

Valcon G-Cloud Lot 3 Service Definition

Security Architecture

[Security Services | Security strategy, Security risk management, Security design, Security incident management, Security audit services, Security quality assurance (QA) and testing, Other]

Version 1.0

1. About Us

Valcon is a leading European consultancy specialising in AI and data-driven business transformation, with a growing and established presence in the UK. A trusted partner to major organisations including multiple UK Government departments and public sector agencies. Valcon connects strategy and operations, helping organisations create value in their transformation programmes.

With over 1,750 consultants across Europe, Valcon brings deep expertise across data, AI, technology and consulting. In the UK, Valcon works with clients across financial services, public sector, retail, industrials and infrastructure. Valcon is backed by private equity firm Rivean Capital.

2. Service Description

We design and implement security controls to protect an organisation's assets, systems, and data from unauthorised access and cyber threats. It encompasses risk assessment, development of security policies, implementation of security controls, identity and access management, data protection, security monitoring, incident response, and compliance with regulations and standards.

Features

- Risk assessment and analysis
- Development of security policies and standards
- Implementation of security controls and mechanisms
- Identity and access management (IAM)
- Data protection measures
- Security monitoring and incident response
- Compliance with regulations and standards
- Integration of security controls with IT infrastructure
- Alignment with business objectives and risk tolerance
- Continuous improvement and adaptation to evolving threats

Benefits

- Enhanced protection of assets, systems, and data
- Reduction of security risks and vulnerabilities
- Compliance with industry regulations and standards
- Improved detection and response to security incidents
- Strengthened security posture and resilience against cyber threats
- Safeguarding of sensitive information and intellectual property
- Increased trust and confidence from customers, partners, and stakeholders
- Support for business continuity and operational resilience
- Alignment of security efforts with business objectives and risk tolerance
- Cost-effective implementation of security controls and measures

3. Approach

Delivering security architecture to a client as a project typically follows a structured approach. Below are the phases commonly used, along with tasks under each phase.

Initiation Phase:

- Define project objectives, scope, and success criteria.
- Identify key stakeholders and establish communication channels.
- Conduct a kickoff meeting to align expectations and goals.
- Develop a project charter outlining roles, responsibilities, and timelines.

Assessment Phase:

- Conduct a comprehensive assessment of the client's existing security posture.
- Identify security risks, vulnerabilities, and compliance gaps through risk assessments, security audits, and penetration testing.
- Analyse threat intelligence data to identify potential threats and attack vectors targeting the client's environment.

Strategy Development Phase:

- Develop a security strategy tailored to the client's specific needs and objectives.
- Define security goals, objectives, and key performance indicators (KPIs) to measure the effectiveness of the security architecture.
- Establish security policies, standards, and procedures aligned with industry best practices and regulatory requirements.

Design Phase:

- Design the security architecture based on the findings of the assessment and strategy development phases.
- Define the architecture's components, including security controls, technologies, and processes.
- Develop architectural diagrams, specifications, and documentation to communicate the design to stakeholders.

Implementation Phase:

- Implement the designed security architecture according to the established specifications and requirements.
- Deploy security controls, technologies, and tools to improve the client's security posture.
- Configure security policies, access controls, and encryption mechanisms to enforce security requirements.

Testing and Validation Phase:

- Conduct testing to validate the effectiveness and functionality of the implemented security architecture.
- Perform security assessments, penetration testing, and vulnerability scans to identify any weaknesses or vulnerabilities.
- Validate compliance with industry regulations and standards through audits and assessments.

Training and Awareness Phase:

- Provide training and awareness programs to educate employees and stakeholders about security best practices, policies, and procedures.
- Conduct phishing simulations and security awareness training to help employees recognise and respond to security threats effectively.
- Promote a culture of security awareness and accountability throughout the organisation.

Monitoring and Optimisation Phase:

- Implement monitoring and logging mechanisms to track security events and incidents in real-time.
- Monitor security metrics and KPIs to assess the effectiveness of the security architecture.
- Continuously optimise the security architecture based on feedback, lessons learned, and evolving threats and technologies.
- 4 Valcon G Cloud

Reporting and Documentation Phase:

- Generate regular reports and dashboards to communicate security metrics, KPIs, and trends to stakeholders.
- Document security incidents, response activities, and lessons learned for post-incident analysis and compliance purposes.
- Provide recommendations and actionable insights to help the client improve their security posture and achieve their security goals.

By following this structured approach, organisations can effectively deliver security architecture projects to clients, helping them enhance their security posture, mitigate risks, and protect against evolving cyber threats.

4. Effort and Cost

Effort will be determined collaboratively between the Valcon and the client based on the skills mix and scope required.

Please refer to the Pricing Document for current rates.

- Rate card prices are exclusive of VAT.
- Expenses are recharged at cost and supported by receipts.
- Expenses may include reasonable travel, accommodation, and subsistence costs.
- The payment schedule will follow milestone completions as agreed in the Statement of Work.

5. Assumptions

The successful delivery of the engagement depends on assumptions and dependencies jointly agreed between the Valcon and the client.

- These may include (but are not limited to):
- Access to required stakeholders, systems, or information
- Timely decisions and approvals
- Availability of resources and infrastructure
- Defined governance and communication processes

All assumptions and dependencies will be recorded and validated as part of the Statement of Work (SoW).