



Information Security Review

Do you suffer from IT interruptions ?
Do your customers trust that your systems are secure?
Do you hold confidential information insecurely?
Can you recover from catastrophic IT failure?
Are you compliant with GDPR ?

How we can help you

High level IT security review

We offer a high level health check on your business IT systems. We assess the IT risks and the opportunities for improvement under the following headings:

- Strategic IT risks
- IT procedures

Gaps identified

We identify where your IT systems are at variance from leading practice or where they are not in place.

Improvement recommendations

We provide high level recommendations in relation to any IT system gaps or variations from leading practices.

Recommendations are supported by detailed actions, in priority order, that is comprises:

- Detailed description of issues or gaps
- Detailed recommendations
- Summary of effort required
- Supporting data such as web references , file names or process guides.

What is in it for you – business benefits?

The key benefits to your business are:

Security Assurance

The assurance of knowing how effective your security controls are and where there are gaps what needs to be done to remedy them.

Client confidence

Provide clients with the confidence that your security controls are demonstrable.

Being able to assure clients, whose personal information you handle, about how well you protect that personal information

Continuity risk assurance

Confidence in your preparedness and ability to address unexpected disaster events.

Comprehensive

Our depth of experience and knowledge provides you with the assurance that the full range of information security risks are assessed.

The business impacts that arise from security gaps identified are quantified and presented in an understandable way.

About our service

We offer a quick review that will identify and prioritise your top security issues and give you the necessary data to fix them. This review will typically take place over two days on site and by its nature is not an exhaustive assessment of all your security controls.

We do not assess the security of Application programs, including Web applications or third parties (without their permission)



Information Security Review

Scope of work ?

The security review will encompass the following areas:

- Access and Security processes
- Policies and security architecture
- Security risk management
- HR and asset management
- Software acquisition and development
- Operations management and communications
- Information security incident management
- IT and Business continuity planning
- Compliance to:
 - Regulations
 - Licences
 - Data Protection
 - Audit and review processes
- Physical security.

The review follows the domain structure of the security standard ISO 27002.

Who we are

The director of O'Farrell Associates, **Michael O'Farrell** is an experienced IT security practitioner having delivered security services to many Irish and international blue chip companies. Michael has more than 24 years IT management and security experience and holds CISSP and CISM certification. He is also member of the Business Continuity Institute.

Email: Michael@ofassociates.com

Phone: +353 (0)87 2838 667

Web: www.ofassociates.com



Our deliverables – sample output

We provide a comprehensive report including:

- A Summary of findings,
- A high level overview of findings complete with a rating, for management use, and
- Details on how to fix the gaps identified and indication of how big the job is (see example below).

| Finding | Current Status | Risk H, M, L | Resources H, M, L | Impact to your organisation | Recommendations For remediation and For Improvement |
|---------|---|-----------------|----------------------|---|---|
| 1. | <p>Description of key finding in business terms supported by technical detail. Supporting data or greater detail may be referenced in a separate appendix where provided. Findings are listed in order of risk level. The <u>Resources</u> level is a guide to how much effort is needed to fix each issue</p> | H | M | <p>Description of the impact of our finding in terms of :</p> <ul style="list-style-type: none"> • Security of your information or systems; • Effectiveness of IT; • Cost to you. • The implications not addressing the finding are detailed. | <p>Recommendation(s) on how to fix this issue. Sufficient detail is provided for a technician to fix the issue. If more is needed that further detail is provided in a separate appendix.</p> |