network futures

#CloudFutures Enterprise Security Architecture Services

Service Description

We define preventative, detective, corrective and directive controls to assist with the implementation and protection of the information technology deployed by the enterprise. We provide professional enterprise security architecture services that help to achieve the goal of aligning security and business needs, using industry standard methodologies and frameworks.

Service Features

Conceptual architecture for business risk: definition of security architecture governance

We help define your Security Architecture which is your route to successful governance of business risk. We help with your understanding of the route for governance of detailed security architectures.

Physical architecture mapping to conceptual architecture: definition of security practices

We help you with the definition of security practices that you require across the solution. This will define the physical (or logical) architecture providing as much detail as possible without containing any implementation details. This will aid and inform your organisation with a high level understanding of physical (or logical) architectures and potential attack surfaces.

Component architecture map with physical architecture: international standards and tools

We have experience in using the best practice as defined by international standards and tools to map the components of the solution to physical (or logical) architecture. To do this, we utilise the standards and products, from internationally recognised standards organisations, to map physical (or logical) architecture to detailed component attack surfaces.

Operational architecture: guidelines, processes and procedures

Our team will steer you through the development of details guidelines, processes, and procedures with which you will be able to manage and secure your solution. We help create guides for implementation, administration, patch management, logging, monitoring, forensics, and more, as required. We understand that every organisation is different, with different expectations of project or programme artefacts, so we help you define these with appropriate product descriptions and develop the artefacts themselves.

Designing architecture components: detailed policies, user awareness, infrastructure compliance

We help you with the development detailed policies, user awareness packs, and ensuring infrastructure compliance through the development of policies, develop content for user education. We will steer you through the development and implementation of physical and logical controls to secure your environment.

Disaster recovery architectures: business continuity needs for each solution

We know that for every solution, there is a different appetite for business risk in the event of disaster. When disasters occur, we understand that your business continuity needs for each solution will be different as appropriate to the criticality of the solution to the business. Our experienced team will help you to develop business risk impact assessments at the earliest stages of each project and programme to drive the design, development, and implementation of appropriate business continuity in each and every solution. Being ready for disaster is simple if you start early. Adding business continuity measures after a disaster occurs, are always more painful, and frequently very expensive and sometimes cost prohibitive, especially if the worst should occur before business continuity needs have been met, and a disaster occurs.

Threat and vulnerability management: controls and directives

Throughout the development of a new solution, we will plan appropriate controls and directives that will help you to react to business risk breaches, and to enable proactive approaches to holistic business risk mitigation. Through integration of modern technology stacks provide robust automation for a better enhanced information security stance than ever before.

Security incident and event management: combined monitoring and analysis

We use combined monitoring and analysis security solutions to help with the automated and manual identification of potential threats and vulnerabilities. SIEM tooling helps to aggregate and automatically analyse activity across the IT estate, offering real-time analysis and monitoring of events. Using SIEM tooling, we help your organisation to recognise potential security threats and weaknesses before business disruption occurs. Modern SIEM tooling offers user and entity advanced behaviour analytics utilising the modern machine learning, and artificial intelligence (AI) technology.

Regulatory business architectures: local and international regulatory controls

We understand that in a global environment, organisations will be subject to multiple local and international regulatory controls. Our team have experience with international security standards such as General Data Protection Regulation (GDPR), and Payment Card Industry Data Security Standard (PCI DSS). We help deliver your organisational compliance with local regulation and international regulation, through the definition and implementation of increased security controls.

Directive controls: improving the maturity level of enterprise security architecture

Our team are used to implementation of directive controls to ensure a particular outcome is achieved. In the past, guidelines encouraged compliance, but today, preventative controls are often used to limit the possibilities of an undesirable outcome. We believe that directive controls help to improve the maturity level of enterprise security architecture through iterative development of initial, managed, defined, quantitative, and optimised controls.