Cybersecurity Program Development Service

Designed to be the next logical step after the completion of a CCS Cybersecurity Gap Analysis, the Cybersecurity Program Development Service achieves the following three main objectives:

1. **Lays the foundation for IT/IS to enable the business under Governance**[1] - IT/IS *Governance in its purest/simplest form is the 'technology' side and the 'business' having meaningful conversations. IT/IS are enablers, nothing more, so the business side needs to share the goals as defined at the highest leadership levels*;
2. **Oversee the development of an appropriate Policy Set**[2] - *An organisation's Policies, Standards and Procedures are its culture, operating baseline, and corporate knowledge respectively. Without a formal process in place to create and maintain this Policy Set, no security program will get off the ground*;
3. **Implement an appropriate Risk Management program** - *From Risk Assessment, through Vulnerability Management and Incident Response, to Business Continuity, there's no point being in business if you don't intend on staying in business*.

The remaining aspects of security (as defined by the Key Domains, see below), are ALL secondary to these foundations. Trying to build a security program, especially the technology aspect, without these in place is no different from building a house on quicksand.

The development of the remaining Key Domains will necessarily be to the needs of the business in question.

Methodology

The above foundations represent a very significant investment in not only up-front resources, but a long-term commitment to the establishment of a sustainable security program. In all likelihood it will be many months, or even a number of years before the foundations laid here are intrinsic to the culture. The process is difficult and there are no shortcuts.

However, significant progress can, and should, be made in *all* Key Domains. Some represent long lead-time projects, some a significant shift in responsibilities and task ownership, and others may involve capital investment. Regardless of the challenges, if these programs aren't run at least somewhat in parallel their benefits may be unacceptably delayed. CCS will enable these programs.

While the development of a security program must be done properly, it's still about risk reduction so it's important not to get caught in 'analysis paralysis'. Take the first steps, the details work themselves out. It is CCS job to ensure that the program does not falter for lack of guidance.

[1] CCS can draft, and help implement, an appropriate Governance Charter to ensure that the Governance function has everything it needs to ensure its adoption and ongoing maintenance.
[2] Optionally, CCS can draft a comprehensive set of Policies and create a sustainable Document Management System.

Below is a summary of the security program development goals;

Key Domain	Program Development Goals
Governance	Business goals built in to every aspect of IT and IS.
Policy Set	Documented 'recipes' for a sustainable security program
Legal	Security supports contractual and regulatory compliance.
Human Resources	Role based access and security training start here.
Asset Management	An asset management system as the core of all program projects.
Risk Management	Finding and addressing your biggest risks.
Vulnerability Management	Reducing the attack vectors for all systems.
Project Management	Building security into every change to the business.
Access Control	Proper handling all joiners, movers, and leavers.
Vendor Mgmnt. & Due Diligence	Extending security to those not directly under your control.
Security Awareness & Training	Educated people making far fewer mistakes.
Data Security	Discover, label, and protect your critical data assets.
Secure Code Development	Secure the 'gateways to your data'.
Physical Security	Literally close the door on theft.
Security Controls - Protective	Proper configuration / placement of protective security controls.
Security Controls - Detective	Proper configuration / placement of detective security controls.
Security Monitoring	Mapping all system output to a known-good baseline.
Incident Response	Reactive and PROactive treatment of anomalies.
Disaster Recovery	How to get back in business while you still HAVE a business.
Business Continuity Planning	Job security for al!

Assessment Plan

A more detailed Project Definition Plan (PDP) will be made available well in advance of project kick-off, but in essence:

Phase 1: Kick-Off / Program Goal Confirmation (performed on-site)

- Meet with senior leadership to reinforce commitment and agree the overarching *business* goals for the security program development;
- Meet with key stakeholders to agree project activities;
- Meet individually with key stakeholders to discuss department / LoB specifics with regard priorities and resource availability;
- Agree all next steps, timelines, and functional responsibilities;

Phase 2: Project Plan Definition (performed off-site) - *Optional*

- Work with client project manager to produce comprehensive project plan.[3]

[3] CCS does not provide a project management function but will work with whomever client assigns (if applicable).

Phase 3: Program Execution (performed on-site)

- Details vary significantly per unique business, but this Phase encompasses the execution of all departmental / LoB action items as detailed in the project plan (if applicable);

Phase 4: Project Close (performed on-site)

- The CCS Cybersecurity Program service is entirely tactical in nature, however, as a close to this stage of program development CCS will provide a final report and presentation to ensure appropriate hand-off to internal client resources.

Timeframe

The process for executing a security program can only ever be unique to each organisation, and depending on available resources/skill-sets/budget, the consulting time required will vary enormously.

In the end the timeframe will depend entirely on the organisation in question, CCS is there to support the work performed, not [in most cases] to do it.

Deliverables

- Governance Charter and sample meeting minutes from first meeting[4];
- Branded and bespoke Information Security Policies;
- Branded templates for all known Information Security Standards and Procedures;
- Document Management process;
- Sample Risk Assessment report based on agreed risk management process(es);
- Information Security Risk Register including current risk treatment plan;
- Other client-specific deliverables will depend on type and length of engagement.

[4] Client must run subsequent meeting and take minutes accordingly.