Cybersecurity Strategy and Operational Assurance Service

Designed to be final phase of the CCS Cybersecurity Development Program series, the CCS Cybersecurity Strategy and Operational Assurance Service can take the place of dedicated in-house cybersecurity expertise for the short, medium, or even long-term. Depending on client needs, the service can include:

1. **Continued alignment of cybersecurity to corporate strategy and business goals** - *Often called 'virtual CISO' or other buzz-phrase, it is nevertheless a fact that few organisations require a full-time employee at this level. The role must be fulfilled however*;
2. **Cybersecurity representation in the Governance meetings**[1] - *Most organisations already have representatives for Sales, Operations, Legal, HR etc, few have dedicated in-house cybersecurity expertise. It is critical that security is in on everything*;
3. **Operational Assurance / Internal Audit**[2] - *Every Key Domain entails the periodic maintenance of some process, some have several. From quarterly vulnerability scans to annual penetration tests, security controls must be operationalised and measured in order to be effective.*

The service is designed to be completely flexible in terms of tasks, deliverables and longevity. In an ideal world this service would not be required, so the service will provide only what is required, for as long as it is required and no more.

CCS fundamentally believes that it is the job of a consultant to teach, not to do [necessarily], security strategy should not be outsourced forever.

Methodology

[Dependent on client requirements.]

Below is a sample of operationally 'periodic' tasks;

Key Domain	Program Development Goals
Governance	Bi-weekly/monthly/quarterly Governance Committee Meetings.
Policy Set	Annual review of Policies, changes to Standards after patching etc.
Legal	Review of adherence to regulatory and contractual obligations.
Human Resources	Review of on-boarding procedures, access control, SAT etc.
Asset Management	Comparison of asset register to vulnerability scan results etc.
Risk Management	Annual risk assessment, or for significant changes.
Vulnerability Management	Weekly/monthly/annual vulnerability scans, pen test, patching etc.
Project Management	Review of risk / privacy impact assessment for significant changes.

[1] Representing Information Security as a separate and distinct function.
[2] These should only ever be temporary as operational functions much be absorbed in-house.

Access Control	Review of access control mechanisms to role requests.
Vendor Mgmnt. & Due Diligence	RFP development, perform due diligence on proposed 3rd parties.
Security Awareness & Training	Review and update of annual SAT, senior hire one-on-one etc.
Data Security	Review of data classification adherence, and industry trends etc.
Secure Code Development	Manual code reviews, automated code checks[3]
Physical Security	Manual walkthroughs and social engineering tests[4]
Security Controls - Protective	Review of protective systems to determine continued suitability.
Security Controls - Detective	Review of detective systems to determine continued suitability.
Security Monitoring	Review of systems output to confirm full infrastructure coverage.
Incident Response	Semi-annual/annual incident response tests with key personnel.
Disaster Recovery	Ensure disaster recovery plans continue to meet business needs.
Business Continuity Planning	Is security fully enabling the business's long-term goals.

Assessment Plan

[Not applicable.]

Timeframe

[Client defined.]

Deliverables

- Cybersecurity strategy in-line with business goals;
- Tactical guidance for stakeholders in each Key Domain;
- Governance Committee representation;
- Operation Assurance for selected Key Domains;
- Internal Audit and Board reporting;
- Client defined tasking.

[3] Conducted by CCS partners and may incur additional costs.
[4] Conducted by CCS partners and may incur additional costs.