15. Security Architecture Principles

Date: 2019-04-29

Note that CCS Architectural Standards are now mastered in Confluence. The updated version of this standard can be found at:
https://crowncommercialservice.atlassian.net/wiki/spaces/AG/pages/585728048/Security+Standards

Status

Approved

Decision

At the meeting the TDDA held 29 April 2019 the attendees approved the issue of the Service Security Architectural Principles ADR. The document would be recirculated after the Supplier Information Security Assurance Policy has been approved.

Context

All Government service shall need to be delivered and operated under the HMG Security Policy Framework https://www.gov.uk/government/publications/security-policy-framework. In order to be able to consume a solution with the confidence, each HMG Department and CCS Suppliers has developed bespoke security profile which they expect the service to be assured against. However, in order that Crown Commercial is able to deliver common good and services across Government, there is a need to define a common set of security controls.

Decision

Crown Commercial shall implement security architectures that are designed to achieve the following security goals. These security goals are to:

- make an initial compromise of the system difficult
- limit the impact of any compromise
- make disruption of the system difficult
- make detection of a compromise easy

An attacker can attempt to subvert technology, people and processes to undermine security, so security architecture must consider all the technology, people and processes relating to the service.

Of course, it is not enough for a service to only be secure. It needs to meet user needs, be cost-effective, and account for any other constraints relevant to the scenario. Therefore, Crown Commercial Service always aims to design a service to be 'secure enough' whilst balancing these other aspects too.

In support of achieving the security goals, outlined above, all deliver programme shall undertake the following security controls:

- Incorporate the security standards defined with the Crown Commercial Service Digital and Technology Strategy into the Service Specification. https://intranet.crowncommercial.gov.uk/task/digital-and-technology-strategy-2018-21/
- Evidence compliance with the HMG Minimum Cyber Security Standard https://www.gov.uk/government/publications/the-minimum-cyber-security-standard
- Demonstrate delivery of the NCSC Cloud Security Principles outcomes https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles
- Evidence the Software Delivery Life cycle is undertaken securely through the application of the NCSC Secure Development and Deployment guidance.https://www.ncsc.gov.uk/collection/developers-collection?curPage=/collection/developers-collection/principles
- An **CHECK/CREST IT Security Health Check (ITSHC)** of the Service has been performed within 12 months of go-live and annually thereafter. The testing has been undertaken in accordance with HMG best practice. https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance/it-health-check-ithc-supporting-guidance
- Comply with the CCS Supplier Information Security Assurance Policy ref ??

Consequence

New services will apply the above security controls unless there is an architectural decision overriding this decision. Each CCS delivery team shall nominate an individual who is responsible for ensuring achievement of the security goals described above.
The ADR shall be reviewed in 6 months and post a review of the supporting documents identified above.