# Cybersecurity Gap Analysis Service

The CCS Cybersecurity Gap Analysis service is designed to achieve three main objectives:

1. **Determine the top cybersecurity risks to your business** so you can fix them at the earliest opportunity - *immediate risk reduction*;
2. **Determine the major projects** that should begin immediately in order to fix the top risks permanently - *fix, don't patch*; and
3. **Lay the groundwork** for development of a sustainable and *appropriate* security program for your business – *keep it fixed*.

This is what security is really all about. Find the top risks, fix them permanently, move on to the next.

## Methodology

CCS utilises a proprietary assessment methodology based on both the ISO/IEC 27001:2013 – Information Security Management Systems Standard[1] and the NIST Cybersecurity Framework v1.1 for coverage of the most widely used and accepted industry best practices globally.

The assessment measures your security capability and maturity for up to 20 Key Domains, depending on your priorities, current posture, and how deep you want to go;

| Key Domain | What is it? |
|---|---|
| Governance | Security is not at 'IT problem', it's a *business* problem. |
| Policy Set | The foundation of any security program |
| Legal | Like it or not, the lawyers have to be involved. |
| Human Resources | The most underutilised resource in security today. |
| Asset Management | You can't manage what you don't know you have. |
| Risk Management | Your risk appetite controls the purse strings. |
| Vulnerability Management | What the bad guys up to. |
| Project Management | Security by design and default (SBD[2]). |
| 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 the basket your eggs are in? |
| Secure Code Development | Security by design and default …again. |
| Physical Security | Firewalls don't stop you walking away with it. |
| Security Controls - Protective | Firewalls, Anti-Malware, IPS, 'Whitelisting' etc. |
| Security Controls - 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. |

[1] All deliverables will feed directly 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 (performed on-site)**

- 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 comprehensive Gap Analysis Report (sample here);

**Phase 4: Presentation of Findings to Senior Leadership (performed on-site) - *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. Like any service, you can have only 2 of the 3 from cheap, good, and fast. You will get what you pay for.

## Deliverables

- Comprehensive Gap Analysis report mapped to both ISO 27001 and the NIST Cybersecurity Framework v1.1;
- 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.