AXIA COMPLIANCE

Cyber Security Program Development Service

Designed as the secondary logical step after the completion of an AXIA Cybersecurity Gap Analysis, the Cybersecurity Program Development Service achieves the following three key objectives:

1. Lays the foundation for IT/IS to enable the business under Governance

IT/IS Governance is the 'technology' side and the 'business' having meaningful conversations. IT/IS are enablers, so the business side needs to share the goals as defined at the highest leadership levels;

2. Oversee the development of an appropriate Policy Suite

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 be successful;

3. Implement an appropriate and effective Risk Management program

From the initial Risk Assessment, through to Vulnerability Management and Incident Response, to Business Continuity, there's no point being in a business if you don't intend on remaining in business.

The development of the remaining Domains will necessarily depend on the unique needs of the business and is tailored to these individual requirements.

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 and appropriate security program. In all likelihood it will be many months, or even a number of years before the foundations laid here are fundamental to the culture of an organisation. The process is challenging and there are no shortcuts to effective cyber security.

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

While the development of a security program must be done appropriately, it's still primarily 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 AXIA's job to ensure that the program does not falter for lack of guidance.

AXIA COMPLIANCE

Below is a summary of the security program development goals;

Domain	Program Development Goals
Governance	Business goals built into 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 effectively 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 Management & Due Diligence	Extending security to those not directly under your control.
Security Awareness & Training	Educated people making far fewer mistakes.
Data Security	Discover, classify, 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	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:

<u>Phase 1: Kick-Off / Program Goal Confirmation</u>

- 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 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.
Development Service

Phase 3: Program Execution

Details vary significantly as every business is different, but this Phase encompasses the execution of
all departmental action items as detailed in the project plan (if applicable);

Phase 4: Project Close

The AXIA Cybersecurity Program service is entirely tactical in nature, however, as a close to this stage of program development AXIA 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.

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

Deliverables

- Governance Charter and sample meeting minutes from first meeting;
- 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.

For additional information on our Cyber Security service please use the

'Contact Us' section of our website www.axiacompliance.com or

email us directly at compliance@axiacompliance.com