AXIA COMPLIANCE

Cyber Security Gap Analysis

AXIA cyber security Gap Analysis Service

Cyber Security is fundamentally, effective risk management and AXIA excel in providing this to clients in protecting against financial loss, reputational damage and regulatory fines.

AXIA's Cyber Security Gap Analysis is developed to help and guide organisations on their cyber journey. We assess a broad number of controls and technologies to provide you with an in-depth report detailing cyber security gaps within your environment.

In undertaking a security gap analysis, your organisation can effectively evaluate its strengths and weaknesses when considering their current cyber security posture.

The AXIA Cybersecurity Gap Analysis service is designed to achieve three key objectives:

1. Determine the top cybersecurity risks to your business so you can fix them at the earliest opportunity resulting in immediate risk reduction;

2. Determine the major projects that should begin immediately in order to fix the top risks permanently; and

3. Prepare the foundation for development of a sustainable and proportional security program for your business.

The AXIA Methodology

AXIA Compliance has developed its proprietary assessment methodology based on both the ISO/IEC 27001:2022 – Information Security Management Systems Standard and the NIST Cybersecurity Framework for coverage of the most widely used and accepted industry best practices globally.

Our assessment measures your security capability and maturity depending on your priorities, current posture, and how extensively you want to invest in security;

What Domains?

Domain	Explanation
Governance	Security is not at 'IT problem', it's a business problem.
Policy Set	The foundation of any security program.
Legal	Lawyers have to be involved.
Human Resources	The most underutilised resource in security today.

AXIA COMPLIANCE

Asset Management	You need to know what you are managing.
Risk Management	Your risk appetite controls your cyber security budget.
Vulnerability Management	What the bad actors are up to.
Project Management	Security by design and default.
Access Control	Who has their hands on the crown jewels?
Vendor Management & Due Diligence	Are your 3rd parties as secure as you?
Security Awareness & Training	It's harder to fool an educated person.
Data Security	How secure is your information?
Secure Code Development	Security by design and default.
Physical Security	Firewalls don't stop you walking away with it.
Security Controls - Protective	Firewalls, Anti-Malware, IPS, 'Whitelisting' etc...
Security Controls - Detective	Detective IDS, File Integrity Monitoring, etc...
Security Monitoring	What is your technology telling you?
Incident Response	Do you want to stay in business?...
Disaster Recovery	...assuming you do, here's how...
Business Continuity Planning	...and here's the time you have to do it in.

All deliverables have been developed to directly feed into a plan for achieving ISO 27001 certification if desired.

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: Obtain Gap Analysis Pre-Requisites - if available (performed off-site)

- Network and/or Data Flow Diagram(s);
- Asset Register(s);
- Policy Set (Policies, Procedures, and Standards);
- Stakeholder Matrix/Org Chart (key stakeholders per business function); and
- Latest Risk Assessment Report and/or Risk Register.

Phase 2: Kick-Off / High-Level Risk Assessment

- Meet briefly with senior leadership to gauge commitment and discuss risk appetite;
- Meet with key stakeholders to agree project activities;
- Meet individually with key stakeholders to discuss relevant business processes, primary data;
- assets, regulatory obligations (if applicable), and top risks;

- Perform deeper dive into current security controls;
- Perform walk-through of facilities (if applicable).

Phase 3: Reporting (performed off-site)

Produce a comprehensive Gap Analysis Report.

Phase 4: Presentation of Findings to Senior Leadership – Optional

Meet briefly with senior leadership to present findings and discuss strategic options.

Timeframe

The entire gap analysis can be performed in as little as 5 days for very small environment, or if the goal is just to determine the top risks to the business.

Deliverables

- Comprehensive Gap Analysis report mapped to both ISO 27001 and the NIST Cybersecurity Framework;
- Prioritised list of top risks to the business with initial remediation options;
- Draft Target Operating Model to compare 'current state' cybersecurity maturity against risk appetite;
- High Level Project Definition to identify the necessary tasks, technology(ies), and resources to implement the desired cybersecurity maturity.

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