



G-Cloud 15 (RM1557.15) Excelsior Solutions Ltd

IT delivery support services

Service Definition

January 2025





1 Introduction	3
1.1 Document structure	3
1.2 How to use this document	3
2 Service description	4
2.1 About our service	4
2.2 Delivery framework	4
2.3 Service features / benefits	5
2.4 Service scope	6
2.4.1 Add-ons and extensions	6
2.4.2 Cloud deployment models	7
2.4.3 Service constraints	7
2.4.4 System requirements	7
2.5 Reselling	7
2.6 User support	7
2.6.1 Support details	8
2.6.2 Accessibility and usability	9
2.7 How users work with our service	11
2.7.1 Browsers	11
2.7.2 Desktop application	11
2.7.3 Mobile	11
2.7.4 Service interface	11
2.7.5 API	11
2.7.6 Accessibility and usability	12
2.7.7 Customisation	12
2.7.8 Service levels and availability	12
3 G-Cloud alignment information	13
3.1 Section introduction	13
3.2 Onboarding and offboarding processes	13
3.2.1 Onboarding	13
3.2.2 Offboarding	14
3.3 Data	15
3.3.1 Data importing and exporting	15
3.3.2 Data-in-transit protection	15
3.3.3 Asset protection	15
3.4 Availability and resilience	15
3.4.1 Guaranteed availability	15
3.5 Governance	15
3.6 Security	16
3.6.1 Operational security	16
3.6.2 Staff security	16
3.7 Auditing	17
3.7.1 Compliance and quality management	17
3.8 Backup, restore & disaster recovery	17
3.9 Training	17
3.10 Service pricing	18
3.11 Invoicing process	18
3.12 Termination terms	18
4 Security and data governance	19
4.1 Data protection and encryption	19
4.2 Data at rest, storage locations, and physical security	19
4.3 Data sanitisation and disposal	19
4.4 Information security management and certifications	19
4.5 Identity and access management	19
5 Supplier information	19
5.1 About us	19
5.2 How to buy	19



1 Introduction

1.1 Document structure

This Service Definition document provides information about the services offered by Excelsior Solutions Limited under the Crown Commercial Service (CCS) G-Cloud 15 Framework. It is intended to support public sector buyers by clearly explaining the scope, functionality, security, pricing approach, and service management arrangements associated with our offerings, and by outlining how buyers can engage with us through the framework.

The document is structured into three core sections:

- **Service description:** Provides an overview of Excelsior Solutions Limited's digital and professional services, including key features, benefits, delivery approach, and assurance measures such as security, data protection, and compliance with relevant standards
- **Operational delivery and framework alignment:** Describes how services are delivered under the G-Cloud 15 framework, including onboarding, service management, change control, service levels, and alignment with G-Cloud contractual and operational requirements
- **Supplier information:** Summarises Excelsior Solutions Limited's organisational background, mission and values, relevant public sector experience, and clear guidance on how buyers can procure our services via the G-Cloud Digital Marketplace

Each section is designed to enable buyers to quickly locate information relevant to their stage of the procurement lifecycle, from initial service evaluation through to contract award and service delivery.

This Service Definition describes Excelsior Solutions IT Delivery Support Services offered under Lot 3 (Cloud Support – Professional Services) of the G-Cloud 15 Framework. The service provides project and programme management, governance, and advisory support to public sector organisations delivering cloud and cloud-enabled change initiatives.

The service is non-technical and non-operational in nature. We do not host platforms, configure systems, integrate software, or provide managed services. Responsibility for technical delivery, platform operation, and system security remains with the buyer and/or their appointed technology suppliers.

1.2 How to use this document

This document is intended to support public sector buyers throughout the full G-Cloud procurement lifecycle, from early service evaluation through to contract award and ongoing service delivery. It is structured to provide clear, accessible information that enables informed decision-making at each stage of the process.

For initial assessment and early-stage evaluation, Section 2 (Service description) outlines the scope of services offered by Excelsior Solutions Limited, including our delivery approach, methodology, and the key benefits provided. This section is designed to help buyers determine how well our services align with their organisational needs and objectives.

For due diligence and contract preparation, Section 3 (G-Cloud alignment information) provides detailed information on how our services are delivered in accordance with G-Cloud 15 requirements. This includes onboarding arrangements, service management and support processes, service levels, change control mechanisms, and exit procedures.

To support assurance around security, data protection, and regulatory compliance, Section 4 (Security and data governance) describes our information security framework, data handling and protection standards, and business continuity and resilience measures.



For supplier verification and procurement purposes, Section 5 (Supplier information) provides background information on Excelsior Solutions Limited, including relevant experience and accreditations, and explains how buyers can procure our services through the G-Cloud Digital Marketplace.

2 Service description

2.1 About our service

Excelsior Solutions provides advisory-led project and programme management services that help public sector organisations plan, govern, and assure the delivery of complex IT and digital change initiatives. Our service focuses on governance, coordination, assurance, and stakeholder alignment, enabling buyers to deliver outcomes with reduced risk and improved transparency.

We work alongside client teams and third-party suppliers to support structured decision-making, clear accountability, and effective programme control. We do not assume operational ownership of systems, environments, or live services. Our services support:

- Programme and project governance across the delivery lifecycle
- Planning, dependency management, and delivery assurance
- Business analysis and requirements clarification
- Architecture and design assurance (non-delivery)
- Supplier coordination and commercial oversight
- Transition planning and service acceptance coordination

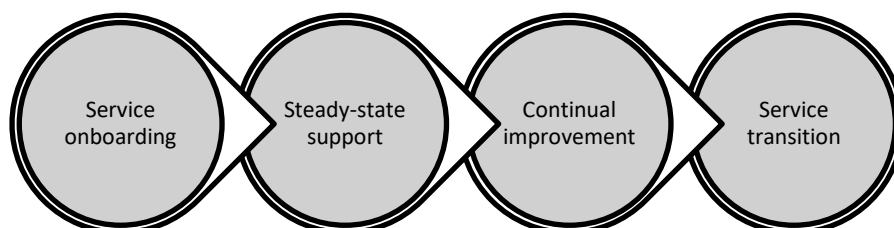
2.2 Delivery framework

Services are delivered using a governance-led delivery framework aligned to recognised public-sector best practice. The framework emphasises:

- Defined roles and responsibilities
- Clear reporting and escalation routes
- Risk, issue, and dependency management
- Evidence-based decision-making

Our framework supports multi-supplier environments by providing governance, assurance and coordination across delivery partners while maintaining buyer ownership of technical implementation and operations.

Structured around a clearly defined lifecycle, which includes:



By focusing on consistent configuration, clear processes and proactive service management, we reduce operational risk, minimise service disruption and ensure reliable support outcomes across all phases of delivery.



2.3 Service features / benefits

Showcasing the strength of our advisory services, clients who procure our recommended solutions benefit from:

Feature	Benefit
Programme and project delivery management	Improves delivery certainty through structured governance and planning
Delivery assurance and governance reporting	Reduces delivery delays by accelerating decision-making and approvals
Business analysis and requirements management	Clarifies requirements to reduce rework and scope creep
Enterprise architecture support and design governance	Improves stakeholder alignment through structured engagement and facilitation
Stakeholder engagement and facilitation workshops	Strengthens architecture compliance and delivery consistency across programmes
Agile delivery management and sprint support	Increases transparency through clear reporting, RAID, and dashboards
Risks, Assumptions, Issues, and Dependencies (RAID) management and delivery risk controls	Reduces operational risk through transition and readiness planning
Service transition planning and operational readiness	Accelerates cloud adoption through coordinated governance, planning and assurance
Vendor coordination and delivery assurance	Improves supplier performance through active management and accountability
Benefits tracking and continuous improvement planning	Enhances outcomes through benefits tracking and continuous improvement



2.4 Service scope

Helping public sector organisations achieve outcomes efficiently and with reduced risk, our service provides structured delivery support across cloud and digital programmes. Ensuring projects stay on track without disrupting live services, we improve governance, delivery assurance, stakeholder alignment, and execution quality.

Embedding delivery leads, business analysts, and architects into client teams, we work flexibly within existing operational and technical landscapes. Enabling organisations to maintain control over delivery processes and decision-making, our approach supports effective programme management, clear reporting, and structured escalation.

Maximising delivery effectiveness, we maintain artefacts such as delivery plans, RAID logs, stakeholder maps, and requirements catalogues. This ensures risks are managed proactively, progress is transparent, and decisions are evidence-based.

Supporting iterative and collaborative delivery, we facilitate workshops, sprint planning, and governance forums. Our teams accelerate project mobilisation, clarify requirements, and improve alignment between technical and business stakeholders.

The service provides people-based professional support to enhance governance and delivery effectiveness. Typical activities include:

- Producing and maintaining delivery artefacts (plans, RAID logs, reports)
- Facilitating governance forums and workshops
- Supporting programme mobilisation and delivery planning
- Coordinating supplier activities and dependencies

The service does not include:

- Technical configuration or integration
- Platform hosting or operation
- System monitoring or incident management
- Managed services or BAU support

2.4.1 Add-ons and extensions

Is this service an add-on or extension to other software services?

This service is a standalone professional service. It is not an add-on to, nor an extension of, any software or cloud platform. Enabling application and workload-level security controls, policy enforcement and continuous visibility to be applied consistently across existing environments, without imposing proprietary hosting models or requiring wholesale replacement of incumbent technologies, the service integrates with existing security and operations tooling, including:

- Identity and Access Management (IAM) platforms
- Security Information and Event Management (SIEM) systems
- Security Orchestration, Automation and Response (SOAR) platforms
- IT Service Management (ITSM) tools
- Cloud security and Zero Trust-aligned architectures



2.4.2 Cloud deployment model

The service is delivered remotely using buyer-approved collaboration tools and processes. No Excelsior-hosted platforms are required. Delivery arrangements are agreed during onboarding.

2.4.3 Service constraints

- Delivery is primarily remote
- Effectiveness depends on timely access to stakeholders and information
- The service relies on buyer and supplier cooperation

2.4.4 System requirements

No specialist hardware or software is required. Access to standard collaboration tools and modern web browsers is sufficient.

2.5 Reselling

No reselling. This service does not involve the resale of third-party software, licences, platforms or services.

2.6 User support

We provide timely, effective support throughout the delivery and operation of our services. Our support model is clear, accessible, and proportionate, with defined channels, response targets, and escalation routes to manage and resolve enquiries efficiently.

Support arrangements are tailored to the nature and criticality of each engagement during onboarding. This ensures customers understand how to access support, the levels of service available, and how issues are escalated where required. Where appropriate, a named point of contact is provided for consistent communication and accountability.

2.6.1 Support details

Do you provide email support?

Yes. We commit to respond to priority requests within 1 hour, and standard queries within 4 hours.

Do you provide online ticketing support?

No.

Do you provide phone support?



Yes. We commit to respond to priority calls within 1 hour, and standard queries within 4 hours.

Do you provide web chat support?

No.

Do you provide AI-driven self-service tools (BOT)?

No.

When can users get phone support?

Monday-Friday 09:00-17:00, extended hours available by agreement.

When is each support channel available?

Monday-Friday 09:00-17:00, extended hours available by agreement.

How quickly do you respond to questions?

We commit to respond to priority calls within 1 hour, and standard queries within 4 hours.

Are response times different at weekends?

We do not offer weekend support.

Can third-party contractors access support?

Yes.

Describe your support levels

Our IT Delivery Support Services provide structured, responsive support throughout the programme lifecycle. Support is primarily delivered remotely, using email, phone, and collaboration tools, with onsite assistance available by exception and prior agreement. Ensuring clear communication and accountability, we allocate a named point of contact where appropriate.

We operate defined response targets, with priority enquiries responded to within 1 hour and standard queries within 4 hours. Support levels are tailored to each customer engagement, reflecting project criticality, size, and complexity. Extended hours or weekend support can be arranged as required.



Enabling rapid resolution of complex issues, our escalation routes are clearly defined. Monthly reviews and progress updates ensure transparency and alignment with customer expectations. Where third-party platforms are involved, product-specific support is delivered in line with vendor SLAs.

Do you provide a technical account manager?

Yes. For our IT Delivery Support Services, we provide a named delivery lead and a Customer Engagement Manager for each engagement. These roles act as your primary points of contact, overseeing day-to-day delivery, governance, and stakeholder alignment.

Where the scope requires technical expertise (such as enterprise architecture, business analysis, or specialised cloud delivery support) we assign technical specialists. These specialists provide guidance, review artefacts, and support escalation of complex issues.

Together, the delivery lead, Customer Engagement Manager, and technical specialists ensure that customers have dedicated, accountable oversight, clear reporting, and access to expert advice throughout the programme lifecycle, aligning delivery to objectives, mitigating risk, and improving overall outcomes.

This approach provides a similar level of support to a Technical Account Manager or Cloud Support Engineer, tailored to programme delivery rather than platform operations.

2.6.2 Accessibility and usability

What accessibility standards does your service interface meet?

Excelsior Solutions delivers this service using buyer-approved collaboration and communication tools, for example email, video conferencing and document-sharing platforms. We do not provide bespoke software interfaces. Accessibility is therefore primarily determined by the buyer's chosen tools and environments.

To support inclusive delivery, we apply accessible working practices including:

- Providing documents in common formats (Word, PowerPoint, PDF) and using clear headings and structured layouts
- Running workshops and meetings in ways that support remote participation and diverse user needs
- Offering alternative formats or reasonable adjustments where required and agreed with the buyer

Where a buyer requires specific accessibility arrangements (for example captioning, transcript provision, or accessible templates), these are confirmed during onboarding and reflected in the delivery plan.

Describe how your service is accessible

Our service is designed to be accessible to all users involved in programme delivery, regardless of location or device. Support, reporting, and collaboration are provided via standard web browsers and widely used collaboration tools, requiring no specialist hardware or software.

Workshops, training, and documentation are delivered inclusively, with materials provided in accessible formats and sessions structured to accommodate diverse needs. Where third-party tools are used, accessibility aligns with their compliance to WCAG 2.2 A/AA standards.



We also tailor engagement approaches during onboarding to address specific accessibility requirements, ensuring all stakeholders can participate fully in planning, delivery, and governance activities.

Describe any interface testing with assistive technology

As our service primarily uses standard collaboration tools, dashboards, and web-based documentation, we do not develop bespoke interfaces requiring dedicated assistive technology testing. However, where third-party tools are used, we ensure they are compatible with common assistive technologies, such as screen readers and keyboard navigation, and align with WCAG 2.2 A/AA accessibility standards.

We also review materials and session formats during onboarding to ensure they are accessible to all participants, including those using assistive devices. Any accessibility issues identified in tools or content are addressed through alternative formats, adjusted workflows, or guidance to maintain full participation in programme delivery activities.

How is your documentation accessible?

All documentation provided as part of our service (including playbooks, delivery handbooks, templates, reporting packs, and training materials) is designed to be accessible to all stakeholders. We provide materials in standard, widely compatible formats (such as PDF, Word, and online collaboration platforms) that support screen readers, keyboard navigation, and other assistive technologies.

Content is structured with clear headings, tables, and visual cues to aid readability and navigation. Ensuring that stakeholders with diverse accessibility requirements can review, understand, and use the documentation effectively, we also provide guidance, explanations, and alternative formats where needed.

During onboarding, any specific accessibility requirements can be identified and accommodated, including formatting adjustments, annotated guides, or tailored digital materials. This ensures that all participants in workshops, training, and delivery governance can access and engage with information fully and independently.

Documentation formats

Our service provides all documentation in widely accessible and standard formats, including:

- PDF
- Microsoft Word/Excel
- PowerPoint
- Online collaboration platforms, such as Microsoft Teams, Zoom
- CSV / XML

All formats are chosen for compatibility with public sector systems and assistive technologies, supporting screen readers, keyboard navigation, and other accessibility tools. Alternative formats can be provided on request to meet specific accessibility or operational needs.

2.7 How to use our service

2.7.1 Browsers



This service does not require the use of an Excelsior-operated web application. Where browser access is required to join buyer-approved collaboration tools (for example Teams/SharePoint or equivalent) or to view documents in the buyer's environment, users should use a modern, supported browser (such as Microsoft Edge, Google Chrome, or Mozilla Firefox) in line with their organisation's IT policy.

2.7.2 Desktop application

No Excelsior desktop application is required. Users access service outputs using standard productivity tools and buyer-approved collaboration platforms. Any optional tooling used to manage project artefacts (for example document templates, reporting packs, or spreadsheets) is provided in common formats and does not require specialist software beyond typical office applications.

2.7.3 Mobile

The service can be consumed by mobile users where the buyer's collaboration tools and policies permit. Participants may join calls, review documents, and provide approvals via mobile devices using buyer-approved applications. Excelsior does not require installation of additional mobile applications.

2.7.4 Service interface

This service is people-based professional support and does not provide a dedicated software interface. Service outputs are delivered through:

- Agreed governance meetings and workshops
- Written deliverables and artefacts (plans, RAID logs, requirements, status reports)
- Buyer-approved collaboration tools and repositories

Where the buyer provides access to their own tools (for example their PMO platform or document repository), we work within those tools in line with buyer policies and permissions.

2.7.5 API

Our service does not require API integration.

2.7.6 Accessibility and usability

The service is designed to be usable with minimal technical barriers by relying on common, widely adopted collaboration methods and formats. Usability is supported through:

- Clear, standardised templates and consistent reporting formats
- Plain-language communications and structured governance routines
- Role-based engagement (stakeholders receive only the information relevant to their responsibilities)
- Onboarding to confirm ways of working, responsibilities, and communication routes

Any specific usability or accessibility needs are captured during onboarding and managed throughout delivery.

2.7.7 Customisation

The service is tailored to each buyer's needs through **delivery approach and governance**, not software configuration. Customisation may include:

- Agreeing delivery cadence, governance structure, and reporting requirements
- Tailoring templates and artefacts (for example RAID format, status reporting, action trackers)
- Aligning roles, responsibilities, and escalation routes to the buyer's operating model



- Adapting engagement methods to buyer constraints (for example security, approvals, and availability)

We do not customise or configure buyer systems or third-party platforms as part of this service.

2.7.8 Service levels and availability

Professional services support is available Monday to Friday, 09:00–17:00 (UK time), excluding UK public holidays, unless otherwise agreed in the Order Form.

Service levels for this offering focus on professional engagement responsiveness (not platform uptime or incident management). Typical targets are:

- Acknowledgement of service requests (for example questions about deliverables, governance, or scheduling) within one business day
- Response/resolution aligned to the agreed delivery plan, governance cadence, and buyer priorities

This service does not provide:

- System availability guarantees
- Platform monitoring or incident response
- Managed service operations or technical support SLAs

Any platform availability or technical support obligations remain the responsibility of the buyer and/or the relevant cloud service provider.



3 G-Cloud alignment information

3.1 Section introduction

Designed for use in public sector environments, we deliver this service using a structured, lifecycle-based delivery model. A key competitive differentiator, our delivery philosophy prioritises clear accountability, predictable outcomes, and secure, compliant delivery while remaining flexible to each buyer's operational and regulatory requirements

Centred on advisory-led enablement rather than managed service lock-in, we work alongside our customer teams to coordinate onboarding activities, support supplier engagement and provide architectural and operational guidance. Support, incident management, and service performance are managed through defined SLAs, prioritisation, and escalation processes.

Remaining resilient, compliant, and aligned to evolving public sector security, governance, and operational needs, we maintain our service through ongoing monitoring, monthly (or as required) service reviews, and continuous improvement activities.

3.2 Onboarding and offboarding processes

3.2.1 Onboarding

Onboarding and offboarding follow structured, repeatable lifecycles designed to establish governance, mobilise professional support and ensure orderly exit. The approach is advisory and people-based, focusing on coordination, assurance, and continuity rather than technical implementation or system operation.





Our step-by-step process is as follows:

Step 1 – Initiate & Confirm Engagement

- Confirm contract scope, objectives, and success criteria
- Identify stakeholders, roles, and decision authorities
- Agree onboarding approach, constraints, and timelines

Outputs: Engagement brief, stakeholder map, onboarding plan

Step 2 – Establish Governance & Ways of Working

- Define governance structure and meeting cadence
- Agree escalation routes and decision-making processes
- Confirm reporting formats and delivery artefacts

Outputs: Governance framework, RACI, reporting and escalation plan

Step 3 – Baseline Scope, Risks & Priorities

- Review existing documentation and programme context
- Clarify scope, assumptions, dependencies, and constraints
- Identify initial risks, issues, and delivery priorities

Outputs: Scope baseline, initial RAID log, delivery assumptions register

Step 4 – Mobilise Delivery Support

- Confirm roles, responsibilities, and resourcing approach
- Schedule governance forums, workshops, and reviews
- Establish collaboration channels using buyer-approved tools

Outputs: Mobilisation plan, delivery calendar, communication plan

Step 5 – Govern, Assure & Refine (Iterative)

- Support ongoing programme and project governance
- Maintain delivery artefacts and decision records
- Provide assurance, challenge, and recommendations
- Refine approach through regular reviews and feedback

Outputs: Status reports, updated RAID, decision papers, improvement actions

3.2.2 Offboarding

Supporting a straightforward and secure exit process, our offboarding processes ensure users can leave the service at the end of the contract term or upon termination, without lock-in or hidden costs.

Step 1 – Confirm Exit Scope & Timing

- Agree offboarding date, scope, and responsibilities
- Identify artefacts, documentation, and knowledge to transfer
- Confirm buyer expectations for closure and handover

Outputs: Offboarding plan, agreed exit timeline

Step 2 – Knowledge Transfer & Handover





- Transfer delivery artefacts (plans, RAID logs, reports)
- Conduct handover sessions with buyer teams
- Ensure continuity of governance and decision-making

Outputs: Handover pack, knowledge transfer records

Step 3 – Close Engagement & Review

- Confirm completion of contractual obligations
- Capture lessons learned and service feedback
- Close access to collaboration channels and conclude engagement

Outputs: Final delivery summary, lessons learned log, exit confirmation

3.3 Data

3.3.1 Data importing and exporting

Excelsior Solutions Limited does not host or process customer operational or production data. Limited business information (such as contact details and delivery artefacts) is handled in accordance with UK GDPR and buyer policies.

Excelsior Solutions Limited is headquartered in the United States and hosts limited customer business contact information required to deliver the reseller service. This may include names, business email addresses, job titles, organisation details, postal addresses, order references and licensing information. Excelsior does not store or process customer operational, identity, access or security telemetry data.

3.3.2 Data-in-transit protection

Excelsior Solutions Limited does not host or process customer operational or production data. Limited business information (such as contact details and delivery artefacts) is handled in accordance with UK GDPR and buyer policies.

3.3.3 Asset protection

Asset protection and resilience controls for systems and platforms are the responsibility of the buyer and their chosen suppliers. Our contribution relates to delivery continuity, including documentation, handover, and governance processes.

3.4 Availability and resilience

3.4.1 Guaranteed availability

Professional support is available during standard UK business hours, Monday to Friday. The service does not provide system availability guarantees.

3.5 Governance

The service operates under documented governance, information security, and personnel security policies aligned to recognised standards. Staff screening conforms to BS7858:2019, and staff can obtain BPSS where required.



3.6 Security

Excelsior Solutions delivers IT Delivery Support Services as people-based professional services. We do not host, operate, configure, or manage customer systems, platforms, or infrastructure. Security controls relating to cloud services, applications, networks, and data hosting remain the responsibility of the buyer and/or their appointed cloud service providers.

Our security approach focuses on protecting information handled during service delivery, maintaining secure working practices, and ensuring that professional services are delivered in line with public sector security expectations. This includes governance, policy adherence, staff security, and secure handling of delivery artefacts such as plans, reports, and decision records.

We operate documented information security policies covering acceptable use, access control, incident reporting, and data protection. These policies are reviewed periodically to ensure continued alignment with recognised best practice and public sector requirements. Security considerations are embedded into onboarding and delivery governance, ensuring that service activities remain compliant with buyer policies and contractual obligations throughout the engagement.

3.6.1 Operational security

Operational security for this service relates to how professional services are delivered, not to the operation of customer systems or cloud platforms. Key operational security measures include:

- Delivery using buyer-approved collaboration and communication tools
- Controlled access to delivery artefacts based on role and need-to-know
- Secure handling, storage, and transmission of project documentation
- Clear separation between advisory services and customer operational environments

Excelsior Solutions does not monitor, manage or access customer production systems, networks, or applications. Any operational security controls relating to those environments are implemented and managed by the buyer and/or their technology suppliers.

Security incidents relating to Excelsior-managed information or service delivery activities are handled in accordance with documented internal procedures. These procedures include assessment, containment where applicable, communication with the buyer, and corrective actions to prevent recurrence. Lessons learned are reviewed through governance forums to support continuous improvement.

3.6.2 Staff security

Staff security is a core element of our service delivery model. All personnel assigned to IT Delivery Support Services are subject to pre-employment screening, ensuring suitability for work in public sector environments.

Our staff security measures include:

- Identity verification
- Employment history checks
- Criminal record checks where applicable

Staff screening conforms to BS7858:2019. Where required by the engagement, we are prepared to ensure staff meet Baseline Personnel Security Standard (BPSS) requirements.

Access to Excelsior Solutions systems and customer delivery artefacts is granted strictly on a least-privilege basis and aligned to role responsibilities. Access rights are reviewed periodically and promptly revoked when no longer required, including following role changes or staff departures.



All staff receive security awareness guidance appropriate to their role, including expectations around confidentiality, secure handling of information, and compliance with buyer security policies. This ensures that professional services are delivered securely, responsibly, and in line with public sector assurance expectations.

Security responsibilities for cloud platforms, applications, and infrastructure remain with the buyer and/or their appointed cloud service providers. Excelsior Solutions security controls are limited to those required to safely and securely deliver professional services.

3.7 Auditing

Excelsior Solutions supports audit and assurance activities relating to the delivery of professional services, not the operation of customer systems or platforms. Audit activity focuses on:

- Verification of adherence to agreed delivery governance
- Confirmation that contractual, security, and policy obligations are met
- Review of delivery artefacts such as plans, reports, and decision records

We do not generate or manage technical audit logs for customer systems. Any system-level audit logging remains the responsibility of the buyer and/or their appointed cloud service providers. Audit evidence is made available to buyers on request, limited to documentation relevant to service delivery and governance.

3.7.1 Compliance and quality management

Excelsior Solutions operates a documented quality and compliance management approach to ensure professional services are delivered consistently and in line with public-sector expectations. Our approach includes:

- Defined delivery standards and governance processes
- Periodic internal reviews of service delivery practices
- Corrective actions where improvement opportunities are identified

Compliance and quality oversight is focused on people, process, and governance rather than technical controls. Responsibility for compliance relating to cloud platforms, applications and infrastructure remains with the buyer and/or their technology suppliers.

3.8 Backup, restore & disaster recovery

This service does not provide backup, restore, or disaster recovery services for customer systems, platforms, or data. Excelsior Solutions maintains internal business continuity arrangements to ensure continuity of professional service delivery. These arrangements support:

- Availability of project and programme management resources
- Protection of internal delivery artefacts (such as plans and reports)
- Orderly continuation or handover of services in the event of disruption

All backup, restore, and disaster recovery controls relating to customer systems or data are implemented and managed by the buyer and/or their appointed cloud service providers.

3.9 Training

Training and knowledge transfer form part of our professional services delivery to support effective programme governance and continuity. Training activities may include:



- Onboarding briefings on governance, roles, and ways of working
- Walkthroughs of delivery artefacts (plans, RAID logs, reports)
- Handover sessions to support buyer self-sufficiency

Training is advisory in nature and relates to processes, governance, and delivery approach. We do not provide end-user training on cloud platforms, applications, or technical tools unless explicitly agreed and procured separately.

3.10 Service pricing

Pricing for IT Delivery Support Services is published separately in the G-Cloud Pricing Document. Services are typically charged on a time and materials basis, aligned to SFIA skill levels and the role performed (for example, project manager or programme manager). This allows buyers to scale services up or down based on delivery phase and requirements.

There are no minimum contract terms, mandatory add-ons, or proprietary tooling charges. All costs are agreed in advance and documented in the Order Form.

3.11 Invoicing process

Invoices are issued monthly in arrears in line with standard UK public-sector payment practices.

- Payment terms: 30 days
- Invoices are issued against an agreed Purchase Order
- Payment is accepted via standard government payment mechanisms

Invoices provide a clear breakdown of services delivered during the billing period.

3.12 Termination terms

Contracts may be terminated at the end of the agreed term or earlier in accordance with G-Cloud Call-Off Terms.

- No minimum contract term unless stated in the Order Form
- Standard notice period: one month
- Early termination provisions apply in the event of material breach

On termination, services are concluded in an orderly manner and any outstanding charges incurred up to the termination date are invoiced in accordance with agreed pricing.



4 Security and data governance

4.1 Data protection and encryption

Excelsior Solutions does not host or process customer operational or production data. Limited business information (such as contact details and delivery artefacts) is handled in accordance with UK GDPR and buyer policies.

Encryption, data protection, and security controls for cloud platforms and systems are implemented and managed by the buyer and/or their appointed cloud service providers.

4.2 Data at rest, storage locations, and physical security

This service does not require long-term storage of customer data. Delivery artefacts are stored in buyer-approved or buyer-provided systems wherever possible. Any temporary working materials are protected using appropriate access controls and are removed when no longer required.

4.3 Data sanitisation and disposal

Excelsior Solutions does not perform data sanitisation of customer systems or storage media. Where limited business information is held for service delivery, it is securely deleted in accordance with internal retention policies and contractual requirements. Responsibility for data sanitisation of customer systems remains with the buyer and/or their cloud service providers.

4.4 Information security management and certifications

Excelsior Solutions operates documented information security policies appropriate to the delivery of professional services. These policies are reviewed periodically to ensure alignment with recognised best practice.

Where certifications are held or pursued, they relate to organisational governance and internal operations rather than customer systems or platforms.

4.5 Identity and access management

Access to Excelsior Solutions Ltd internal systems is controlled through role-based access and least-privilege principles. Access is reviewed regularly and revoked when no longer required.

Excelsior does not manage user access to customer systems or cloud platforms. Authentication and authorisation for those environments remain the responsibility of the buyer and/or the relevant service provider.

5 Supplier information

5.1 About us

Excelsior Solutions provides governance-led professional services specialising in project and programme management for public-sector organisations. We focus on delivery assurance, stakeholder coordination, and structured governance to support successful outcomes.

5.2 How to buy

Excelsior Solutions Limited's services are available for direct purchase through the Crown Commercial



Service (CCS) G-Cloud 15 Digital Marketplace.

Buyers can locate Excelsior Solutions Limited on the Digital Marketplace and select the appropriate service listing.

Following selection, the buyer and Excelsior Solutions Limited will:

1. Agree a Statement of Work (SoW) outlining the scope, deliverables, timelines, and pricing
2. Establish a Call-Off Contract in accordance with G-Cloud framework terms
3. Issue a Purchase Order (PO) to confirm commencement of services

All engagements are conducted in full compliance with public-sector procurement regulations and the conditions of the G-Cloud framework, ensuring transparency and governance throughout.

For enquiries or pre-contract discussions, please contact us via our central point of contact:

- Phone: 240-478-2334
- Email: info@excelsortech.com