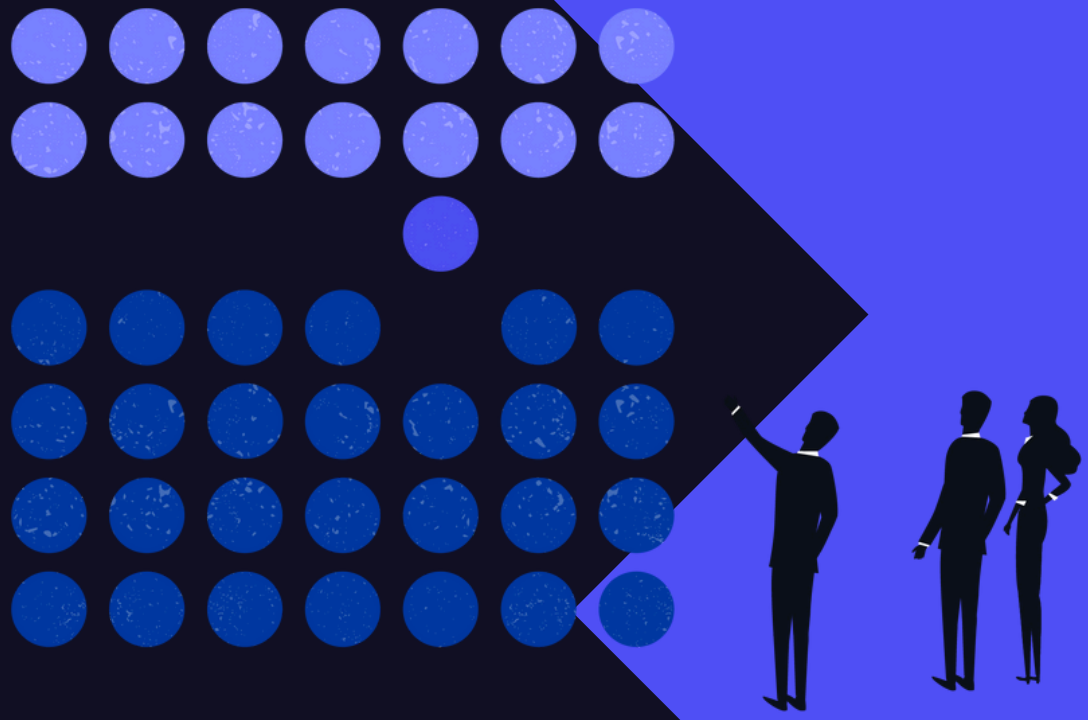
BidCraft



Secure by Design

Responding to MOD requirements on SbD

What is Secure by Design?

The UK government is adopting a Secure by Design (SbD) approach for all central government departments and arms'-length bodies when delivering digital services and tech infrastructure. It is a profound cultural shift from the traditional (sometimes one-shot) accreditation-led responses to a more proactive and holistic method of managing security risk. Systems and capabilities need to be built with security in mind from the start and through the life. This is a good thing, and we need to show we understand and buy in.

The Ministry of Defence is already applying this approach to new procurements, so this guide will focus on MOD principles.

"In a competitive world where the cyber threat and our reliance on digital technology is constantly increasing, it is imperative that cyber-security is a driving function in all that we do. Whether projecting power or keeping the homeland secure, we must preserve our freedom of action through proactive cyber defence and integrated 'Secure by Design' thinking."

Lt Gen Robert Magowan Deputy Commander UK Strategic Command

Historically, the focus on security within many organisations, including suppliers to MOD, has often been driven by compliance requirements.

This focus meant that security measures risked being implemented as a checkbox activity, aimed at meeting the minimum standards required for compliance rather than a genuine attempt to improve the security posture.

Naturally compliance became the focus of our proposals and presentations on bids.

Secure by Design represents a departure from this mindset towards a culture where security is a foundational element of the design and development process.

Rather than being an afterthought or a measure bolted onto a nearly completed project, security is considered from the outset and throughout the lifecycle of a system.

SbD requires a deeper integration of security considerations into every phase of project planning, design, development, and operation. Done well, it's hard work.

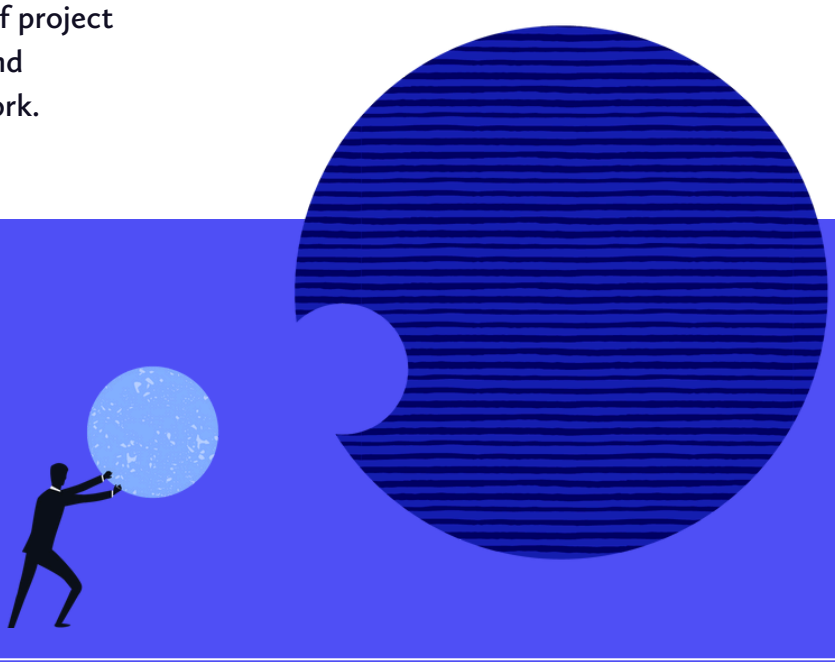
It necessitates ongoing risk management, continuous assessment of threats, and the implementation of security measures that are proactive rather than reactive.

Suppliers are now expected to embed security into the DNA of their projects and services, ensuring that it is not just about meeting compliance standards but about genuinely securing systems against evolving threats.

This cultural change aims to create a more resilient and secure digital infrastructure, reflecting the increasing complexity and severity of cyber threats faced today.

What does that mean for bid people?

We need to describe what we do differently (and make sure the solutions we're proposing are right). No more picking up the old boilerplate and hoping for the best.



The MOD principles

SbD is a framework that government departments can tailor to their own needs. There are a set of principles and activities being developed by Cabinet Office for cross-government, which you will find are slightly different to the ones presented by MOD. Make sure you know exactly what principles your customer is using for each opportunity.

The MOD was an early adopter of the SbD approach and tailored it to their specific complex integration of cyber/digital/physical needs. They are now leading the implementation and are ahead of the Cab Office's cross-government programme.

The MOD Industry Security Notice 2023/09 lays out the MOD way. New projects will all go through the approach, and existing ones will need to transition.

The 7 principles are:

Principle 1: Understand and Define Context

Understand the capability's overall context and how it will use and manage MOD data while achieving its primary business/operational outcome(s).

Principle 2: Plan the Security Activities

Establish security workstream of the capability, perform initial planning including assessment of cyber threat and potential risks while defining clear security requirements, validation and verification.

Principle 3: Implement Continuous Risk Management

Embed cyber security risk management into existing programme governance as a continuous process.

Principle 4: Define Security Controls

Define, architect and implement security control requirements to address risks identified. Reuse existing services and patterns where they exist.

Principle 5: Engage and Manage the Supply Chain

Understand the supply chain role and risks posed, including how to ensure they meet their responsibilities and implement good security.

Principle 6: Assure, Verify and Test

Work with security experts to gain security assurance, test and validate throughout the capability's lifecycle.

Principle 7: Enable Through Life Management

Ensure continuous security monitoring and improvements, including ongoing assurance requirements are enabled, met and disposed.

Get ready to bid

The move away from 'accreditation as assurance' will mean we will need to respond differently to give the assurance, and evidence our implementation of an SbD approach.

This of course means we will have to describe that approach in a different way in proposals, presentations, and any other interactions with the customer teams during bidding.

This also means this is not just the remit of the security team – the entire solution needs to take into account the approach through the whole-life of the project/service delivery.

Step 1: Understand the SbD requirements

Thoroughly review MOD SbD guidelines and publications to understand the specific security principles and requirements that must be incorporated into bids. The approach is evolving so stay up to date (eg DefStan 05-138 is going to issue 4 soon). Find out about CAAT.

Make sure this is a full team activity and not left to the security team alone. Everyone needs to grasp the nuances of what it means for their element of the solution and proposal. For example, Finance need to understand the implications for costs and financial management.

To reiterate – this is not a job just for the security team any more.

Where possible, engage with MOD representatives to clarify any uncertainties about the SbD and related requirements and expectations. Raise any conflicts in advice or requirements (eg a request for a DART reg.).

When there are market engagement sessions foropportunities or frameworks – attend and ask questions. Get involved in trade associations like techUK or Make UK Defence that have links to government.

Step 2: Assess your current capabilities and the gaps

Conduct a gap analysis to compare your organisation's current security practices against SbD and the latest CSM requirements.

Identify areas that need improvement or adjustment to meet MOD standards. Get serious about delivering and bidding for government work.

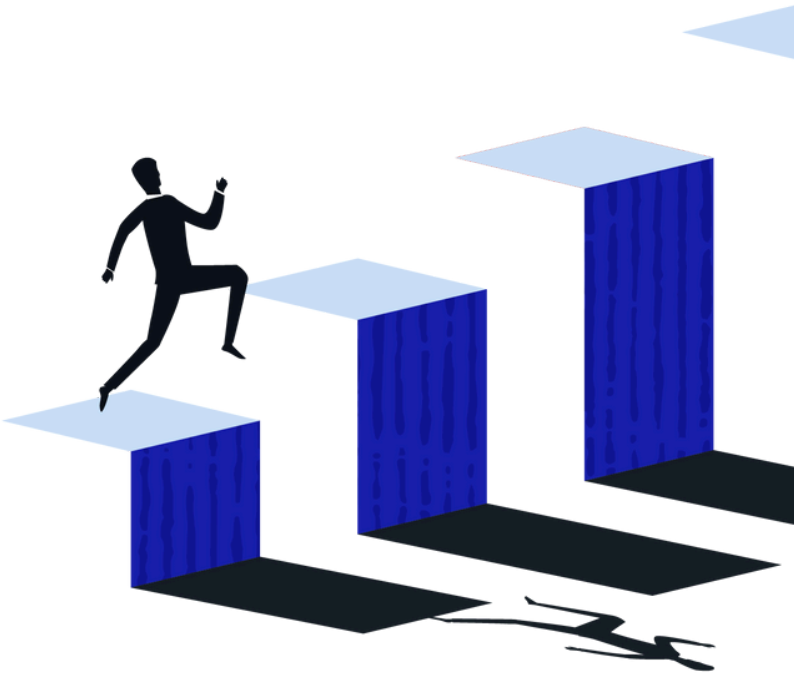
Assess whether your team has the necessary skills and resources to implement SbD principles. Consider training or hiring if there are skill gaps. There could be partner organisations you can work with for training or delivery.

Work out how your risk management plans need to update to align with SbD principles, showing continuous risk assessment and mitigation strategies.

Assess and document the security practices of any subcontractors or suppliers to ensure they also adhere to SbD principles and the relevant DEFSTAN/DEFCON. This is crucial, as the MOD will consider the security of the entire supply chain.

Look for new suppliers as needed early so you are ready to bid. Consider how your supplier management will need to adapt around contracting, reporting, and management.

Step 3: Prepare to bid



Review your case studies for alignment with or actual delivery of SbD approaches. This will be difficult if you have not had to do it yet, but build the case for why your experience and skills are doing the right things even if the work was not specifically labelled SbD.

Develop model answers for security and other questions that will need to take into account SbD and the new approaches.

This will provide guidance for the team and help you understand what you will have to solution.

Read the SAL when you get it. Raise any conflicts with the Authority - they'll be learning too.

What do we write?

Let's use the MOD principles against a proposed new hypothetical IT system to illustrate the kinds of considerations we need to make and what kind of things we should write about. Use this as a trigger for thinking with your team – give yourself the specific context of the services you provide and the typical contract you are delivering under. This guide clearly can't be exhaustive, so use your team's experience and intelligence to work out what is right for your organisation and the opportunities you pursue.

1. Understand and Define Context

What we have to do: Start by demonstrating an understanding of the new service/system's operational context, including the business objectives, potential threats, and how it will manage and use MOD data to achieve its intended outcomes.

Highlight the importance of recognising the system's environment, users (and think about the fairly special types of user Defence has), data flow, and interactions with other systems to tailor security measures effectively.

Things we could write about to provide assurance:

- What is this part of the MOD organisation trying to achieve and how does that fit into the wider objectives? Show our understanding of how this capability will help achieve that.
- What is the broader context of threats and challenges – both internal and external? Think about operational threats developing, technological changes, potential internal weaknesses from culture to specifics like obsolescence.
- Who are the owners and users of the capability being procured, and what are their particular needs? Show your understanding and describe how you will do user research as appropriate or other activities to enhance understanding.
- Give a view of the technical and data context and interdependencies with other systems, and detail how the security architecture is designed to integrate with the current technical infrastructure, considering compatibility and interoperability issues.
- Highlight specific vulnerabilities in the technology stack used by the organisation and how the security design will address specific issues (e.g. is obsolescence and issue?).
- Consider any specific regulatory and compliance requirements (e.g. data protection).
- Give some of the main risks as examples, and the mitigations we would propose.

2. Plan the Security Activities

What we have to do: Detail the planning of security activities, including threat assessment, risk analysis, and the definition of security requirements.

Emphasise the initial and ongoing planning processes that ensure security is a core component of the project from inception.

Things we could write about to provide assurance:

- Outline who we would appoint to lead the security workstream on the project, and what internal and external capabilities they would be able to call on for effective planning and then delivery.
- Describe the recognised security control framework that will be used (e.g. NCSC Cyber Assessment Framework, NIST SP 800-53, ISO/IEC 27002:2022). Explain the rationale for selecting it to guide the security planning process. Discuss how the framework's structure and principles align with the project's objectives and the organisation's security policy.
- Detail the establishment of a security governance structure that defines clear roles and responsibilities for security tasks, as outlined by frameworks like NIST SP 800-53. Include the creation of a dedicated security team if applicable.
- Describe the process of developing security policies and procedures that comply with the chosen framework, ensuring that these documents are accessible and understandable to all stakeholders.
- Describe the approach to planning and what it would result in (reflecting the customer requirement if they have given it, or your chosen method if not).
- Describe the threat and risk assessment method and the rationale for picking it (why it's appropriate for the context).
- Outline what would be produced as a result of the planning and how that would be used – e.g. this could be RAID logs, Risk Assessment Reports, System Security Plans, Cryptographic Management Plans, OSMPs, etc.
- Describe how the planning will then be embedded in delivery – from governance to disposal.
- Make sure the concept of through-life security is clear in the planning approach.

3. Implement Continuous Risk Management

What we have to do: Explain how continuous risk management will be embedded into the programme's governance. Highlight the methodologies and tools used for ongoing risk identification, assessment, mitigation, and management.

Cover adaption to new threats, vulnerabilities and changes in the operational environment.

Things we could write about to provide assurance:

- Start by emphasising and explaining how this is an embedded approach rather than a periodic activity performed in a security silo – get across how we will actively make this happen. Reiterate the context and the risk appetite, and how the risk management informs decisions.
- Adopt a continuous risk management framework, such as NIST's RMF detailed in SP 800-37.
- Detail how risk management activities will be integrated at each stage of the project lifecycle, from initiation through development to maintenance, ensuring continuous assessment and adjustment.
- Describe how we make this a continuous activity – how we carry out each stage of the process from identification through assessment and management, covering elements such as:
    - Identification – how we will model threats and gather potential risks, discover vulnerabilities, how this involves other teams and capabilities, what tools and data we use, and how we make this an ongoing activity that incorporates the impact of change.
    - Assessment – how we perform the assessment, when and by whom, using what kinds of internal and external information and analytical tools, how severity will be calculated (e.g. likelihood and potential impact), and how risk responses and treatment plans will be decided; how will assessment be continuous.
    - Monitoring and management – the processes, people and tech involved; the kinds of controls that will be used to mitigate risks; what changes as the capability moves from design through delivery and operations; and how often reviews will be held.
- Outline how this activity will be documented (e.g. risk registers) reported and evidenced through the project and delivery governance and operational processes.
- Describe the tools (e.g. risk registers, automated monitoring and alerts) that will be used at each stage, who uses them, and their security given the information they contain.

4. Define Security Controls

What we have to do: Describe the process for defining and implementing security controls based on identified risks.

Cover the use of industry best practices and standards for security.

Things we could write about to provide assurance:

- Again, bring the context into the decisions around controls – knowing the risk appetite, operational context, and assets to be protected should inform the security architecture designed and implemented for the specific capability to ensure what is proposed is proportionate to the criticality of the service:
  - E.g. If the Authority has determined the risk appetite as Very Low CRP Requirements as per DEF STAN 05-138(v3) then the control measures are basically maintenance of Cyber Essentials certification;
  - whereas High would entail many more controls like personnel vetting and policies on remote access.
- Describe how the controls will be selected:
  - State what control frameworks will be used as guidance (e.g. MITRE ATT&CK Mitigations, OSWASP Top 10 Risks).
  - Highlight the process for customising these controls to fit the specific context and needs of the project.
  - What standards and design patterns will be taken into account (e.g. MOD has approved design patterns and tooling for specific situations)?
  - How will the controls be agreed and approved?
- Provide a detailed timeline for the implementation of security controls, ensuring that key milestones and dependencies are clearly identified.
- Include procedures for adjusting risk mitigation strategies in response to evolving risk assessments or security incidents, learning from breaches to prevent future vulnerabilities.
- Give some example controls that are appropriate for this specific service/capability in this context – e.g. encryption used, access controls, integrity checks.

5. Engage and Manage the Supply Chain

What we have to do: Outline the approach to managing supply chain risks, including how suppliers are vetted and how their compliance with security requirements is ensured.

This is particularly interesting given the MOD context and threats the users face.

Things we could write about to provide assurance:

- Acknowledge the kinds of threats that come from the supply chain for the specific capability being procured to show we understand the context and importance.
- Describe the responsibilities involved (the teams and owners of each element).
- Supplier selection – describe how you will conduct thorough due diligence on potential suppliers before engagement. This includes assessing their security policies, practices, and reputation in the market.
- Define clear security requirements for suppliers, referencing industry standards and frameworks. Ensure these requirements are incorporated into contracts and service level agreements. Outline requirements for data protection, incident reporting, and compliance with relevant laws and regulations.
- Consider if you will require suppliers to provide evidence of compliance with security requirements, which may include third-party audit reports, certifications, or compliance attestations.
- Describe the process for the continuous assessment of supplier risks, including regular reviews of their security posture and compliance with agreed-upon standards and practices. Establish metrics for monitoring supplier performance against security requirements. This could include metrics on incident response times, compliance with SLAs, and the effectiveness of security controls.
- Make the human connection as well as contract compliance. Build collaborative relationships with key suppliers to foster open communication about security concerns and practices. Encourage suppliers to proactively report security issues and collaborate on mitigation strategies.
- Describe your response plan for supplier-related incidents, from notification through to business continuity and recovery.

6. Assure, Verify and Test

What we have to do: Discuss how security assurance, verification, and testing will be conducted throughout the lifecycle of the IT system.

This includes penetration testing, security assessments (internal and external), and compliance checks.

Things we could write about to provide assurance:

- Start by basing the assurance in the objectives. Establish clear objectives for security assurance that align with the organisation's risk management strategy and the specific security requirements of the system or application.
- State the recognised assurance and testing frameworks and methodologies the organisation uses (and why) to ensure consistency and comprehensiveness.
- If you're developing code describe the approach to static and dynamic vulnerability scanning you will use.
- Describe the development of a detailed testing plan that outlines the testing methodologies, tools, and schedules. This plan should cover all stages of the development lifecycle, from early testing of concepts and architecture to post-deployment.
- If it is appropriate for your solution, implement automated testing tools and processes to ensure continuous testing of security controls and vulnerabilities. This includes integrating security testing into the CI/CD pipeline for real-time feedback.
- Complement automated testing with manual testing by security experts, particularly for complex security scenarios that require human judgement and understanding of context.
- Describe any third-party security experts you will bring in to conduct audits and penetration tests. External assessments provide an unbiased view of the security posture and can uncover vulnerabilities that internal teams might overlook.
- Detail the documentation you will deliver – security assurance practices, test results, audits, assessments, etc.
- Cover incident management if appropriate, continuous improvement, any user testing or similar. Think about all the types of assurance and testing you can deliver with a security view.

7. Enable Through Life Management

What we have to do: Highlight the strategies for continuous security monitoring, improvement, and secure disposal of systems, ensuring they remain secure throughout the lifecycle.

Include appropriate feedback mechanisms and continuous improvement. This is where the move from accreditation to culture change is critical.

Things we could write about to provide assurance:

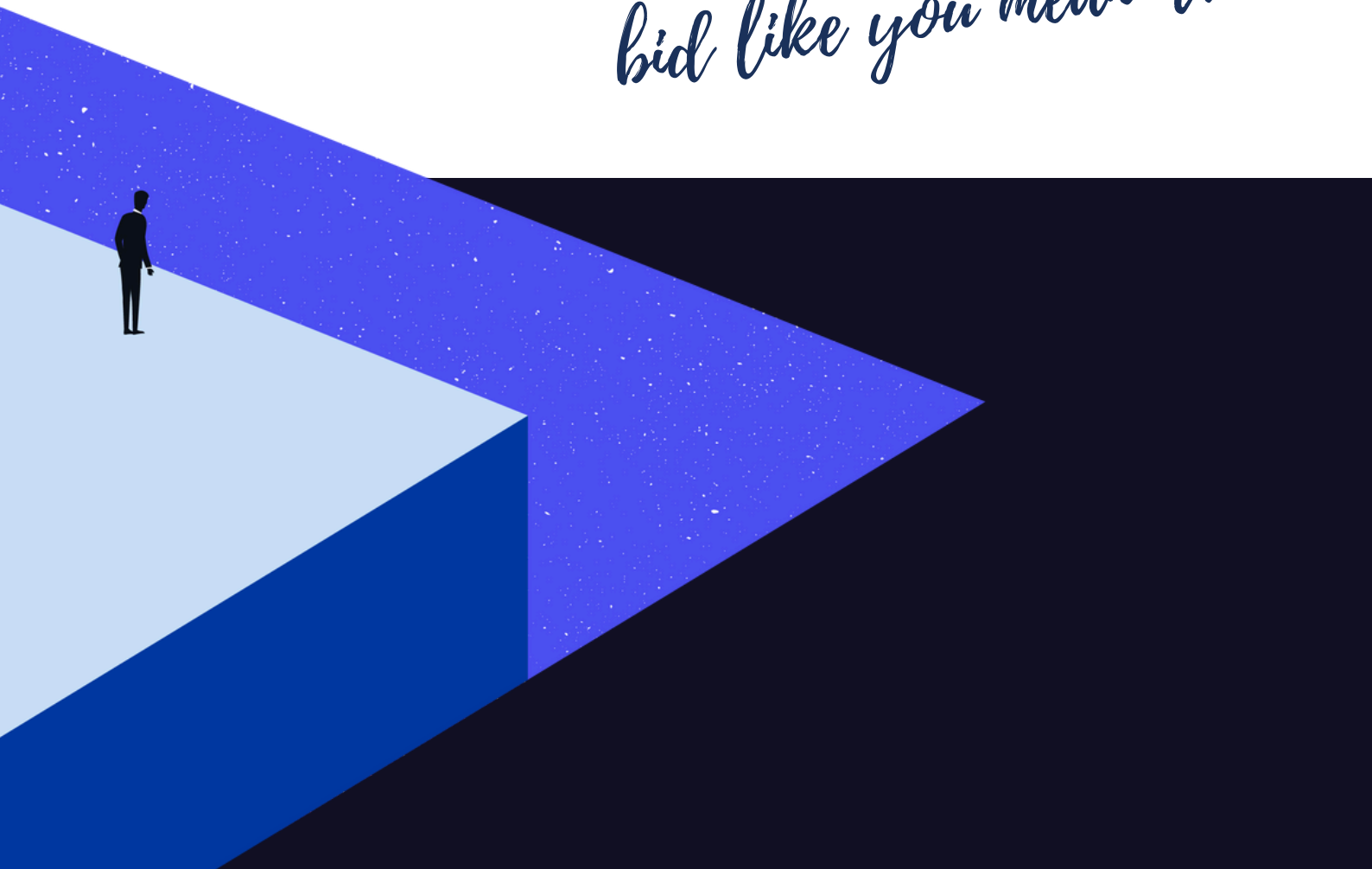
- Outline the specific customer context and importance for this service – including consideration of the Defence Lines of Development as appropriate.
- Describe a comprehensive security strategy that covers the entire lifecycle of the system, detailing how security will be managed at each stage - design, development, deployment, operation, and decommissioning.
- Outline if you are integrating security practices into the development and operational phases if appropriate, using approaches like DevSecOps, to ensure security is a continuous consideration.
- Describe the continuous security monitoring and continuous improvement activity you will perform.
- Have a secure change management process that evaluates the security implications of changes to the system or application. This includes changes in software, hardware, configurations, and third-party components. Think about the implications for the technical context (data and systems).
- Describe any automated tools used to manage configurations and ensure compliance with security policies and standards. This includes patch management systems to deploy security updates efficiently.
- Think about if you will provide ongoing security training and awareness programmes for all personnel involved in the lifecycle management of the system. This could cover secure coding practices, operational security measures, and incident response procedures. What vetting will be needed for personnel as well?
- Make sure you cover decommissioning, disposals and exit as appropriate. E.g. Describe a secure decommissioning process for systems and components that are being retired, ensuring that all sensitive data is securely erased and hardware is disposed of safely.

Last thoughts

To effectively describe your approach to SbD, you need to understand how you will embed security principles throughout the lifecycle of systems and products. This takes some thinking and planning before you get into the weeds of a bid, so do it now.

Do that gap analysis and start to plan. You do not want to be working out what SbD means in the thick of the bid...

If you're going to bid, bid like you mean it!



bidcraft.com

curious@bidcraft.com

BidCraft