Enhance your Information Security Strategy with ISO 27001:2013

Information technology - Security techniques - Information security management systems - Requirements

Expert commentary by Rob Acker, LRQA Information Security Technical Manager

The rise of cyber crime has led to a historical high in the cost of information security breaches. What can you do to ensure your organization's key information assets stay safe from cyber threats?

The promise and risks of operating in a hyperconnected world

Internet usage has more than doubled in the past decade, reaching an all-time high of 3.5 billion users in 2016, representing half the world's entire population.

Organizations of all sizes should already recognize the power of the internet as a source of information, in promoting secure digital transactions, and getting business done efficiently and effectively, just to name a few.

As always, with opportunity and innovation also comes risk - the risk of unauthorized access to key information systems. We have all witnessed some of the most high-profile information security breaches play out in the international media. As customers, we may have had first-hand experiences of how a breach can impact our lives and also the trust we have in those affected organizations.

Independent studies show cyber security breaches are a matter of 'when', not 'if'

Ernst & Young's 2016 Global Information Security Survey found that 86% of respondents said their cybersecurity function did not fully meet their organization's needs, and 48% said their outdated information security controls or architecture are a high area of vulnerability. Information security management processes are still immature, with 57% having had a recent significant cyber security incident.

While the the true cost of breaches is probably still generally under-reported, organizations tend to spend far more money responding to incidents than the worth of any data that is stolen.

According to a 2015 study from the Ponemon Institute, the cost of cyber crime on companies globally rose 19% in just one year to an average of US$9.2 million.

PricewaterhouseCoopers estimated in a 2016 Information Security Breaches Survey that the cost of restoration to normal operations post-breach consumed two to 10 man days for 60% of respondents, and 11 to 50 man days for 20% of them, despite the fact that no valuable data was stolen from these organizations.

Financial value aside, equally significant is the cost to brand reputation and the organization's capability in returning to business as usual. A global survey by ISACA, a non-profit information security association based in Singapore, found that 57% of respondents believe a concern over reputation is the single greatest challenge companies will face following a data breach.

I believe the information security management standard (ISMS) ISO 27001:2013 provides organizations with an internationally recognized framework for keeping their business-critical data safe.

> "An effective system provides protection against the known - and more importantly - unknown threats.
>
> It challenges us to look at our own vulnerabilities and ask ourselves whether we have confidence in our controls."

Rob Acker
LRQA Information Security Technical Manager

10 Steps to Cyber Security

Recognizing the specific threat that cyber attacks pose to businesses and in turn the health of the UK economy, CESG – the information assurance arm of the UK's GCHQ – issued '10 Steps to Cyber Security' in September 2012. This was then re-launched in January 2015 and advises business leaders on how they can improve cyber security to better protect their organization's information assets.

The core message of the CESG advice is the need for businesses to establish an effective information risk management regime or culture, which is supported by the board and senior managers by setting the policy which is then driven through the organization and beyond to sub-contractors and trading partners.

Crucially, top management needs to then continue to engage with the cyber risk to ensure impetus is upheld, and the necessary resource is made available to meet the threat from a dynamic risk environment.

ISO 27001:2013 and '10 Steps'

There is close alignment between the measures identified by the CESG and the ISO 27001:2013 standard. The measures and steps identified by CESG are in the realm of an ISMS.

An ISMS identifies the assets you value, for example personal or customer data, commercial or financial business information and seeks to protect them.

An organization which implements an ISMS compliant to ISO 27001:2013 has gone through the process of identifying assets, undergoing a vulnerability and threat analysis, determining the level of risk and treatment required and puts in place controls to minimize, or where possible eradicate, the vulnerability.

The '10 Steps' gives practical advice and a useful first step for companies looking to establish an ISMS.

ISO 27001:2013 can then be used by top management to be more selective in their choice and design of control measures based on the organization's appetite for risk and hence the principle of matching control to risk is then strengthened.

We have carried out an exercise comparing the identified '10 Steps' against some of the requirements within ISO 27001:2013 which are shown in the table below.

A system approach

A systematic approach to protecting key information assets is a powerful weapon in combating information risk. With the risk of cyber attack is on the rise, the risk from other sources should not be neglected either.

Breaches in data protection, data loss and fraud are all significant issues that can cause loss in service, increased costs and impact to reputation.

Assessing risk is the foundation on which an ISMS is built. It provides the focus for the implementation of security controls and makes sure they are applied where most needed and are cost effective.

The risk assessment helps to answer the question: 'How much security do we need?'

As part of the risk assessment process, an organization will not only identify but place a value on the information asset before determining the response strategy and the controls that should be put into place to manage those risks.

One of the strengths of ISO 27001:2013 is that it helps organizations establish a proportionate system. Risks that cannot be treated directly can be accepted (with subsequent periodic review and confirmation). Those that can be treated may already have adequate controls or may benefit from third party services (e.g., holding data in an ISO 27001 certified data center). This is the value in a management system approach.

From the available evidence, the most significant breaches occur where there are multiple factors, where people, processes and technology combine. Being too focused on specific controls will run the risk of not paying sufficient attention to the bigger picture.

The development of an ISMS compliant with ISO 27001:2013 requires an organization to take this holistic approach, giving assurance that security issues are being addressed in accordance with currently accepted best practice.

Having the management system externally scrutinized to ISO 27001:2013 by an accredited third party such as LRQA gives organizations an independent and unbiased view of the appropriateness and effectiveness of the system. Importantly, it demonstrates capability to external stakeholders and beyond.

As an ISMS technical manager, I often hear our clients talk of 'preparing for the audit'. When we certify our client's systems, we don't just give them a certificate but we ask them to commit to an ongoing relationship as part of the certification program. We visit our clients on average every six months as part of a surveillance program. This means they are regularly opening themselves up to external scrutiny. Speaking to some of our clients, I have noticed that this triggers certain behaviors that ensure they are primed, ready for the surveillance visit. The upshot is that this periodic 'challenge' keeps them in a state of preparedness.

Advice, such as that given by CESG and the CPNI can help to bring the management system theory to life, and so provide practical solutions.

An effective system provides protection against the known - and more importantly - unknown threats. It challenges us to look at our own vulnerabilities and ask ourselves whether we have confidence in our controls. In preventing the cyber criminal from logging in, let's not inadvertently allow them to walk through the door!

ISO 27001:2013 and 10 Steps

10 steps to cyber security		27001 Control/Clause	Key point
1	Home, mobile working	A.6.2	It's important to ensure that information is kept secure even when an employee is working from home, at client premises or on the move.
2	User Education & Awareness	A7.2.2	All employees and third party contractors need to be aware of key risks and how to report incidents. This can be achieved through security briefings as part of a new starter induction program which are then followed up regularly throughout their time with the company.
3	Incident Management	A.16	The ability of any organization to contain an incident and then return to business as usual as quickly as possible is vital following an information security event. ISO 27001 requires organizations to include information security within their information security continuity management process.
4	Information Risk Management Regime	6.1 & 8.2	Management sets the tone in any organization. Where top management take information security management seriously, it will help instil a risk-aware culture throughout the company. ISO 27001 is explicit in requiring top management to give their support and clear direction.
5	Managing User Privileges	A.9.2	Users can be a major source of information leakage and only allocating access based on role will reduce errors and support the responsibilities incumbent on the user to ensure they follow good security practices.
6	Removable Media Controls	A.8.3.1	With the rise in availability of memory sticks and other portable devices, it is critical for organizations to have procedures in place for managing their use but we should not overlook wider issues such as ensuring safe disposal of media.
7	Monitoring	A.12.7, A.12.4	Keeping an eye out for unexpected activity makes good business sense. Audit logging of user activities gives valuable evidence in the event of a breach and can help in any future investigation.
8	Secure Configuration	A.12.1.2, A.14.2.2, A.14.2.3 A.14.2.4 & 8.1	Understanding your systems and controlling changes to them helps to maintain their integrity and ensure that they are appropriately protected
9	Malware Protection	A12.2	Ensuring your systems are patched up to date will reduce the potential for malicious or mobile code to exploit known vulnerabilities
10	Network Security	A13.1	Knowing and controlling who has network access and what it is used for reduces the potential for unauthorized access by individuals or devices.

A version of this article first appeared in the British Computer Society (BCS) Enhance your IT Strategy Twenty: 13' publication.

Better safe than sorry

Information is one of the most valuable and business-critical assets for any organization. In today's hyperconnected world, organizations are exposed to large scale information security threats and destructive cyber-attacks, regardless of size, industry, or geographical location.

When information security systems are not properly managed and maintained, organizations run the risk of sustaining serious financial and reputational losses.

Ensuring your organization has the right controls in place to reduce the risk of serious data security threats and avoid any system weaknesses from being exploited is no longer an option.

This is especially so since the publication of the EU General Data Protection Regulation, which places more stringent requirements and harsher fines and penalties on organizations in the event of data breaches.

Our expertise

LRQA has been at the forefront of standards development and involved in information security management system (ISMS) assessment and certification for many years.

Our roster of high-profile clients in the finance, telecommunications, software, internet, consultancy, justice and government sectors, trust LRQA to deliver high quality, consistent and impartial assessments with the full back-up of a highly dedicated support package.

Our assessors are management systems experts qualified in information security and other aspects of IT, whose objective view will give you confidence in your own security measures as judged against best industry practice.

About us

LRQA is a recognized, world leading professional assurance services organization. We specialize in management systems compliance and expert advice across a broad spectrum of standards, schemes and business improvement services including customized training and assurance programs.

We are recognized by almost 50 accreditation bodies and deliver our services to clients in more than 120 countries.

Our unique assessment methodology takes your management systems from compliance to performance, in order to reduce business risk, and enhance the effectiveness, efficiency, and continuous improvement of your management systems.

LRQA's unique assessment methodology helps you manage your systems and risks to improve and protect the current and future performance of your organization.

Lloyd's Register
LRQA

Improving performance,
reducing risk

Our Information Security Assessment and Training Services

We provide a range of online and face-to-face assessment services suitable for organizations of all sizes and locations, and can help you make the most of the standards.

Training

LRQA's range of custom and packaged training services helps organizations at any stage of their ISMS.

Our range of training courses include:

- **Introduction to ISO 27001:2013**
- **ISO 27001:2013 Implementation**
- **ISO 27001:2013 Internal Auditor, Lead Auditor, Lead Auditor Conversion**

Gap Analysis

This assessor-delivered activity offers the opportunity to focus on critical, high-risk or weak areas of your system in order to create a certifiable system. It can also look at how existing management systems or procedures can be used within your chosen standard.

Whether you are in the early stages of implementing your management system or looking to go for a 'dry run' before the assessment visit, the scope of the gap analysis can be decided with your business development manager or assessor and gives you flexibility in choosing the visit scope and duration.

Certification

This is typically a two-stage process consisting of a system appraisal and an initial assessment, the duration of which is dependent on the size and nature of your organization.

Your business development manager will design a solution to meet your specific needs while our assessors will be open, helpful and take a practical approach. This is one of the many ways we add value to the assessment process.

Surveillance

Once we've approved your ISMS, we carry out regular surveillance visits where we check its ongoing effectiveness. This gives you, and your top management, the assurance the management systems are on track and continually improving.

Integrated management system assessment

Companies looking to combine their management system with an existing management system (such as quality) can benefit from a co-ordinated assessment and surveillance program. This service is continually being developed.

To find out more about how LRQA can help you with your requirements, visit **www.lrqausa.com,** email **inquiries-usa@lrqa.com** or call **866 971 5772**

Follow us:

www.lrqausa.com

Lloyd's Register Quality Assurance Inc. 1330 Enclave Parkway, Suite 200, Houston, Texas, 77077
Lloyd's Register and variants of it are trading names of Lloyd's Register Group Limited, its subsidiaries and affiliates. Lloyd's Register Quality Assurance, Inc. is a Delaware USA corporation.

Care is taken to ensure that all information provided is accurate and up to date. However, Lloyd's Register accepts no responsibility for inaccuracies in, or changes to, information.