Go-to-market Playbook

How we Connect and Protect the UK’s Most Critical National Services

serbus

connect + protect

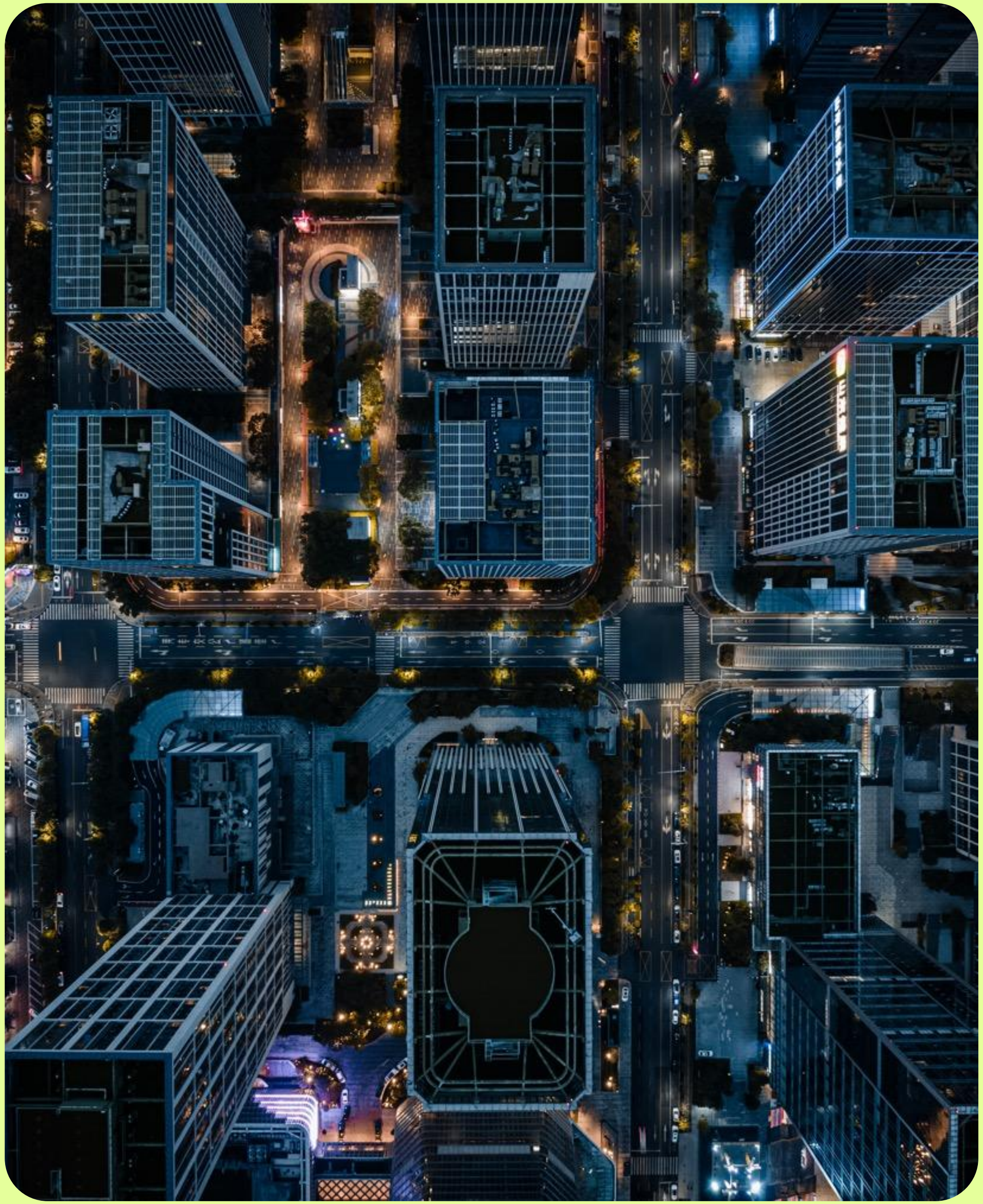
Legal notice

Confidentiality Clause

1. This document may contain personal data protected under the UK GDPR and the Data Protection Act 2018.
2. It is intended only for the authorised recipient.
3. Any unauthorised access, use, disclosure, copying, or distribution is prohibited.
   If you are not the intended recipient, please notify the sender immediately and securely delete this document.

Contents

Introduction and Purpose 01
Brand Positioning and Core Messaging 02
Values and Behaviours 03
Security DNA 04
Social Value & ESG 05
Sector Messaging 06
Customer Discovery & SPQ Framework 07
Capabilities & Services 08
Partnering and Frameworks 09
FAQs 10



SECTION 01

Introduction & Purpose

Purpose of the Playbook

This playbook is your core reference for understanding and communicating:

- The **serbus brand**
- Our **Security DNA**
- Our **sectors, services and value**
- How we **qualify, position and progress opportunities**
- Our **internal processes and routes to market**
- It ensures everyone across business development, delivery, SMEs and leadership **speaks with one voice** when describing serbus to customers, partners and stakeholders.

This playbook does not replace technical documentation or detailed operational manuals. Instead, it acts as the **reference** for how serbus operates commercially and culturally.

Each section supports a stage of customer engagement:

Brand Narrative & Security DNA

Introductions, first meetings, communicating our credentials.

Sector Overviews

Tailoring messaging to audience & personas within the environments we serve. Typical customer challenges covered.

Solutions & Services

Positioning solutions and overcoming objections.

‘SPQ’ Conversation Starters

Discovery conversations & qualification.

Routes To Market

Direct and Indirect Channel & Consortium Partner routes to market.

FAQs

Employee, customer and partner frequently asked questions.

SECTION 02

serbus Brand, Positioning & Core Messaging

Our Name

Our name is serbus, a core brand asset. Do not capitalise or alter our name.

Our name is not ‘serbus Group’, ‘serbus IT’, ‘serbus Security’, or ‘serbus Technology’.

It’s just … serbus.

Brand Story

serbus connects and protects the UK’s most critical national services.

Our people are trusted to build and maintain exceptionally secure, highly resilient communications infrastructure so that the information and operations of vital services are always available whenever and wherever they’re needed.

Elevator Pitch Guidance

Use concise conversational structure

1. Who we are: Sovereign CNI (Critical National Infrastructure) Specialist.
2. What we do: Secure infrastructure, communications and services
3. Who we serve 6 market verticals: Government, Enterprise, Defence, Health, Industrial and Data Centre
4. Why it matters?: Reliable operations for vital national services….keeping UK a safe and secure place to live and do business

Sector Focused Elevator Pitches

Government

serbus delivers secure and resilient interconnected infrastructure, ensuring the UK is the safest place to live and do business.

In the face of lower budgets, increasing threats to operations and unpredictable policy changes, we provide UK-based, security-first communications and infrastructure that runs and improves critical public services, enabling operations through robust ICT delivered by flexible and trusted UK-based sovereign technical and support services, with clear communications even in the most challenging locations.

Customer Reference: Home Office

Enterprise

serbus delivers a wide range of our services across many different Enterprise operations, supported by our 100's strong vetted, trusted contractors, we keep businesses running.

Often responding to short requirements timescales, and wide ranging locations we have decades of experience in advising, planning, implementing and supporting robust and secure ICT.

High standards, strong compliance, and efficient engineers work closely with end customers and channel partners to get the job done.

Customer Reference: CDW

Defence

serbus delivers flexible sovereign solutions for critical communications infrastructure that works anywhere it's needed, reliable, secure and ready to evolve fast.

Operating in complex environments facing rapidly evolving security threats, we provide agile secure connectivity and proven resilience for operations everywhere, built on a true understanding of secure by design, sovereignty, partnership and interoperability between nations, with cleared and trusted operations in and from the UK

Customer Reference: MoD

Sector Focused Elevator Pitches

Health

serbus delivers specialist digital services, delivering critical support and improving patient care, keeping services available and efficient through reliable, secure, specialised communications infrastructure delivered by people who care as much as you do.

In the face of minimising disruption to patient care, cost-saving and efficiency targets, and increasing threats to operations, we enable transformation that will save lives and improve patient outcomes, bringing proven experience in complex clinical environments with reliability and security built in, supported by consulting and advisory services.

Customer Reference: NHS Trusts

Industrial

serbus delivers robust digital infrastructure that secures your operations and boosts productivity, providing proven systems for operational technology that put security first, keeping critical processes running reliably while enabling monitoring, optimisation and automation.

In the context of increasing productivity targets, increased cyber security threats from OT adoption, increased IT/OT convergence and inexperience with connected systems, we bring government-proven reliability and security, a flexible 360º maintenance and support model on or off-site, and cleared, compliant experts working in complex facilities.

Customer Reference: Premier Foods

Data Centre

serbus delivers scalable data centre infrastructure that maximises returns and minimises risks, providing secure infrastructure and services for advanced data centres, supported by government-grade cyber security and reliability.

In the face of maintaining resilient systems for business-as-usual, rapidly increasing cyber security threat levels, urgent capacity demands and energy efficiency and ESG targets, we offer scalable, secure infrastructure, proven experience with rapid and compliant deployment, and flexible 360º cyber security and support delivered on UK soil

Customer Reference: CoreWeave

Writing Principles

Every word we use us important, across every part of our business. So, no matter your role or title, using these principles will help you to write consistently and with impact.

Everything under control

We may work in complex environments, but we're always the calmest heads (and voices) in the room. We speak with confidence because it breeds confidence in turn. Our customers are assured they're in safe hands.

Clarity for cut-through

We keep our words simple, sensible and straightforward. We get to the point quickly and clearly. We use everyday language, contractions, and sentence-style capitalisation to make sure we cut through the noise.

Always the specialist

We share our insight and show how well we know our chosen sectors and environments. We speak our customers' language. We use an active voice. And we focus on what matters. This all helps us form close relationships.

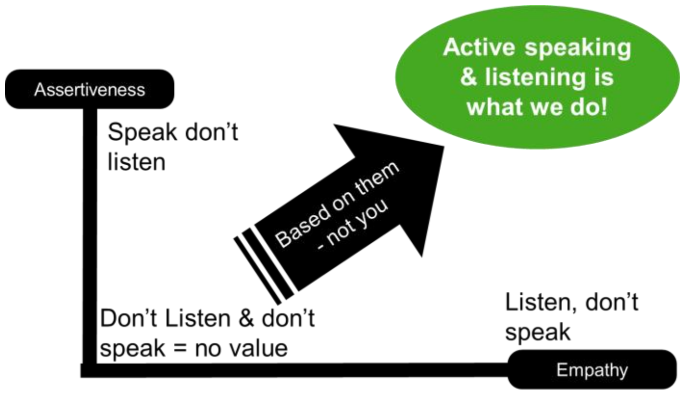
Listening Principles

Every interactions is important, across every customer, every partner and every supplier. So, no matter your role or title, using these listening principles to help you to add-value consistently, and with positive impact.

We always actively listen

It’s about the customer and their operational needs.

Move from the symptom, to understanding the underlying problem, and then use that joint understanding to create jointly agreed actions.



Active Listening

- Signs of attention
- Suspend inner voice > listen
- Pay attention
- Take note
- Restate / looping
- Correct mis-understandings
- Ask clarification
- Align pace of dialogue

▶

- Personalise
- Adapt
- Be concise
- Integrate ideas / don’t replace them
- Tone
- Positive with realism
- Give supporting collateral

***Add value and energy into every interaction*.**

SECTION 03

Values and Behaviours

Our Values and Behaviours *(“that we’ve S.E.T.T. in stone ☺”)*

Security that sets us apart

We embed high security standards, and a secure mindset in everything that we do .

Experience and empathy over ego

We prioritise operational needs and are selflessly committed to meeting them.

Teamwork at all times

We work in partnership, collaborating, learning and adapting as we go.

Trust built on always delivering

We actively listen, understand the why, and are dedicated to getting the job done

These values define how we work: with security at our core, true collaboration, empathy, and a consistent commitment to delivery. Our customers can rely on us to bring clarity, focus and excellence to every partnership.

SECTION 04

Our Security DNA

When to highlight our Security DNA

Always. It’s always been there across each business. All we’ve done is highlight it and make it a core reason for why we stand out as different for customers and partners in a world where securing people, processes, facilities, and data is increasingly important.

The serbus Security DNA defines how we operate, how we deliver, and why customers trust us in highly regulated, sovereign CNI environments.

It is not a sales script or marketing statement; it is our delivery assurance framework that underpins every service we provide across all sectors.

Whether engaging in early discovery, solution design, proposal development or service delivery, the Security DNA provides customers and partners with confidence that serbus operates to approved, auditable and trusted compliance and security standards.

Our Security DNA is structured across nine core elements:

- People
- Processes
- Vetting & clearances
- Compliance
- Property
- Supply Chain
- Systems
- Data

Together, these demonstrate our end-to-end commitment to operational security, compliance and risk management.

When to Position our Security DNA

Early Discovery

When customers wish to discuss/raise concerns about:

- Cyber security risks
- Compliance obligations
- Data protection requirements
- Delivery team vetting or clearances

Use DNA principles to establish trust and credibility.

Solution Design

When developing architectures or services models that must align to:

- Regulatory frameworks
- Accreditation or audit standards
- Customer internal governance requirements

Use relevant DNA proof points to communicate that solutions are mapped to compliance expectations.

Proposals + Tenders

When responding to:

- Security schedules
- Compliance obligations
- Information assurance questions

Our Security DNA helps to demonstrate compliance and governance within our delivery engine.

Stakeholder Assurance

We know what security means…

Vetting of Engineers: Reference people, vetting and clearances.

Compliance Accreditation: Reference Compliance & Processes

Data Protection: Reference Data and systems

Supply Assurance: Reference Supply Chain

Governance Controls: Reference iComply

Our Security DNA Pillars

Security DNA Pillar	Description	Scenarios: When to Reference
1. People	Trusted professionals with extensive security clearance to handle sensitive work, accustomed to operating in regulated and mission-critical environments. Continuous training in information assurance, cyber hygiene, and operational security – knowing what to say and what not to. With a proven track record supporting MoD, Government and national infrastructure projects.	Highlighting why we can be trusted to maintain security Vetting of employees and delivery engineers
2. **Processes**	Security built into every stage, from planning to delivery and through-life support. Controlled, auditable workflows aligned with government best practice. Rigorous change, incident, and risk management procedures that are Quality assured under recognised security and governance standards.	Through-life delivery Incident management Compliance accreditation discussion
3. **Vetting/ Clearances**	All personnel are formally vetted and authorised to support sensitive projects. Eligibility and background checks meet the highest standards of national assurance. Clear roles, responsibilities, and access levels defined for every engagement.	Confidentiality and trust underpin every contract we deliver Vetting of employees and delivery Engineers
4. Compliance	Aligned with UK Government security and data protection frameworks. Regular independent audits and continuous improvement programmes. Adherence to ISO 27001, Cyber Essentials Plus, and NCSC guidance. Compliant across all aspects of data handling, privacy, and access control.	Required compliance accreditations **Link to iComply**

Our Security DNA Pillars

Security DNA Pillar	Description	Scenarios: When to Reference
5. Property	Secure facilities with controlled access and segregated work areas. Physical, digital, and procedural security integrated throughout. Robust visitor and asset management procedures. Environment designed for confidential and classified operations.	Physical security discussion Facilities where we can be part of the secure customer operations
6. Our Supply Chain	Trusted partners subject to the same rigorous assurance standards. End-to-end visibility and control across our supplier network. Continuous risk assessment to protect project integrity. Secure procurement and vendor due diligence processes.	Supply chain assurance (especially within sovereign markets)
7. Systems	Hardened networks and infrastructure built on best-practise principles. Secure communications platforms for sensitive collaboration. Proactive monitoring, patching, and threat detection. Configurations aligned with government and defence benchmarks.	Data protection and resilience discussion
8. Data	Classified data managed with uncompromising integrity and robust control. Encryption and access management built into every layer. Data encrypted in transit and at rest. Role-based, least-privilege access is enforced and audited. Data residency and sovereignty assured within UK jurisdiction. Full lifecycle protection, from capture to secure disposal.	Data protection and resilience discussion Taking us up the solutions stack from infrastructure to data services

iComply

Secure by Design. Resilient by Culture.

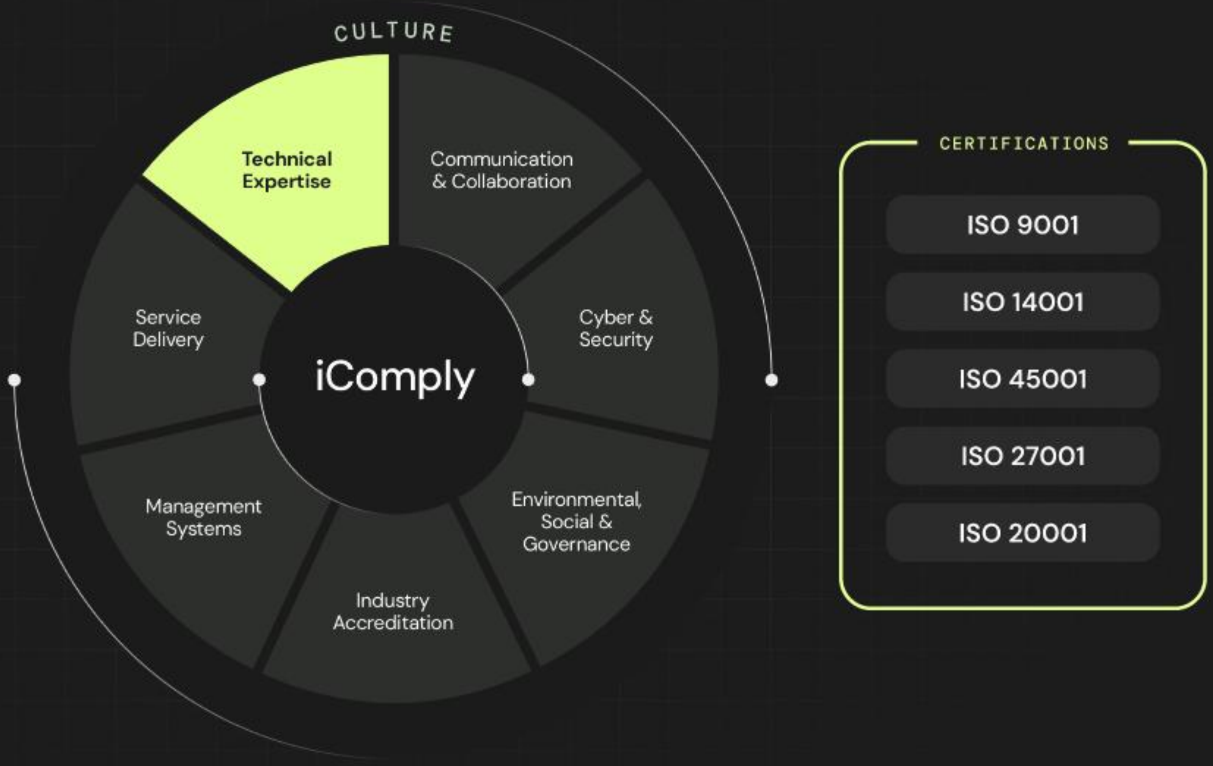
serbus meets the highest standard of security, quality and governance across our operations.

Through iComply, our in-house governance and assurance framework, we present how we embed compliance into our DNA, ensuring everything that we do is secure, transparent and accountable.

Our comprehensive UKAS certifications demonstrate this commitment, including:

- ISO 9001 (Quality)
- ISO 14001 (Environmental)
- ISO 45001 (Health & Safety)
- ISO 27001 (Information Security)
- ISO 20000 (Service Management) – pending

Please visit our iComply website to explore our iComply platform.



SECTION 05

Social Value &ESG

Social Value: Our Approach

This section of our playbook explains how serbus delivers responsible, secure and sustainable solutions and how our work contributes to national resilience, community development and ethical operations.

Use this content to:

- Communicate our commitment to security and sustainability
- Demonstrate our social value commitments alongside secure delivery
- Support bids, tenders and assurance conversations where ESG performance is required

Relevant to:

- **Business Development:** Lead ESG conversations and respond to tender requests
- **Bid Team:** Evidence ESG compliance and social value scoring criteria
- **People Managers:** Reinforce recruitment, wellbeing and training commitments

At serbus, we embed Environmental, Social, and Governance (ESG) principles into everything we do.

From how we design secure infrastructure to how we manage our supply chains and support our people, our goal is to operate in a way that strengthens communities, protects the environment, and upholds the highest standards of governance.

ESG isn’t an add-on, it’s part of everything we do
From board-level strategy to frontline delivery, we integrate ESG goals into every decision, ensuring that security and sustainability go hand in hand.

ESG & Social Value Commitments

Strengthening National Resilience

serbus plays a vital role in supporting UK national resilience, contributing to the security, continuity and performance of critical communications and digital infrastructure.

By delivering secure, sustainable technology solutions, we help organisations protect people, data and national operations, enabling the UK to remain connected, resilient and future-ready.

Championing Inclusion and Wellbeing

Our culture is built on respect, equality and purpose. We are proud to foster a workplace that promotes diversity, inclusion and wellbeing, ensuring that every individual feels valued and empowered to contribute.

We prioritise:

- Diversity, equality and inclusion across all roles and leadership levels.
- A safe, supportive environment that promotes mental health and wellbeing.
- Transparent communication and a responsible workplace culture built on integrity and accountability.

Investing in People and Skills

- We believe resilience begins with people. serbus is committed to growing the UK's secure technology talent base through targeted recruitment, training and professional development.
- Supporting veterans and those leaving the military to transition into civilian technology and cyber careers.
- Offering apprenticeships and continuous learning for technical and security professionals.
- Partnering with UK training bodies, universities and industry to build national cyber and digital capabilities.
- Promoting lifelong learning to ensure our teams remain at the forefront of secure ICT delivery.

ESG & Social Value Commitments

Environmental Responsibility

We are committed to minimising our environmental impact and operating responsibly across all aspects of our business.

- ISO 14001 certified Environmental Management System.
- Reducing waste and carbon through efficient logistics, equipment lifecycle management and WEEE disposal.
- Designing energy-efficient infrastructure and sustainable ICT solutions for clients.

Governance and Ethical Standards

Strong governance underpins everything we do. We maintain transparent, ethical business practices and leadership, supported by UKAS-accredited certifications, NCSC-aligned processes, and responsible procurement frameworks.

- ISO 9001, ISO 27001, and ISO 45001 certifications ensure quality, security and safety across all operations.
- Full compliance with UK regulatory frameworks and public sector procurement standards.
- Ethical supply chain management and fair business conduct across all partnerships.
- Working with partners and suppliers who share our commitment to sustainability and climate-conscious delivery.

iComply: ESG in Action

- Our iComply framework connects our ESG principles with daily operations, providing governance, accountability and continuous improvement across our services.
- It ensures our environmental, social and governance commitments are not just policies, but practical systems that drive measurable results.
- **Learn more**

SECTION 06

Target Sectors

How to Use Sector Messaging

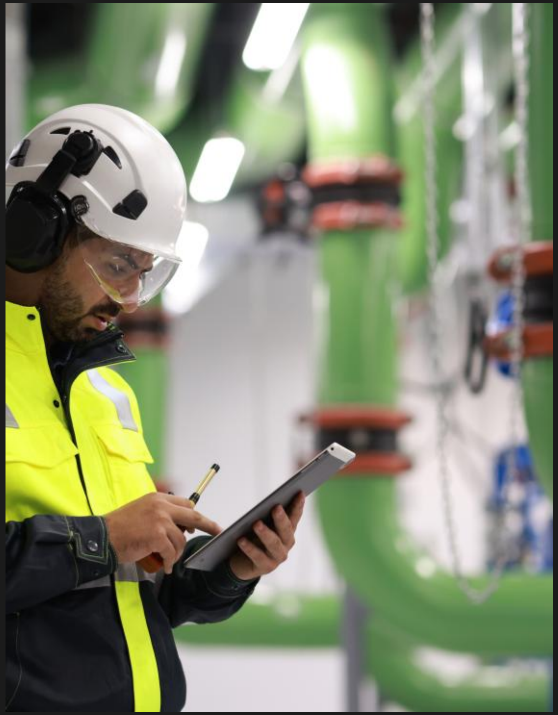
Sector messaging exists to ensure that serbus conversations always begin with customer relevance rather than product description.

Use sector elevator pitches to:

- Open meetings and discovery sessions
- Position serbus in a relevant operational context
- Align discussions to customer challenges before proposing services

Guidance:

- Use sector SPQ discovery questions to help position a solution-led discussion
- Align discussion to customer challenge before proposing services



Sector Focused Elevator Pitches

Government

serbus delivers secure and resilient interconnected infrastructure, ensuring the UK is the safest place to live and do business.

In the face of lower budgets, increasing threats to operations and unpredictable policy changes, we provide UK-based, security-first communications and infrastructure that runs and improves critical public services, enabling operations through robust ICT delivered by flexible and trusted UK-based sovereign technical and support services, with clear communications even in the most challenging locations.

Customer Reference: Home Office

Enterprise

serbus delivers a wide range of our services across many different Enterprise operations, supported by our 100’s strong vetted, trusted contractors, we keep businesses running.

Often responding to short requirements timescales, and wide ranging locations we have decades of experience in advising, planning, implementing and supporting robust and secure ICT.

High standards, strong compliance, and efficient engineers work closely with end customers and channel partners to get the job done.

Customer Reference: CDW

Defence

serbus delivers flexible sovereign solutions for critical communications infrastructure that works anywhere it’s needed, reliable, secure and ready to evolve fast.

Operating in complex environments facing rapidly evolving security threats, we provide agile secure connectivity and proven resilience for operations everywhere, built on a true understanding of secure by design, sovereignty, partnership and interoperability between nations, with cleared and trusted operations in and from the UK

Customer Reference: MoD

Sector Focused Elevator Pitches

Health

serbus delivers specialist digital services, delivering critical support and improving patient care, keeping services available and efficient through reliable, secure, specialised communications infrastructure delivered by people who care as much as you do.

In the face of minimising disruption to patient care, cost-saving and efficiency targets, and increasing threats to operations, we enable transformation that will save lives and improve patient outcomes, bringing proven experience in complex clinical environments with reliability and security built in, supported by consulting and advisory services.

Customer Reference: NHS Trusts

Industrial

serbus delivers robust digital infrastructure that secures your operations and boosts productivity, providing proven systems for operational technology that put security first, keeping critical processes running reliably while enabling monitoring, optimisation and automation.

In the context of increasing productivity targets, increased cyber security threats from OT adoption, increased IT/OT convergence and inexperience with connected systems, we bring government-proven reliability and security, a flexible 360º maintenance and support model on or off-site, and cleared, compliant experts working in complex facilities.

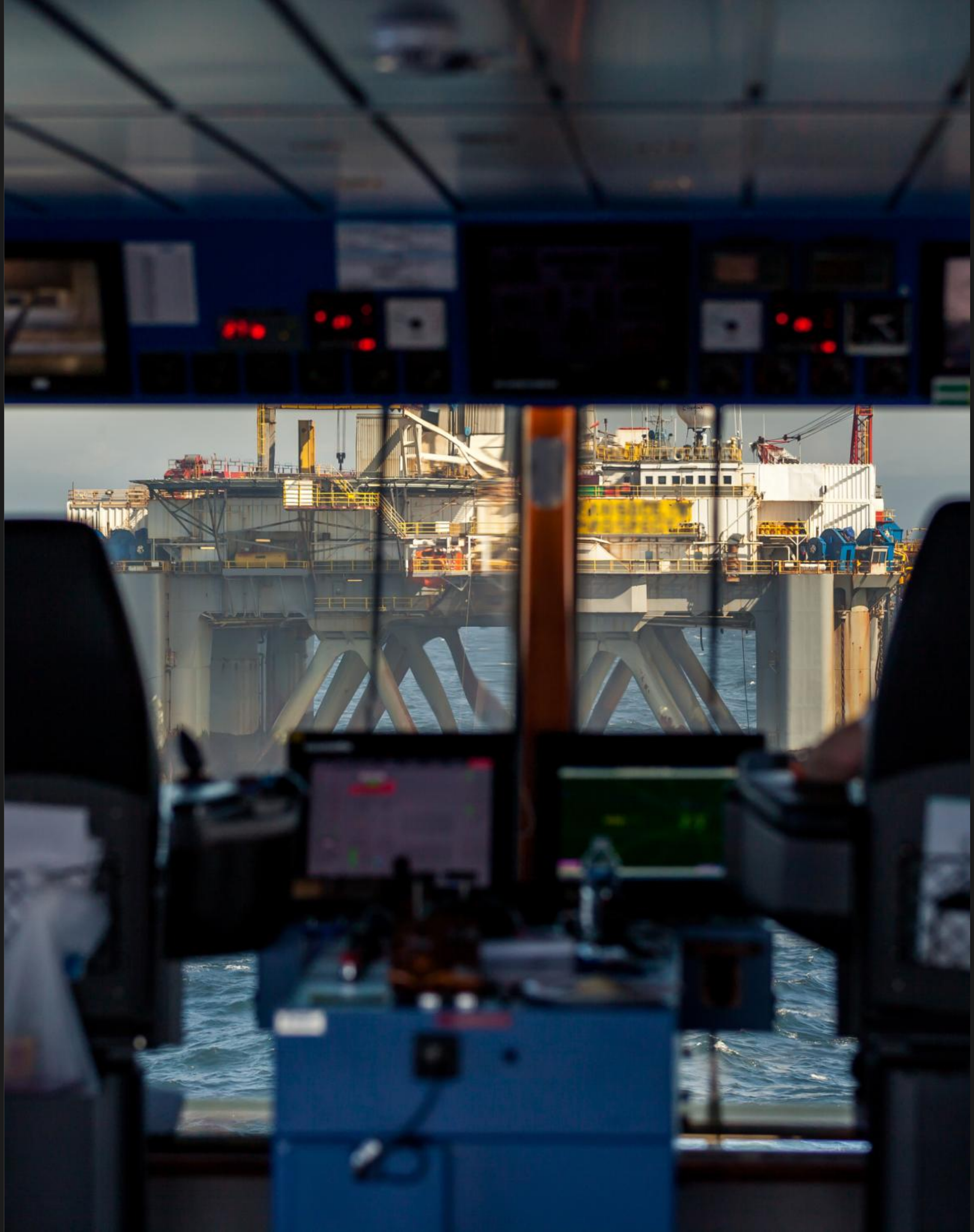
Customer Reference: Premier Foods

Data Centre

serbus delivers scalable data centre infrastructure that maximises returns and minimises risks, providing secure infrastructure and services for advanced data centres, supported by government-grade cyber security and reliability.

In the face of maintaining resilient systems for business-as-usual, rapidly increasing cyber security threat levels, urgent capacity demands and energy efficiency and ESG targets, we offer scalable, secure infrastructure, proven experience with rapid and compliant deployment, and flexible 360º cyber security and support delivered on UK soil

Customer Reference: CoreWeave



Customer Discovery & SPQ Guidance

Purpose

SPQs (Scenario – Problem – Questions) provide a consistent discovery framework that helps move conversations away from product pitching and toward understanding operational challenges, risk exposure and compliance pressures.

They ensure:

- Customer discussions start with context and impact
- Opportunities are qualified properly before solution design
- Technical resource is engaged only when appropriate
- Business development conversations remain aligned with sector priorities

How to Use SPQs

SPQs are discovery tools, not sales scripts.
They exist to ensure that solutions are built around **genuine customer needs**, not assumptions or product availability.

1. Set the Scenario

Begin by framing the environment using the sector scenario statement:

- Confirms you understand the customer's world
- Establishes relevance and credibility
- Aligns the discussion to regulated or mission-critical conditions

Read or paraphrase the scenario to open the conversation.

2. Explore the Problem

Use the problem statement to guide discussion around. E.g.,:

- Operational vulnerabilities
- Compliance or assurance gaps
- Service disruption risks
- Resource or skills limitations

This stage should deepen understanding, not validate assumptions.

3. Ask Qualification Questions

Use questions to uncover:

- Specific points of instability or failure
- Gaps in security architecture/posture
- Limits in current governance or controls
- Capacity constraints impacting resilience

Do not rush to answer your own questions, give the customer time to respond and expand.

4. Close with the 'Would it help if…'

The final "Would it help if…" statement:

- Transitions discovery into solution relevance
- Connects customer problems to serbus value
- Opens the door to solution discussion
- Only use this once customer challenges have been clearly articulated.

Example SPQ: Health

Scenario:

Health providers depend on uninterrupted access to clinical systems, patient data, and critical communications across hospitals, trusts and remote care environments. Expansion of digital services, remote diagnostics, and medical IoT is increasing pressure on secure connectivity and reliable infrastructure.

Problem

Many trusts operate on ageing infrastructure, fragmented networks and inconsistent security controls, creating downtime risks and vulnerabilities in clinical workflows.

Budgets are lessening, with headcount reductions across the operational activities but at the same time, healthcare must continue, improve, and ICT infrastructures need to be the best they can be across current and new build sites.

Question (Solution)

How are you securing communication between clinical sites, remote teams and critical systems?

Where do network/system outages or instability create risk to patient care or performance targets?

Do you have the internal resource to maintain secure infrastructure across all clinical locations?

Would it help if we could harden and secure your critical connectivity, reduce downtime risks and support safe, resilient care delivery and patient outcomes?

Example SPQ: Defence

Scenario:

Defence organisations require high-assurance, highly resilient communications and infrastructure that support deployed operations, classified work, and rapid mobility across secure environments.

Defence has many use-cases with different technologies and services needed for each.

As the transition from on-prem to cloud continues, data management, accessibility and security at the highest levels is a factor.

Problem

Unsecure networks, legacy technologies and pressured deployment timelines can create vulnerabilities and operational bottlenecks.

Sovereignty is talked about a lot, but rarely understood in the supply chain, and data management is paramount to full control of operations.

Question (Solution)

Where are you experiencing challenges maintaining secure communications across fixed, tactical or remote sites?

Do your current mobile platforms meet the security levels required for mission-critical use?

Are legacy or mixed-vendor systems affecting assurance or readiness?

How quickly can you deploy secure infrastructure when operational needs change?

Would it help if we could provide established defence-grade secure mobile solutions and resilient comms infrastructure that protect users and operations wherever they are?

Example SPQ: Industrial

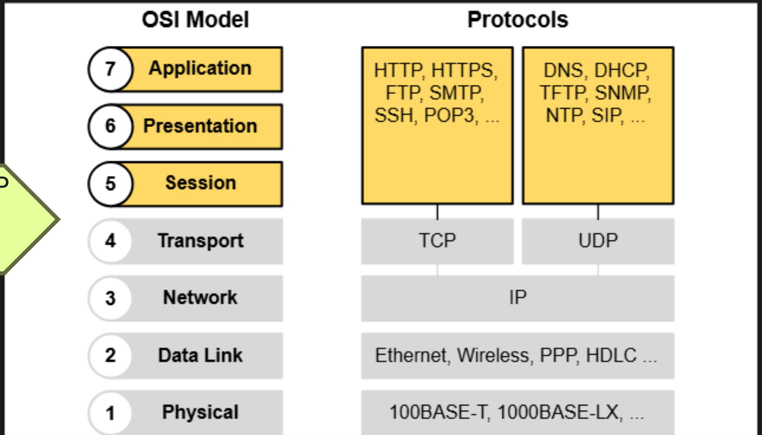
Scenario:

Industrial operators depend on stable, secure communications to keep production lines running, protect OT environments, and maintain safety and regulatory compliance across plants, remote sites and supply-chain partners.

Problem

Legacy OT systems, mixed IT/OT networks and third-party integrations often introduce security gaps, downtime risks and operational fragility.

Transitioning from non-IP to IP protocols or connecting IP with other protocols creates new data management, access and cyber risks



OSI Model	Protocols	
7 Application	HTTP, HTTPS, FTP, SMTP, SSH, POP3, ...	DNS, DHCP, TFTP, SNMP, NTP, SIP, ...
6 Presentation		
5 Session		
4 Transport	TCP	UDP
3 Network	IP	
2 Data Link	Ethernet, Wireless, PPP, HDLC ...	
1 Physical	100BASE-T, 1000BASE-LX, ...	

Question (Solution)

How are you securing communications between control rooms, OT assets, remote sites and contractors?

Where do you experience instability or outages that impact production output, safety systems or site operations?

Are legacy PLCs, SCADA networks or segmented OT environments creating challenges for consistent security and monitoring?

Do you have enough skilled resource to maintain secure, resilient infrastructure across multiple plants or geographically dispersed sites?

Would it help if we could harden and secure your operational networks, strengthen resilience across IT and OT, and reduce risks to production and safety-critical operations?

Example SPQ: Enterprise (FS; Consultancies)

Scenario:

Large enterprises with distributed teams depend on secure, high-availability communications to protect sensitive client data, ensure continuity of operations, and maintain trust across regulated markets. Rapid cloud adoption, hybrid working, and high-value data flows increase pressure on secure infrastructure and resilient connectivity.

Problem

Complex estates, multiple cloud environments and cross-border collaboration introduce points of failure and exposure, especially where critical communications rely on mixed, legacy or third-party systems.

Speed of build is fast, but resilient and secure systems is a must – so understanding and balancing both needs is necessary.

Question (Solution)

How are you securing communications between global offices, hybrid workers and sensitive client environments?

Where do you see vulnerabilities in collaboration platforms, data transfer paths or remote access for high-risk teams (advisory, research, investigations, M&A, etc.)?

Are client audits or regulatory frameworks highlighting gaps in resilience, encryption, or access controls?

Do you have the internal capacity to maintain consistent, high-assurance security across all regions and business units?

Would it help if we could provide secure, resilient communications and infrastructure that protect sensitive workstreams and maintain operational continuity across all global locations?

Example SPQ: Data Centre

Scenario:

Data centre operators are scaling rapidly to support AI/ML compute demand, cloud adjacency, high-density workloads, and the rise of edge and micro-DC environments. With increasing interconnectivity between sites, cloud regions and customer estates, operators must maintain zero-downtime resilience, secure inter-site connectivity, and fully assured operational environments, all while navigating tighter regulatory and sovereign-data requirements.

Problem

This acceleration often exposes gaps around east–west traffic security (data flow between servers, racks, clusters, and systems), mixed vendor infrastructure, supply-chain assurance, and resilience across high-density or multi-region sites.

Question (Solution)

How are you securing inter-site and interconnect pathways as you expand capacity for AI, hyperscale or multi-cloud customers?

What risks exist around single points of failure, failover orchestration, or resilience in your high-density or edge locations?

Are compliance audits highlighting challenges with operational assurance, supply chain integrity, or segmentation of critical operational traffic?

Would it help if we could secure and harden your connectivity across all regions, eliminate operational weak points, and support resilient, compliant 24/7 operations tailored to high-growth, high-density environments?

Example SPQ: Government – Home Office

Scenario:

Home Office operations demand assured, secure communications and infrastructure capable of supporting sensitive environments, multi-agency collaboration and continuous national operations.

Problem

Complex estates, legacy systems, and tight compliance frameworks can create security gaps and slow operational performance.

Spend is allocated across multiple frameworks and direct/through partners.

Clearances and engineers who understand government operations and sensitivities are needed to help deliver efficiently.

Question (Solution)

How are you ensuring secure, authenticated communication across departments, mobile teams and secure sites?

Which parts of your infrastructure cause operational risk or limit resilience?

Are current controls meeting audit, accreditation or protective security requirements?

Would it help if we could provide secure, resilient infrastructure and communications trusted for critical national services?

SECTION 07

Solutions and Services

Solutions and Services

Purpose:

This section explains:

- What serbus delivers across each capability area
- How employees should position those capabilities during discovery, solution design and bid development
- When to escalate to subject matter experts and delivery leads

Capabilities should only be discussed after SPQ discovery confirms customer need.

How to Use the Capabilities Pages

Capabilities pages support **solution shaping**, not prospecting. Use this section of the playbook to:

- Translate validated customer challenges into service solutions
- Connect operational risk to specific delivery capabilities
- Support bid development and compliance mapping
- Prepare subject matter expert sessions where required

How to Position Solutions

Anchor to SPQ Discovery

Capabilities should always map back to customer problems identified during SPQs. For example:

Discovery Focus	Solution Focus
Network reliability gaps	Secure Infrastructure
Mobile communication encryption concerns	Secure Communications
Skill limitations or governance pressures	Bespoke Secure Services

Articulate Outcomes

Always frame capabilities around outcomes, rather than technology-first descriptions. For example:

- Resilience
- Compliance
- Improved security posture
- High-availability/Continuity of service

What we deliver

Secure Infrastructure

We advise on, design, and build critical digital infrastructure that can be relied upon

Secure Communications

We provide secure communication for vital people and technologies, wherever and whenever it’s needed.

Secure Services

Our security cleared technical teams can support in-house services or manage them for you

We build the network foundations. We create communication systems on those networks, and we keep them optimised, secure, and running. And we specialise in doing all of this in challenging and changeable environments.

Secure Infrastructure

What we offer

We advise on, design, and build critical digital infrastructure that can be relied upon.

Onsite	Offsite Build and Scale
Digital Infrastructure (design, build, manage)	Logistics (just in time) & Managed Deliveries
Structured Cabling Solutions & Systems	Rack Infrastructure Builds (Network & Power)
Data centre ICT	Equipment build, configuration, pre-stage & test
Racking & Cabinets installation and migration	Warranty & RMA (Return Merchandise Authorisation)
Operational Technology (OT) Sensors & Infrastructure	Hot Swap / Spares Equipment
IOT Sensors & Infrastructure Installation	Secure Storage & Customer Swing Space
Technical equipment connectivity design (medical/ military/ gov.)	
Security cleared engineers, processes, and facilities	

Secure Infrastructure

What we offer
We advise on, design, and build critical digital infrastructure that can be relied upon.

Onsite	Offsite Build and Scale
ICT Infrastructure refresh & roll outs	Managing complex/ Secure IT infrastructure
Customer Premises Equipment (CPE) management	Virtual Machine (VM) creation, management & support
End User Device Install, Refresh & management	Microsoft Endpoint Configuration (SCCM / MECM)
UPS, PDU's, Power & Electrical	Civils works (road digs & chamber management)
AV / Entertainment Infrastructure	Disaster Recover Failover Facilities
Precision Comms Room / Data Centre Cooling / Hot & Cold Aisle Containment	Secure locations
Security – CCTV, Analytics & Access Control	
Technical equipment connectivity design (medical/ military/ gov.)	
Security cleared engineers, processes, and facilities	

Secure Communications

What we offer

We provide secure communication for vital people and technologies, wherever and whenever it’s needed.

Secure Mobile	Networks
Secure Mobile Application integration	Mobile Wireless (Satellite) Design & Installation)
Advanced Mobile Solutions (AMS) - Government & Commercial	Private 4G / 5G Networks (design, install, deliver)
Secure Private & Public Hosting	Secure cloud capabilities
Multi-user/system secure connectivity	In-building Wireless & DAS
Secure Voice, Video & Messaging	Industrial Ethernet
Mobile Device Management & Security	Secure bearer connectivity & management
Network Obfuscation & Anti-contagion	Layer 2 / 3 Networking & Secure VPNs
Security cleared engineers, processes, and facilities	

Secure Communications

What we offer

We provide secure communication for vital people and technologies, wherever and whenever it’s needed.

Secure Mobile	Networks
End to End Encryption & DataDiodes	Enterprise/ Private/ Emergency wireless provision
Situational Awareness & Geospatial	Secure Layer 4 Networking (DPRM)
Android Team Awareness / Tactical Assault Kit (ATAK)	Wi-Fi Solutions & Network Equipment
Press to Talk Communications (PTT)	API creators & SQL admins
Ruggedised Mobile & Compute Devices	Datadiodes & Encyrption
Ultra Secure Browsing & Secure VPN	End User Device (EUD) provision & management
Mobile Airtime, IoT, SIM & eSIMs	Cyber / Security Threat Defence
Security cleared engineers, processes, and facilities	

Secure Services

What we offer

Our security cleared technical teams can support in-house services or manage them for you.

Managed Services	Professional Services
Operation of ICT infrastructures, applications, & service	Technical Advisory
ITSM Service Desk & Management	Project & Programme Management
1st, 2nd, 3rd line ITIL Service implementation	Data centre, ICT / building design
Field Service Engineers (24/7/365)	Partner eco-system services management
Managed Security Information & Event Management (SIEM)	Digital Transition & Transformation
Desktop Application Management, remote access, & release rollout automation	Technical infrastructure/ Mobile 4G/5G Due Diligence, In-building connectivity & Surveys
Asset Tracking & Management (HW/SW)	Solution Design, Proof of Concept & Pre-stage
Security cleared engineers, processes, and facilities	

Secure Services

What we offer

Our security cleared technical teams can support in-house services or manage them for you.

Managed Services	Professional Services
Asset Tracking & Management (HW/SW)	Solution Design, Proof of Concept & Pre-stage
Change & Problem Management	PEN & Physical Security Access Testing (Red Teaming)
Services Operations Centre (SOC) & Network Operations (NOC)	Resilient infrastructure strategies: DR, Backups, Restores & Business Continuity
Procurement, Supply & Stock Management	Infrastructure Audits, CAD & Documentation
Managed Print / follow me Print Support & Services	Data Management & Analytics / Shared Drives, Access, Storage
Optic Fibre & Duct Management, (FDS) segregation, routes and protection	Cooling / power design, & Load/ PAT testing
WOW (Workstation on Wheels) Support & Monitoring	Knowledgebase Creation, User Training, documentation, & Management
Comms Room Tidy & Management	Wi-Fi Surveys, Design, Installation, Support
Security cleared engineers, processes, and facilities	

SECTION 09

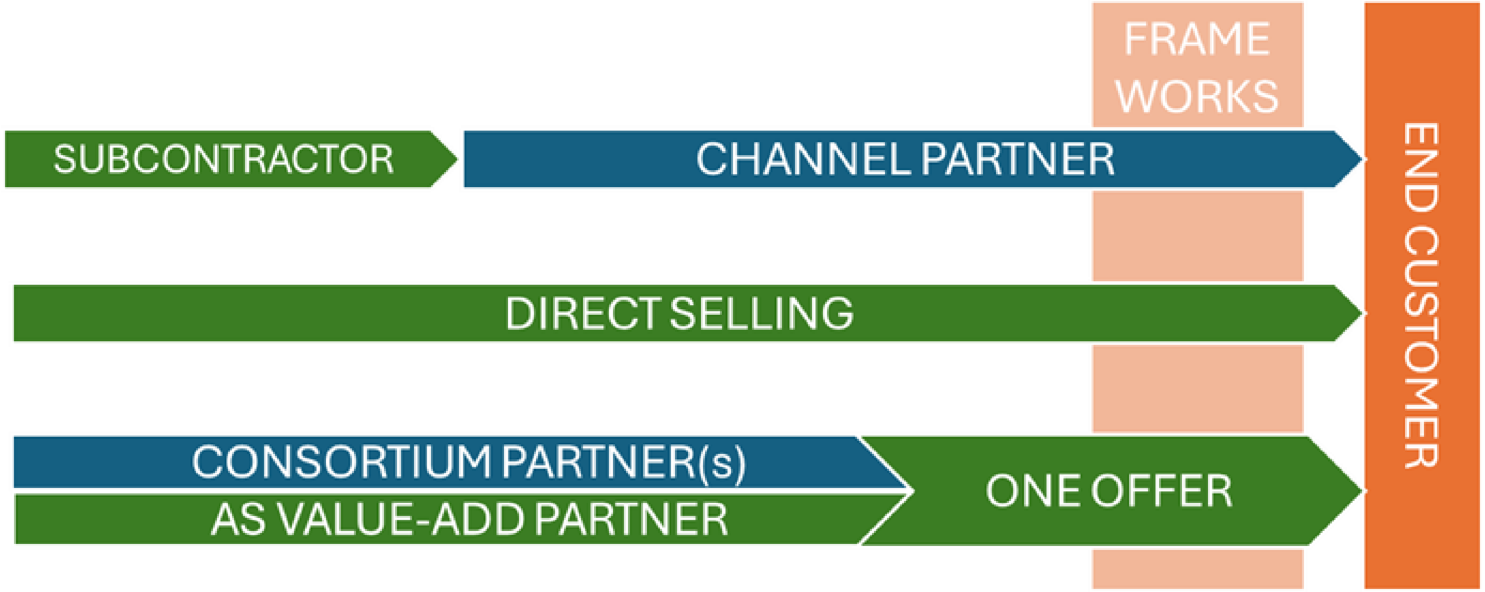
Partnering & Frameworks

Commercial in confidence | Confidential information. Refer to slide 2 for full notice.

Partnering and Frameworks

This section outlines how we take our brand and solutions to market through a range of partnering models and commercial frameworks:

- **Direct:** Our direct route to market involves selling and delivering services straight to end customers with no third-party involvement.
- **Indirect – 'Sell-through' Channel:** Our indirect routes to market include sell-through models with channel partners such as distributors and systems integrators, who resell and deliver our services to customers.
- **Indirect – 'Sell- with' Consortium Partnerships:** We also work with consortium partners in a "sell-with" model, combining capabilities to present a united, joint offer that delivers greater value to our customers.

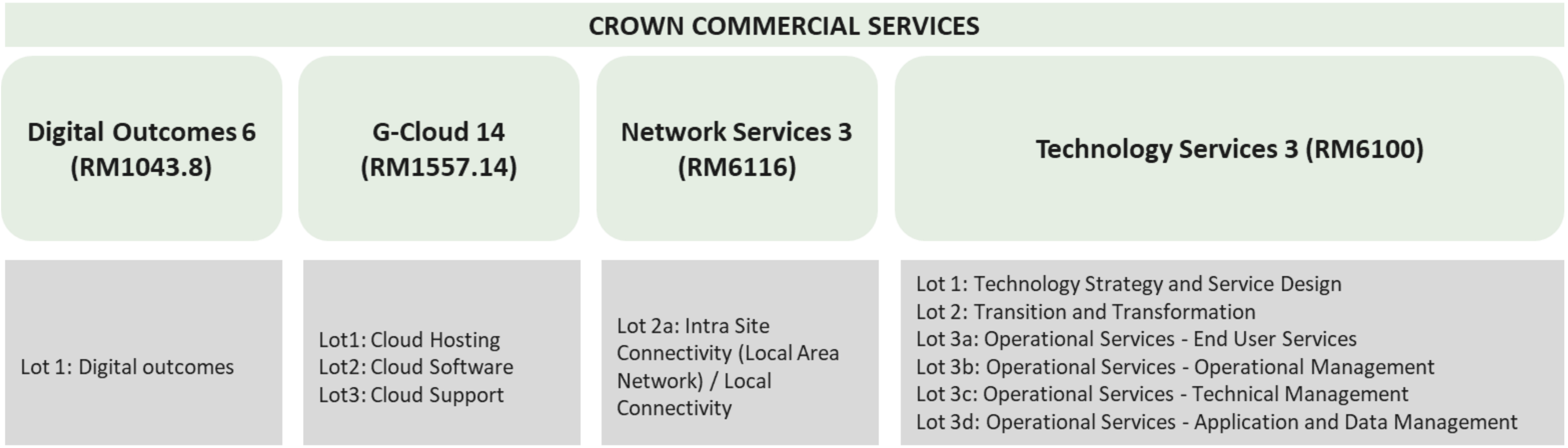


Partnering and Frameworks

Public Sector Frameworks

- When working with public sector organisations, we must sell through approved procurement routes called Crown Commercial Service (CCS) frameworks, which determine supplier eligibility.

- We are accredited on multiple CCS frameworks aligned to our services, including Digital Outcomes 6, G-Cloud 14, Network Services 3, and Technology Services 3 (see diagram below for an overview).



CROWN COMMERCIAL SERVICES

Digital Outcomes 6 (RM1043.8)	G-Cloud 14 (RM1557.14)	Network Services 3 (RM6116)	Technology Services 3 (RM6100)
Lot 1: Digital outcomes	Lot1: Cloud Hosting Lot2: Cloud Software Lot3: Cloud Support	Lot 2a: Intra Site Connectivity (Local Area Network) / Local Connectivity	Lot 1: Technology Strategy and Service Design Lot 2: Transition and Transformation Lot 3a: Operational Services - End User Services Lot 3b: Operational Services - Operational Management Lot 3c: Operational Services - Technical Management Lot 3d: Operational Services - Application and Data Management

FAQ’s

So what do I now call the old serbus?

- Our team at Hereford have a great history in providing Secure Communications into Defence and Government and are now integrating as all new businesses do, so ‘Hereford’, ‘Secure Communications team’, or even ‘Defence Portfolio’ work.

Do we support Critical National Infrastructure or Critical National Services?

- Both. CNI is a broad market term, whereas CNS are the activities that keep the CNI operational. We interchange based on when fits best.

How do I know who to contact about each Service?

- We are allocating points of contact for each service, and will communicate that when complete. Until then, ask your line manager or reach out to the Exec to get guidance.

Thank you

serbus

connect + protect