Security Architecture

Purpose:
To provide security architecture consultancy to ensure the secure development, implementation and delivery of cloud systems.

Overview:
Actica can provide security architecture advice and support at all stages of programme, project and system delivery. Our consultants include a number of Chartered Cyber Security Professional and Certified Cyber Professional (CCP) Security Architects who are experts in the development and review of security, business and technical architectures. Our services include:

- **Security Architecture Development.**
  We provide consultancy to develop the security architecture for an organisation, project or system, aligned to standard methodologies (e.g. TOGAF, SABSA, etc.) or other formats as required. This service starts with information gathering to understand the business and technical context. We ensure there are clearly identified business requirements and outline solution architecture(s) in place; if not, we can develop them to ensure a stable foundation. We conduct assessments to identify the threats and inherent risks associated with the proposed solutions. We undertake analysis to identify and document potential risk treatments and the architectural security requirements. We develop security architecture options by identifying potential controls and accompanying trust models. Where applicable we make use of existing architectural blueprints or patterns, tailored as required. We analyse the options with respect to residual risk, cost, timescale and impact on the business, to identify the preferred architecture. The output is a security architecture that demonstrates how the controls will address the risks in accordance with objectives and risk appetite; it enables subsequent secure design and implementation.

- **Security Architecture Implementation Consultancy.**
  We help implement the security architecture, including security design and implementation support. This task involves identifying the specific implementation for the controls identified in the security architecture. We work alongside the solution and technical architects and developers to ensure that the security controls are integrated with the overall solution and configured appropriately to reduce the vulnerabilities. Throughout the task we liaise with all stakeholders to ensure the selected controls are aligned to the business objectives and risk appetite. The output is a security design and implemented secure solution that enables the client to achieve its business objectives while effectively balancing cost, risk and business impact.

- **Security Architecture and Design Review Consultancy.**
  We provide consultancy to review externally-produced security architectures and designs. We analyse the selected security controls to identify whether they effectively address the risks, in accordance with the client's business objectives, budgets and risk appetite. We identify the extent to which the security architecture is consistent with good practice. If necessary, we will conduct a high-level risk assessment to underpin the analysis. We present the output to business and technical stakeholders. The output is a security architecture / design review report which enables the client to understand and amend the security architecture, if required, to ensure an effective solution can be developed.

- **Secure Development Lifecycle Consultancy.**
  We provide guidance on the secure development, build, operation and management of systems & services. We liaise with the client to understand the business and technical context, including business strategy and objectives; IA strategy; development, build, deployment, operation and management processes and governance structures in place; and the underlying technical infrastructure underpinning the systems and services. We analyse and provide advice including access to the systems by developers / administrators, management systems, protective

monitoring, security testing and vulnerability scanning, patch management, operational security management, etc., ensuring it is consistent with the methodologies in place (e.g. Waterfall, Agile, ITIL, DevOps, etc.). The output is improved lifecycle processes that achieve a better balance between residual risk, cost and business impact.

Information Assurance:
We can provide relevant security advice for services of any classification. We employ security cleared personnel who operate with information at all levels of the Government Security Classification Policy (GSCP). Our systems are approved to hold classified information.

Pricing:
This service is priced based on anticipated resource requirement. Resources will be charged in accordance with the agreed SFIA day rates. Two pricing options are available:

- Firm price. The firm price will be based on the anticipated resource requirements including provision for risk. Provision for travel and subsistence cost will be made. Payment will be required against achievement of agreed milestones. Customers may request clarification of the number of days by SFIA grade for their specific deliverables, which will be confirmed by Actica for contract award.
- Limit of liability. The limit of liability will be agreed based on an anticipated resource requirement. Charges will then be made monthly in arrears against resource effort expended. A limit of liability will also be agreed to cover travel and subsistence. Travel and subsistence costs will be charged at cost monthly in arrears against cost incurred.

Service management details and constraints:
Our service is subject to ISO9001 certified quality controls. A lead consultant shall be appointed who will have responsibility for liaising with the client and managing the Actica team providing the required services. In addition, a Project Authority will be appointed who is normally a Director within the Company who will act as the point of escalation. We support our clients on-site, via email or by telephone, during standard office hours and with a 1 business day response time to acknowledge support requests.

Data backup and recovery:
Where our staff use infrastructure and information provided by our clients, it is the clients' policies and procedures that prevail. Ordinarily, our consultants are supported by our own infrastructure up to, and including OFFICIAL, and we have facilities for higher classification information to be received, stored and transmitted. Our consultants' laptops and our corporate systems are backed up regularly and our corporate Disaster Recovery Strategy and Plan ensures that we are able to continue to provide services to our clients in any event.

On-boarding/off-boarding:
For all of our assignments we operate our standard on-boarding/mobilisation activities. At assignment closure, we undertake a review and ensure that skills have been transferred to client staff where appropriate.

Ordering and invoicing process:
Specific details of the clients requirement should be sent to cloud@actica.co.uk. Following discussions about your requirement, Actica will send a fully priced proposal detailing the services to be provided. Once approved, a valid purchase order should be sent to finance@actica.co.uk for processing. Once the work is completed and accepted by the client, Actica will invoice the client for the work. Payment is expected within 30 days. We are able to use a range of electronic purchase and payment systems (e.g. CP&F).

Consumer responsibilities:
To liaise with the Actica lead consultant and ensure access to existing security information and key stakeholders including the system accreditor.

Contact Details
Actica Consulting Limited
4 Stirling House
Stirling Road
Surrey Research Park
Guildford
Surrey, GU2 7RF

Telephone: 01483 484090
Email: info@actica.co.uk
Website: www.actica.co.uk

Registered Office in England as above
Company Number 03396854