporting infrastructure, and is commonly used to support go-live decisions, accreditation, supplier assurance, and ongoing security monitoring.

Testing Approach and Methodology

Testing is performed by experienced, UK-based security professionals using industry-recognised methodologies aligned to NCSC guidance, OWASP, and CREST principles. The approach combines automated vulnerability discovery with expert manual testing to identify both common weaknesses and more complex exploitation paths.

Testing activities may include:

- Discovery and mapping of externally exposed assets
- Identification of configuration weaknesses and outdated components
- Testing for known vulnerability classes (e.g. OWASP Top 10)
- Authentication and access control testing (where in scope)
- Secure configuration and protocol assessment

Testing is conducted in a controlled manner to minimise operational risk and is agreed in advance with the buyer, including scope, timing, and rules of engagement.

Risk-Based Focus

Findings are assessed in context, taking into account service criticality, data sensitivity, and exposure. We avoid reporting large volumes of low-value findings and instead focus on vulnerabilities that present genuine risk to the organisation.

Each issue is:

- Validated to reduce false positives
- Assessed for likelihood and impact
- Prioritised using a clear risk rating

- Mapped to relevant good practice or guidance

This enables buyers to focus remediation effort where it matters most.

Reporting and Remediation Support

We provide clear, concise reports suitable for technical teams, security leads, and governance stakeholders. Reports include an executive summary, detailed findings, and practical remediation guidance.

Reporting outputs include:

- Overview of testing scope and methodology
- Summary of key risks and exposure
- Detailed vulnerability findings with evidence
- Clear remediation recommendations
- Optional re-test validation

We also offer walkthrough sessions to explain findings, answer questions, and support remediation planning.

Integration with Wider Security Activities

External vulnerability testing can be delivered as a standalone assurance activity or integrated into broader security programmes, including security health checks, cloud assurance, and ongoing vulnerability management. The service supports continuous improvement rather than one-off compliance.

Outcomes for Buyers

By using this service, buyers gain:

- Independent assurance of external security posture
- Early identification of exploitable vulnerabilities
- Clear, prioritised remediation actions
- Reduced risk of external compromise
- Improved confidence in public-facing services

This service enables public sector organisations to proactively reduce cyber risk and strengthen external defences.