How small and medium-sized enterprises can formulate an information security management system
Cyber security is just as important for small businesses as it is for big corporations. The UK Federation of Small Businesses has called for practical guides that use clear, non-technical language to help small and medium-sized enterprises mitigate the risks of cyber attacks.

This brochure aims to do just that. It is a simplified, structured approach to assessing risk and examining appropriate measures so SMEs can frame a system that fits their budget. It is based on the Gordas/Price Royal Holloway Information Security Thesis Series | Information security for SMEs ‘How small organisations can formulate an information security management system’.

CLARUS has chosen this paper as an practical example for SMEs, demonstrating its expertise in addressing cloud security challenges. CLARUS is focused on enhancing trust in cloud computing services by developing a secure framework for the storage and processing of data outsourced to the cloud through a 3-year research and innovation action. CLARUS will allow end users to monitor, audit and control the stored data without impairing the functionality and cost-saving benefits of cloud services.

As seen in

ComputerWeekly.com
Implementing information security management systems in SMEs and ensuring their effective governance

As a small and medium enterprise (SME), you belong to a special category of organisation that requires protection of business information. Your risk profile and big corporations is now becoming more similar to big corporations. You both use technology extensively and would face serious consequences in the event of a data breach. Budget restrictions, limited resources or limited information security expertise probably make it hard to set up an effective and efficient information security control environment.

What’s more, most of the available security standards and guidance are not built with sufficient usability in mind or tailored to an SME’s level of expertise. Now is the time to get savvy when it comes to implementing even basic information security controls. This means you also need to change your perceptions of security and take advantage of being small and agile, which will help you mitigate the risks you face.

Now is the time to make information security a top priority and accept the costs associated with its assurance because the cost of measures can be much lower than the penalties suffered if an incident happens. Improving your cyber security is an opportunity to gain a competitive advantage, improve customer service and boost reputations by demonstrating that you have taken steps to defend against attacks.

An integrated solution for your information security is the only viable option for SMEs

The simplified implementation approach for an information security management system (ISMS) for SMEs proposed by Gordas and Price will help you make information security a priority. It is based on extensive research, gap analysis and the authors’ experiences in ISMS. It involves the evolution of functional management systems through three maturity levels, and a new high-level risk assessment methodology that allows organisations to eliminate weaknesses in their security arrangements.
through a risk assessment and a control selection exercise that would take no more than a day.

What you need to do to make information security a top priority

» A risk management framework tailored to your requirements, not those of big corporations.
» A new approach for implementing an ISMS based on their maturity level, the highest being a full scope ISO/IEC 27001 ISMS.
» An information security governance approach for SMEs.
A coherent framework for risk management in SMEs

Simple strategy for information risk management – to be repeated annually

» Establish the context.
» Assess the risk.
» Select the information security controls.
» Implement missing control measures.
» Monitor and evaluate the effectiveness of information security risk management.

Information risk management is a challenging task across enterprises of all sizes. However, as an SME you are more special because you need a simple, practical and coherent approach that would allow you to be effective and efficient in risk assessment and risk management. Gordas and Price propose a simple strategy for information risk management, inspired by the Plan-Do-Check-Act (PDCA) method. Each step produces results used as input data for the next step. The process is iterative and should be repeated at least annually, or when major information systems or business process changes occur.

The goal of risk assessment is to identify top risks and to provide top managers and other stakeholders with the information required to make informed risk mitigation decisions. Most organisations are only able to treat five to 10 information risks per year. The risks that are not mitigated will be kept on hold and re-evaluated the following year, when they may become top priorities or have a smaller impact due to implemented safeguards.

Let’s look at the first three steps in more detail

1. Establish the context

Context establishment is an essential step for any risk management
methodology, as it should define the scope, boundaries and purpose of the information security risk management.

2. Assess the risk

The goal of this step is to determine the threats and vulnerabilities that increase the likelihood of an information security incident. Gordas and Price recommend applying an information-centric approach that requires just an inventory of critical information assets. This is better than an asset-centric approach that entails a detailed IT components inventory.

*The best solution for an SME is a concentration on critical information flaws and business process.*

This step is broken down into several smaller steps.

**Threat assessment**

Information types in organisations may have significantly different requirements for information security in terms of confidentiality, integrity and availability (CIA).

For most SMEs, the most relevant threats are typically **malware, hacking, operational errors**, and **physical** and **environmental threats**. The assessment team should agree the overall threat rating for each of these high-level threats, taking into account information characteristics that may be affected (CIA).

*The outcome of this step: overall threat rating* for the information flows in the organisation.

**Vulnerability assessment**

In the vulnerability assessment step, management should determine the degree to which organisational information flows are vulnerable to high-level threats. The high-level threat types are transferred from the threat assessment. This does not require a detailed vulnerabilities list.
The outcome of this step is: overall vulnerability rating of the information flows in an organisation.

Overall risk likelihood
The likelihood of an incident occurring is a determinant factor for the extent of control measures that should be implemented for an adequate level of protection. It is determined using the overall threat rating and overall vulnerability rating mentioned above.

Overall information risk rating
The outcome of assessing the risk is the overall information risk rating.

This is determined by the assessment team using the business security requirements rating from the context establishment phase together with the likelihood ratings from the overall risk likelihood phase.

This output is used in the control selection phase to determine the next steps needed to secure the system.

3. Information security control selection


The risk assessment team selects the organisation’s risk profile (low, medium or high) from the overall information risk rating. If the rating is low, then implementation of Priority one controls from the control database is recommended; if the rating is medium, the organisation should implement controls with Priority one and Priority two; and for a high-risk organisation, implementation of all controls is recommended (Priority one, Priority two and Priority three controls).

Neither the controls database nor the information security risk rating are static because threats, vulnerabilities, likelihood, consequences and options
for treatment are changing and should be reviewed regularly. Nevertheless, Priority one controls represent the minimum control baseline that should be implemented by all organisations.

PRIORITY ONE

» Mandatory organisation controls.
» Internal audit.
» Management review of the ISMS.
» Mandatory information security controls.
» Information risk management.
» Management responsibility and commitment to data security.
» Information security policy.
» Roles and responsibilities.
» User education and awareness.
» Managing user privileges.
» Malware protection.
» Physical protection.
» Business continuity and disaster recovery.

PRIORITY TWO

» Initial to intermediate information security controls.
» Acceptable usage policies.
» Home and mobile networking.
» Incident management.
» Removable media controls.
» Patch management.
» Secure configuration.
» Network security.
» Security education/training.
PRIORITY THREE

- Intermediate information security controls.
- Sensitive physical information.
- Sensitive physical information.
- Computer/network installations.
- Cryptographic solutions.
- Intrusion prevention systems.
- Malware awareness.
- Security event logging.
- Environmental protection of critical IT facilities.
- Power protection of critical IT facilities.
- Data loss prevention tools and processes.
- Security governance and management.
- Optimised information security controls.
- Continuous improvement process.

Why implementing a set of security measures alone is not enough
As an SME, you need an approach that fits your resources, level of expertise and specific requirements. You should take into account also the speed with which process re-engineering may be performed in your company while still supporting your business operation.

Only a proper management system can ensure adequate and effective information security. This should include organisational policies, structure, planning activities, responsibilities, practices, procedures, processes and resources as specified by ISO/IEC 27001.

As an SME, you are advised to establish information security control priorities that could be implemented in a tiered model, taking into account their internal controls maturity level and the threat landscape.

The approach should be compatible with ISO/IEC 27001 requirements and enable smooth transition to a certifiable ISMS.
Who should be involved
It is very important to ensure the participation of all employees, starting by securing the support and commitment of management. The understanding and involvement of all stakeholders is essential, not only during maintenance and operation, but also in the implementation phase.
Three-phase ISMS evolution

Gordas and Price propose a three-phase approach that takes into account the evolution of functional management systems to different levels of maturity. The approach can be adapted to suit SMEs’ individual requirements.

*SMEs are recommended to perform a GAP assessment first, to see which controls are already in place and whether they are effective. Prioritisation of implemented information security controls can enable an organisation to concentrate efficiently on its critical business processes, applications and information flows.*

**Phase 1:** An ISMS with reduced maturity level, partially compliant with ISO/IEC 27001. The controls for this phase are those with implementation priorities one and two from the high-level controls database.

**Phase 2:** An ISMS with intermediate maturity level, partially compliant with ISO/IEC 27001. The controls for this phase are those with implementation priorities one, two and three from the high-level controls database (see page 5).

**Phase 3:** An ISO/IEC 27001 ISMS, fully compliant with standard requirements. The controls for this phase are all those in ISO/IEC 27001 Annex A.

Gordas and Price consider that the management part of ISO/IEC 27001 (plan-do-check-act core requirements) should be implemented for all organisations.

**Continuous improvement approach**

The approach emphasises the importance of continual improvement, and the implementation approach is designed to provide a smooth transition between the different maturity levels.

A formal continual improvement process may be defined at phase two, as some degree of comfort is offered by the risk management process which is implemented in the first phase.
SMEs are recommended to ensure continuous improvement in information security throughout the organisation by performing the following activities:

» Perform regular internal audits and management reviews. The results should provide a clear direction for improvement and keep the ISMS effective.
» Monitor information security incidents, react to them promptly and establish a resolution knowledge base.
» Address information security aspects as part of the business planning processes.
» Take appropriate corrective and preventive measures.

The implementation of a continual improvement management process in SMEs is of major importance because most SMEs will not be able to implement all the required information security controls due to resource constraints. As a consequence, the only way to mitigate the impact of missing controls is by performing appropriate information security monitoring and incident review.

**A tailored approach for SMEs**

SMEs are exposed to similar threats to large corporations

An effective and efficient risk management approach is essential for SMEs’ success

In SMEs, establishing a risk management programme should become a board-level priority and all relevant business functions should be involved.

A simplified risk management approach can help SMEs make information security a top priority while suiting their budget restrictions, limited resources and limited information security expertise.
ISO/IEC 27005 provides a risk management process, but to implement it in an SME, a risk assessment methodology should be provided.

- This should yield results in days rather than the usual months taken by large enterprises.

- The Gordas and Price risk management framework enables organisations to perform a high-level, information-centric risk assessment, supported by an information security controls database mapped to the organisation’s overall risk profile.

- This permits organisations to perform a proper risk assessment in the context of business risks and provides accurate information about the top information security risks. This is essential for an effective risk treatment programme.

- Being compatible with ISO/IEC 27001, it permits the organisation to use all the ISO/IEC 27000 series guidelines, thereby playing a much more constructive role in its security by contributing to its business success.

As an SME, you can now also apply your agility to information security readiness for sustainable success. This is also an opportunity for information security practitioners to play a much more constructive role in the enterprise and show they are doing a good job by contributing to business success.
About the authors

Vadim Gordas is an information security professional with information security compliance, governance, risk management, IT audit and infrastructure security experience in the finance, insurance and banking sectors. He is currently information security manager for StatPro, responsible for development and consistent implementation of the group information security framework.

Geraint Price is a lecturer in information security at Royal Holloway. His research interests include public key infrastructures, cyber security and the human aspects of secure systems design.

The Royal Holloway is a partner of CLARUS, a European initiative that is building trust in cloud services by putting the focus on user concerns, enabling them to monitor, audit and control their stored data while gaining the benefits of cloud computing.

CLARUS is funded under Horizon 2020, DG CONNECT of the European Commission