Adaptive SME security

Information security guidance for Small to Medium Enterprises

A collaborative project by the ISO27k Forum | v1 | July 2024

Contents

Executive summary

This guideline describes a pragmatic, five-phased approach for Small to Medium-sized Enterprises to manage their information risk and security arrangements.

The flexible, generic approach is readily adapted for any type of SME such as small commercial organisations, family businesses, charities, clubs, societies and groups, plus tiny owner-operator sole-proprietor self-employed micro-organisations. It can grow with, and support the growth of, SMEs.

Whereas most other information security standards and advisories address relatively large, mature organisations, we have focused on SMEs, tiny ones particularly, addressing our security and resourcing challenges and relative immaturity. Established approaches for information or cyber security such as ISO/IEC 27001 and NIST CSF can be difficult to apply and in some cases may be wholly inappropriate for little SMEs, leaving a gap this guideline seeks to address, pragmatically.

We have taken a ground-up approach, recommending basic but essential and valuable information security practices for tiny 'micro organisations' given our minimal resources, and then suggesting additional activities more appropriate for the small, medium or even larger businesses.

This is self-help guidance, practical steps that SMEs can take by ourselves. SMEs facing more significant risks or with no expertise in this area can always call on security consultants for specialist advice, a commercial decision.

In other contexts, SME can also mean Subject Matter Expert. The Authors of this guideline are SMEs who work in or for SMEs. We have 'lived experience' in this area – decades of it – but this guideline offers *generic* advice. Your situation, risks and security needs are unique. Please contact us or other competent specialists for tailored advice.

Document information

History/version control

This guideline was developed collaboratively by members of the ISO27k Forum in May-July 2024.

We'd like to thank colleagues on the ISO27k Forum and LinkeDin for insightful comments, additional references and improvement suggestions.

We'd love to hear from you too. Does this guideline help? What have we missed or got wrong? How could it be better?

Please contact the authors or raise your ideas through social media, chambers of commerce, industry forums and the like – help us develop and spread good security practices to all SMEs.

Copyright

Authors

- Gary Hinson, consultant & editor
- Aled Treharne, CTO Growthinvest
- Marappan Ramiah, consultant
- Phil Mauger, Security Manager
- Richard Regalado, consultant
- Savva Pistolas, consultant
- Shruti Kulkarni, consultant
- Tristan Roth, consultant

None of this is legal advice. Your risks and security control requirements vary. Treat this generic guidance with caution.

Introduction

About information risk and security

Every organisation, regardless of size, needs to both protect and exploit information such as financial records, customer information, intellectual property and internal communications. Protection is appropriate and necessary because information can be both valuable and vulnerable.

Information is any organisation's lifeblood. Aside from its value to the organisation, information can also be valued by its owners, or by adversaries, competitors and criminals. Information can also have negative value, for example if it is untrue, misleading, incomplete, out of date or misinterpreted, or if it reveals something that should have remained secret.

The vulnerability of information results in part from the need to make it accessible in order to exploit or realise its value. Information may also be damaged by issues such as inappropriate disclosure, loss, substitution or corruption. Events such as fires, floods, media or equipment failures, electrical interference and power cuts can occur naturally or accidentally, as well as deliberate attacks. Such threats, coupled with vulnerabilities, cause a vast number and wide variety of incidents worldwide, every day.

The impacts or consequences of incidents involving information can be crippling, possibly even terminal. They often involve some combination of:

- Plain loss of information, whether temporary or permanent, that reduces or destroys its value.
- Loss of control over information means an inability to govern or secure and perhaps exploit it.
- Financial damage includes direct costs associated with preventing, identifying and dealing with incidents, plus consequential costs relating to the security controls and incidents that still occur.
- Loss of trust or confidence arising from incidents can be a limiting factor for its owners, while reputational harm, brand devaluation and loss of custom are obvious concerns for any organisation, particularly of course where trust is an important factor (which it usually is). Customers, partners, investors, employees, the authorities and society may lose faith in an organisation that can't keep their information safe.
- Reduction of options: the need to address incidents, urgently, sucks resources from more proactive business-aligned areas, systematic improvements and strategic initiatives.
- Noncompliance penalties, fines, restrictions on future business and legal costs all add to the misery.

Strong information security helps organisations avoid the pitfalls by achieving and maintaining sufficient confidentiality, integrity and availability of information. Investing in information security is an investment in the organisation's future. It protects the vital information that fuels its success and fosters trust.

Note the need to protect all forms of information - including computer data, of course, but other forms and formats of information are also both valuable and vulnerable. Intangible ideas, knowledge, experience and expertise are subject to information risks too.

If you're interested and have the time, continue exploring information risk and security concepts in appendix A.

About SMEs

SMEs comprise the vast majority of all organisations worldwide - more than 99% by some accounts. SMEs are like plankton - tiny, largely unrecognised and yet absolutely crucial to the survival of fish and whales. **The entire global economic system rests on SME foundations and hence depends on SME security.**

SMEs are surrounded by sharks and whales - a hostile and threatening business environment. Our simplicity, focus and nimbleness give us the edge to survive. This guideline, written by SME security experts for the global SME community, further harnesses the power of numbers. Working together, we can make a difference.

SME challenges

SMEs face an uphill battle when it comes to information security. Unlike larger organisations, we clearly have limited resources. Financial constraints, smaller or non-existent IT teams and a lack of expertise can make it difficult for SMEs to implement robust security measures. Segregation of duties, for instance, is difficult, costly or practically impossible for the tiniest of SMEs. Greater reliance on third-parties for security tools, services and advice can create additional vulnerabilities if the suppliers are themselves insecure or incompetent, offering bad advice.

Greenfield startups are typically SMEs with strong growth plans. Even at this early stage, they often have valuable intellectual property and a risk-seeking culture - potentially a fiery combination. Integrating lightweight (adaptive) information risk and security management practices into the organisation from the outset pays dividends later on, whether the venture flourishes or founders.

The daily pressures of running a small business can further complicate matters. Balancing security with other pressing needs is a constant struggle for SMEs. Strategic decisions are generally made by one person or a small, close-knit group, leading to security blind spots if there is inadequate risk awareness and unrealistic expectations.

Compounding this challenge is the fact that many SMEs don't understand the threats we face or the potential consequences of security incidents. Some of us mistakenly believe we are too small to be targets, or that relying on commercial cloud services guarantees complete security. Such naïve assumptions and wishful thinking leave us vulnerable.

> *"Some organisations feel that because they are relatively small or don't hold substantial amounts of sensitive consumer data, such as credit card numbers or medical information, they are unlikely to be the victims of a cyberattack. The reality is that any organisation that connects to the internet and conducts business activities online, should be mindful of how they manage cyber security risks."*
>
> Cyber risk - a practical guide,
> Institute of Directors, NZ

SMEs with limited security expertise can be misled by inaccurate or incomplete information about the threats. Failing to keep pace with the constantly-evolving tactics of cybercriminals makes us ill-prepared.

The perceived high cost of security solutions can also deter SMEs from investing in necessary safeguards, despite the long-term financial and reputational damage that incidents can cause. Coupled with the perception that SMEs have poor defences and are thus soft targets, we may be even more likely to be attacked.

While internet dependence certainly isn't unique to SMEs, it's worth noting that our heavy reliance on online information, cloud services and marketing can further amplify the vulnerabilities for many of us and our supply chains. We're riding the tides with hungry fish, sharks and whales, remember, doing our best to avoid the rocks and storms.

SME opportunities

SMEs are a vital force in the global economy. Our small size gives us distinct advantages that fuel our success and competitiveness. Unlike large corporations, SMEs have simpler organisational structures, allowing us to make decisions faster. This agility lets us react quickly to changes in the market and customer needs, provided we spot them. Without being bogged-down by bureaucracy or lengthy internal discussions, SMEs can seize fleeting opportunities and capitalise on new trends and business openings more quickly.

Furthermore, the small size of SMEs means a sharper focus. With fewer departments and a smaller team, everyone in an SME is more likely to appreciate, share and support the organisation's key goals. A unified approach and intolerance for disruptive or counterproductive activities leads to streamlined operations and improved overall effectiveness. We must all pull our weight.

The inherent agility of SMEs is a catalyst for innovation. Faster decision-making allows rapid implementation of new ideas, and experimentation. The ability to gather feedback quickly and iterate on those ideas enables us to develop groundbreaking solutions and cultivate a culture of continuous improvement. The capacity for innovation positions proactive SMEs as potential disruptors within our industries and markets.

However, we should acknowledge a potential drawback associated with the tight management structure of SMEs. The level of management support for a particular project (such as an information security initiative) can significantly impact its success. Because the organisation is smaller, management's stance on a project is often clear-cut – we are either strongly behind it or not interested at all. While decisive leadership can be an advantage, it also presents a vulnerability. If a key supporter leaves or priorities shift, the whole initiative could be derailed, put on hold or canned. Making sensible strategic decisions is never easy, and there is always a risk of following fads and fashions, particularly in IT, regardless of the security implications.

Objectives of this guideline

This concise guideline empowers SMEs in information security, elevating overall security, resilience and compliance. Stakeholders, from owners to customers, gain the knowledge to safeguard their interests and the organisation's reputation. The guideline streamlines compliance with legal and contractual obligations, while advocating for practical and budget-conscious security solutions well-suited to the SME context. Furthermore, it encourages the adoption of established good security practices, particularly the systematic risk-led approach championed 3 decades ago by Shell, which has proven so effective in managing information security risks. By streamlining, adapting and adopting the lessons from larger organisations, SMEs can play to our strengths, significantly strengthening our security posture and prospects.

Being buffeted and bullied by others, an inevitable consequence of being small, is something we are conscious of in writing this guideline: our aim is to inform, inspire and encourage SMEs, rather than cranking up the pressure.

This guideline offers SMEs a *generic* framework with an adaptive approach.

It is expressly designed to suit a wide variety of SMEs, so please interpret and *adapt* it according to your specific context, size, industry, regulations, objectives, needs, resources, technologies, maturity, risks, threats ...

The clue is in the name.

Intended audiences

To offer appropriate, pragmatic guidance, we envisaged three SMEs of different sizes, locations, industries and security maturity, with the following three mythical readers in mind …

Micro organisation

Just a handful of people, from 1 to ~10 employees

"Anne is a mid-20s solo entrepreneur. After studying for her engineering degree, Anne started her professional career as an intern for an engineering company before spotting an opening for roving geotechnical engineering support for the local construction industry. Soon after setting up a company, website and social media presence, she found herself travelling further afield from client-to-client, working from hotels and vehicles using cloud services. Anne found it beneficial to collaborate with other colleagues when bidding for work, but after losing out on a contract to a consultant that she had invited to comment, she had become more cautious about sharing sensitive details of her bids. Just last week, a major potential client sent Anne a supplier security questionnaire concerning her cybersecurity arrangements for the engineering and architectural information on a prestigious city centre block. The construction firm needed a prompt response to pass up to the group and their insurer, so Anne risks losing the tender if she can't respond positively and quickly. This prompted Anne to work on cybersecurity as an urgent commercial imperative …"

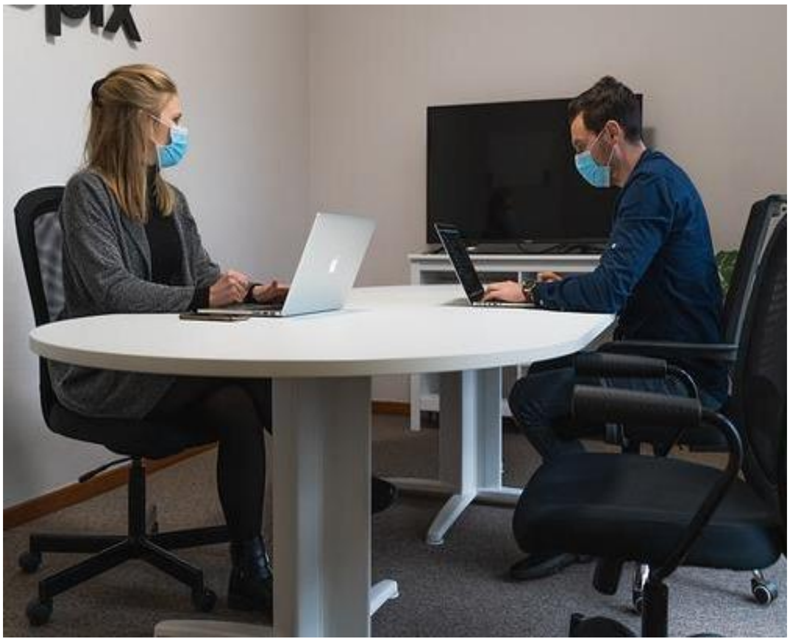
Small organisation

up to ~50 employees

"Anil is part of the management team for a small office services organisation that is primarily composed of office workers, mostly doing bookkeeping/accountancy and HR support for clients. Employees are provided with company laptops that they use occasionally in the office but generally at home or with clients to complete their project-based workloads. There is no corporate IT function since IT hardware, software and cloud services are provided and managed by an IT support company. The IT company does not get involved in IT or security strategy, which Anil feels leaves a gap that needs to be filled, especially as customers increasingly expect better support on security matters and competitors are making inroads. …"

Medium-sized organisation

up to ~250 employees

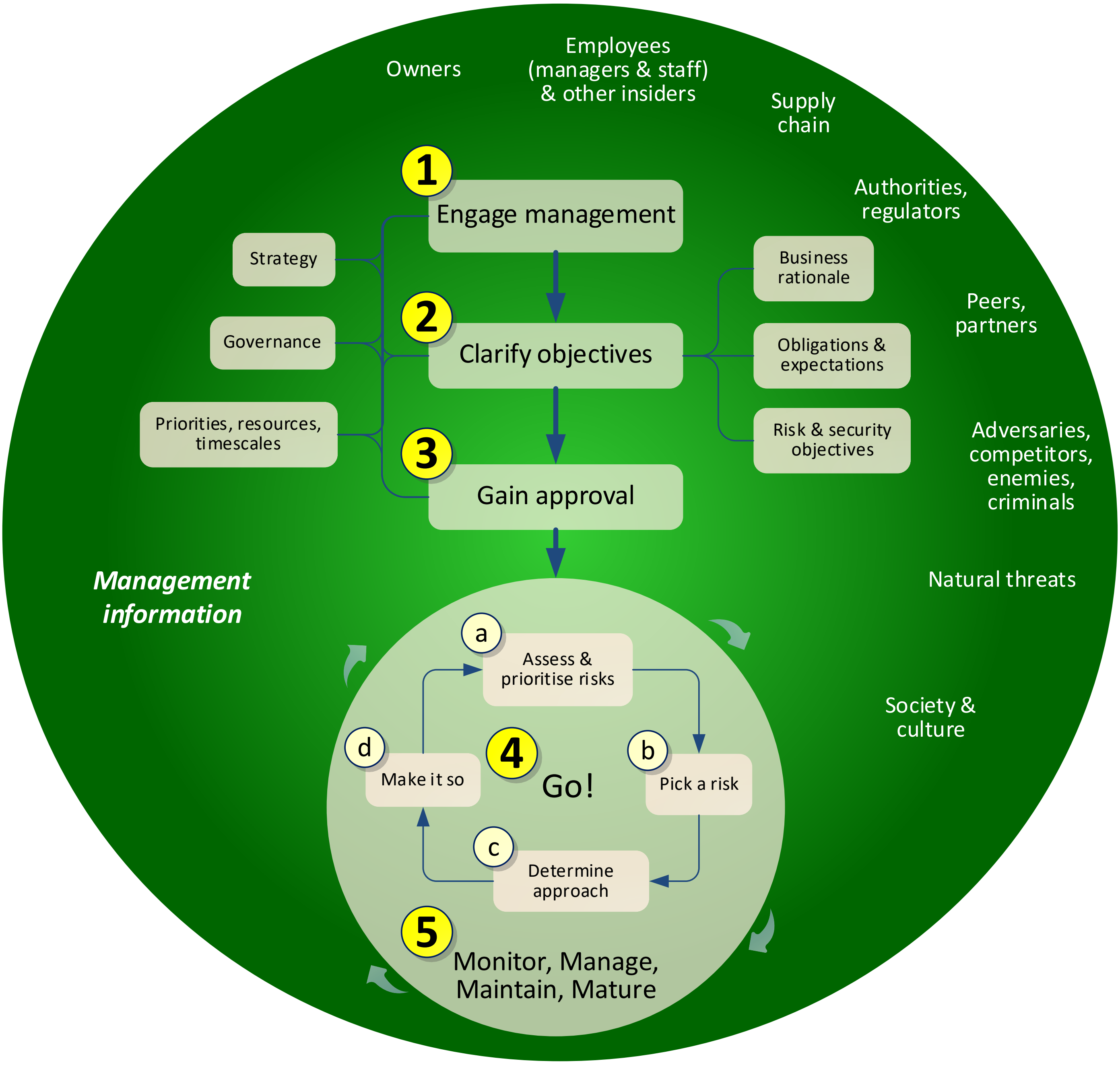


"Alison and Andy work for a marketing function attached to a heavy machinery manufacturer. The manufacturer's production facility is based in the Far East, while the marketing team is based in Paris, serving the bulk of its European, North American and Middle Eastern customers, plus some other customers that it has acquired independently. Andy runs the company website including the ordering and customer services portal. Alison is nominally the Head of IT, leading a small team with some contractors and consultants for specific areas or projects. A substantial part of her job is reconciling competing demands and priorities from group HQ and her peers on the Senior Leadership Team, plus leading the IT function. Andy has been asking for more help on cybersecurity lately following a couple of incidents. He and Alison are increasingly concerned about the possibility of ransomware and social engineering attacks, while the CEO expects IT to be 'doing' privacy …"

Even organisations with *more* than 250 employees are very welcome to consider and adopt the adaptive approach, or pick-and-choose whichever aspects best suit their requirements. This guide wasn't exactly written for you but you're not excluded. The same charge applies.

Adaptive SME approach

The adaptive approach was designed for SMEs as a simplified, slimmed-down version of that described in security management standards such as ISO/IEC 27001 and NIST CSF:



Phases ① to ③ involve getting management on-board, elaborating on the objectives, designing the approach and securing the resources needed for the work ahead. They could be combined … but we feel it is worth considering them separately, given their importance and value. In our experience, organisations that dive headlong into phase ④ (typically in a rush to become certified) risk alienating senior management and failing to achieve the business value necessary to *sustain* the approach over the long term. The effort invested into phases ① to ③ pays off later, making this a key part of the adaptive SME approach. Remember: **On your marks ➔ Get set ➔ *Go!***

Develop a vision of the future as a way to communicate the changes ahead and more importantly their outcomes and value to the organisation, convincing stakeholders and colleagues to support the efforts required. Before getting into the details, consider what are we protecting, against what and why? What matters most/least? What are the priorities?

Here are some prompts to get you started, reflecting different sizes of SME:

Micro	Small	Medium
Outline high-level goals: why is information risk of concern to the organisation? Focus! What *must* be done?	◀ That plus … Elaborate on and clarify those goals: who needs to work on what, by when and most of all why? What *should* be done?	◀◀ That plus … Link information risk and security objectives to business strategy, providing options for senior management to consider. What else *can* usefully be done?
Set aside a little of your valuable time to work on information risk and security	Intrigue and involve relevant managers	Engage relevant managers, specialists and advisors
Start sketching or writing down aspects that are working OK *vs* those that need improvement	Review any existing risk and security documentation for suitability and quality	Map out and compare risk and security documentation relative to other areas of the business

Deliverables from phase ①

Some signal of management engagement, interest and support – the green light to press ahead.

Phase ② - clarify objectives

Since every organisation is unique, so are its information risk and security challenges. Even adjacent shoe shops on the very same high street probably have different suppliers, products, pricing, customers, priorities, owners, financing, employees, histories and strategies: sure, they both have valuable data relating to shoes, and they are both in the same retail industry segment, but scratching beneath the surface reveals plenty of differences.

The risks and hence security requirements depend on the information *e.g.* if a micro-organisation is in the business of handling rental agreements, they would obviously need to secure personal information received from customers, plus sensitive commercial and financial information concerning the agreements (contracts). Perhaps less obviously, they also hold personal information concerning employees, business contacts, former and prospective customers and more, while information about their own business situation is probably commercially confidential. Broadening the perspective to take in requirements for information integrity (*e.g.* accuracy) and availability (*e.g.* retaining historical records) extends the analysis of what's important, what are the priorities for the business.

Aside from the key/primary goals, it is worth teasing out and elaborating on other less obvious/secondary objectives. Information security can enable or support the achievement of various strategic business objectives such as to:

- Be a trustworthy and trusted, reliable supplier/partner.
- Be an attractive employer, nurturing and growing worker capabilities.
- Be a valuable customer, sharing an interest in a supplier's business.
- Be competitive, a leader in the field, a shining example, a beacon of success.
- Be socially, ethically and ecologically responsible.
- Be sufficiently strong to cope with the inevitable setbacks.
- Facilitate innovation, making good use of creativity.
- Grow organically or by acquisition and thrive in the long term.
- Protect and exploit information, creating, adding and locking-in value.
- Provide top-quality, reliable, trustworthy, valuable goods and services, including customer care and support.
- Return a healthy profit, optimising use of available assets.
- Use security as a business enabler …

Security maturity objectives involve developing or enhancing valuable corporate capabilities, such as resilience – workers being able and willing to deal effectively with *whatever* occurs.

It is important to remain business-focused in this phase, emphasising the value of adaptive information security as a business-enabler (cost-effective security enables business activities that would otherwise be too risky) as well as a defensive/survival and compliance mechanism.

As part of this phase, discuss with management the question of who is, or should be held, **personally accountable** for securing information. Larger organisations typically nominate managers as 'owners' of various information assets *e.g.* the HR director may 'own' the HR system and its database of personal information used throughout the company. They have the ability to make strategic decisions including the allocation or withholding of corporate resources necessary to protect their assets against unacceptable risks while exploiting them legitimately for business advantage – and, yes, risk acceptance is ultimately their choice, albeit on advice from colleagues and specialists. A simpler approach may work for SMEs, starting with awareness and appreciation of the true meaning of Accountability as opposed to **responsibility**, and the need to reduce illegitimate exploitation of information without unduly preventing legitimate exploitation for business purposes.

Consider who is or should be **responsible** for information security *e.g.* who is operating and managing the information security processes, activities, Example risk registers *etc.* under direction and leadership of the accountable person or people. Note that although responsibility may be delegated to others, accountability for delegating remains firmly with the accountable party: regardless of whether the arrangement works well or fails dismally, they made the delegation and resource allocation decisions, and may be called to account for that. It is 'sticky'.

Bring information risk under management control, increasing confidence and reducing unplanned, unexpected and often nasty surprises … while also facilitating greater exploitation of information for business purposes…

Consider how much risk the organisation is (a) willing and (b) able to take, and why. What are the factors driving this - customer expectations? Compliance obligations? Technological choices or business situations?

Consider information risk in relation to other forms of risk (strategic, commercial, financial, compliance *etc.*). Be realistic about the need to survive severe incidents and disasters, whatever their cause.

Satisfy obligations under applicable laws, regulations, contracts *etc.* Consider discretionary/optional requirements or objectives - ways in which information security, privacy, governance, risk management and compliance support or enable the organisation to achieve its business objectives:

- Explore other alternative or complementary approaches and guidance *e.g.* ISO/IEC 27003, NIST CSF, CyberEssentials (see appendix B).
- Consider possible information risk and security governance arrangements *e.g.* keeping it entirely in-house or seeking external assistance, perhaps even sign-up for a managed commercial service or online tool.
- Protect all forms of information, not just digital data and IT systems (see step ⓐ).
- Maintain contact details for support systems and services such as the police, fire service, electricity and telecoms suppliers, your national CERT, any information governance bodies and compliance authorities such as the Tax Department or Information Commissioner's Office.

> *"The first thing an organization must do when implementing a cybersecurity framework is to 'know your environment.' An organization must know what assets (hardware and software) are on its network. They must also identify the data on the enterprise that they are obligated to protect. After doing this, to minimize their attack surface, an organization can prioritize the application of security controls to assets based on where high-value data resides."*
>
> *A Guide to Defining Reasonable Cybersecurity*
> *CIS 2024*

Find, join and participate in local small business groups, chambers of commerce, industry forums, national or international organisations (such as ISSA, (ISC)^2, ISACA, CIS and the Institute of Directors), online communities (such as the ISO27k Forum) and social media (such as LinkeDin), trade delegations *etc.* to gain useful information, make business contacts, sound-out issues and ideas, and generally pull together on information risk and security.

Deliverables from phase ②

A set of business-related information risk and security objectives, clearly described, debated, prioritised and agreed with stakeholders.

Phase ③ – seek management approval

Trust us, the build phase will be smoother and create less anxiety for all concerned following sensible planning. A well-defined strategy for the build activities to follow in phase ④ - essentially a programme to implement good practice information security - will help enormously if there are lots of things to do and several people or teams involved, or for that matter if it is entirely down to you but you are already busy running the business.

Aside from information risk and security, there are inevitably other business priorities and competing demands. A balanced approach is necessary. However, do not lose sight of the scary possibility that a ransomware attack or physical disaster such as an office fire could happen at any moment. Addressing security alongside other needs requires a realistic assessment of the situation, the requirements and the potential consequences of inaction. In short, time is of the essence.

So, squeeze the most benefit from your organisation's investment in information security by **tackling your biggest information risks first**.

Start by considering the broad business, cultural and technological **contexts** within which information risks are to be managed e.g. the relative priorities of various ongoing commitments and initiatives. Develop an overall **strategy** and/or **implementation plan** outlining major elements to come in phase 4. Clarify the **scope** *e.g.* which business functions, information systems or functions are included/excluded.

Clearly articulate and build upon the **objectives** previously defined. Define key metrics to measure, drive and demonstrate achievement of the objectives at the programme level.

Keep **management** informed and actively engaged (in-the-loop) throughout. Include management checkpoints at key points in the programme to review progress, address issues and re-plan as necessary.

Establish suitable **governance** arrangements, determining who makes key decisions, and how plans, progress, metrics and issues are reported. This is important for accountability – not just for the build in phase ④ but as the basis for the operational risk and security arrangements in phase ⑤ once the build is complete.

Be honest about the amount of work that can realistically be achieved with the resources and time available, given competing priorities. Be sensible about management's engagement and time needed for important decisions, reviews, progress meetings, risk workshops *etc.* They still have a business to run! Can you focus their involvement and provide better quality information to smooth the way?

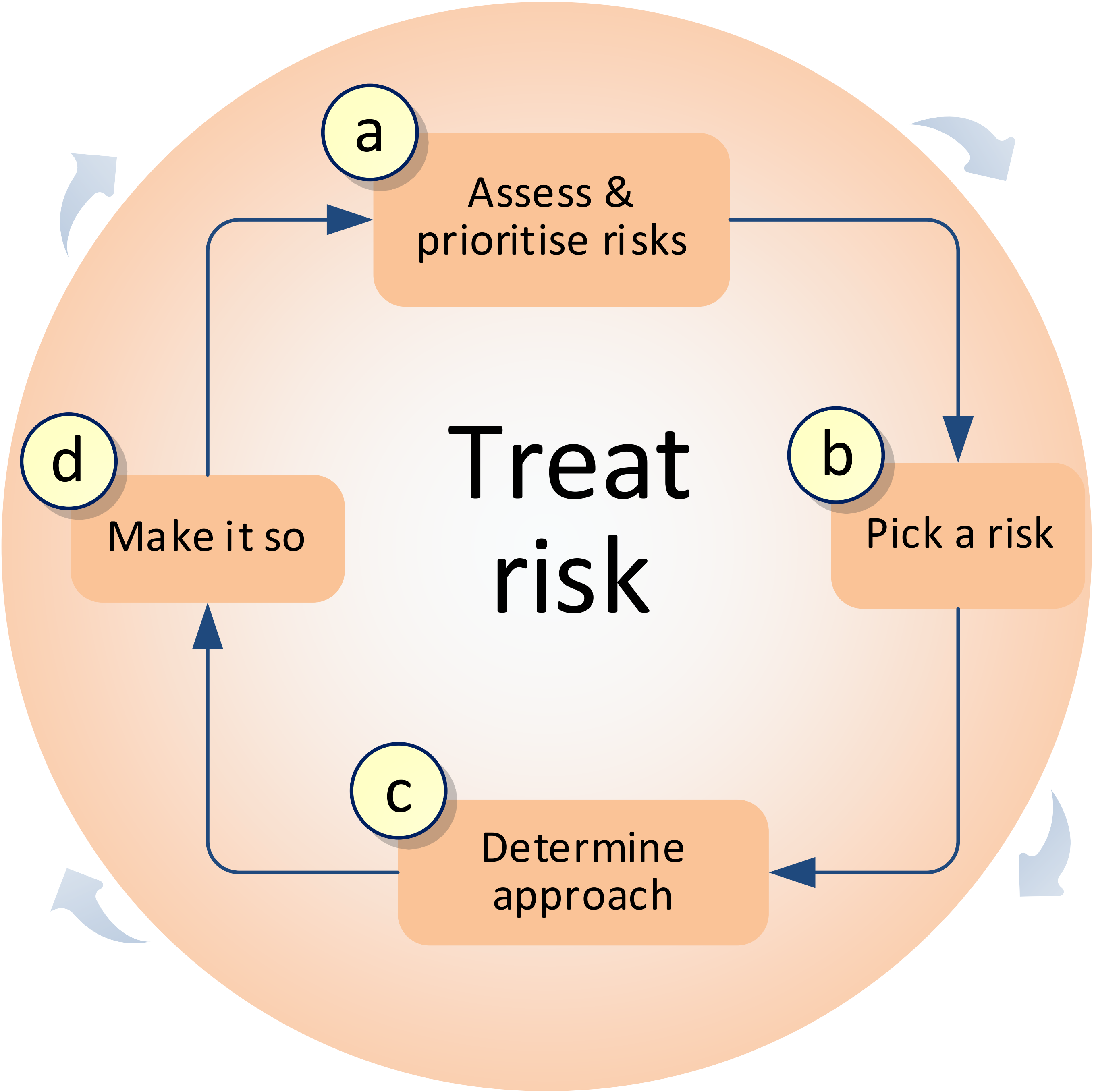
Resourcing is clearly vital for the remaining work, so quantify and secure the required resources - people, technology and finance. If resources are over-stretched, adjust the programme accordingly and iterate, discussing changes with management given the strategies, objectives, priorities, resources *etc.* The aim is to tease out any concerns or issues, negotiating to a position that is realistic, achievable and acceptable to the stakeholders, particularly management and the implementors. Acknowledge the risks associated with the programme, such as the likelihood of problems, changes and constraints within the individual projects and overall. *Insist* on **flexibility** to deal with whatever comes up, with sufficient **contingency** in proportion to the risks.

Deliverables from phase ③

An approved project plan showing steps and checkpoints, timescales and resources allocated by management. The key accountabilities and responsibilities relating to information risk and security should be documented and understood, at least in outline *e.g.* in the form of specified roles or job descriptions, reporting lines *etc.*

Phase ④ – go!

This phase of the adaptive SME security approach initiates the core information risk treatment process – a continuous rolling cycle of these four steps, explained further below.



Each run through the cycle deals with a significant information risk – typically the most important, urgent or valuable one at that point, sometimes a cluster of related risks, sometimes running several cycles in parallel.

Gradually, with practice, the cyclical process becomes more intuitive and efficient. Once fully up to speed, the cycle continues rolling indefinitely into phase ⑤, continually reviewing and fine-tuning the organisation's risk and security arrangements, responding to changes and presenting improvement opportunities.

Yes, it *adapts*.

Step ⓐ - assess and prioritise information risks

What information do we seek, want or need to protect and exploit? What information is important to the business? Think about various types or classes of information either owned by the SME or placed in our care by others, such as:

- Accumulated knowledge and know-how, experience and expertise, gut-feel.
- Biometric information such as fingerprints, voice prints, facial characteristics.
- Business reports, metrics, measures, trends, statistics …
- Communications such as emails, text messages, recorded telephone calls.
- Contact details for customers, partners, suppliers and personnel.
- Contracts, agreements, commercial arrangements and understandings.
- Customer lists, past, present and future (prospects).
- Databases and other sizeable collections of information, including paper records, backups and archives.
- Designs, diagrams *etc*. *e.g*. an architect's blueprints, network maps.
- Engineering information, bills of material, parts lists.
- Financial information.
- Goodwill, brands, reputation.
- Intellectual property.
- Internal reports, presentations, communications *etc*.
- Invoices received and sent, plus receipts, confirmations *etc*.
- Knowledge, expertise, business know-how.
- Medical information.
- Personal information about individual people.
- Personal information.
- Pricing lists and discounts …
- Productive relationships with various third parties.
- Proposals, business cases and descriptions of projects, products, processes *etc*.
- Security information such as security logs and configurations, CCTV footage, passwords, PIN codes, keys.
- Sensitive information shared with or entrusted to us by third parties in good faith.
- Signed contracts and agreements, business correspondence *etc*.
- Strategies, plans, intentions, priorities, concerns, risks.
- Strategies, plans, priorities, intentions, approaches and methods, policies, procedures ...
- Trade secrets and other types of proprietary information.
- Trade secrets, proprietary information, intellectual property *e.g.* source code for a software development company.
- Any other information that gives us commercial advantage, or on which we depend to do business and thrive.

Notice these bullet points are types of **information** not just digital data. It's true, *most* information is stored, processed and communicated by computers these days, but not *all*: we also need to protect non-digital formats, and defend against other threats besides hackers, malware and bugs.

If that is too hard and open-ended, focus initially on the significant and most valuable information, the 'crown jewels', the information assets that would be virtually impossible to replace if lost, damaged or otherwise compromised.

Next, what kinds of information-related situations, scenarios, events, incidents, disasters or crises might materially affect the organisation? For inspiration, consider:

- Information-related incidents that have actually occurred, including commonplace everyday things (such as typos and little accidents) that might turn out to be more serious (*e.g.* a simple mistake in a spreadsheet formula might affect our tax returns or annual accounts), as well as more dramatic cyber incidents, service outages and natural disasters. Look for patterns suggesting common factors and persistent causes.
- Near-misses: incidents narrowly averted due to good fortune. 'Being lucky' is not a sustainable strategy, whereas recognising, learning and responding to near-misses drives continuous improvement, hopefully without suffering any incident costs.
- Incidents affecting similar organisations such as industry peers or neighbours (*e.g.* social engineering tricks using industry lingo to fool workers), plus organisations using similar technologies (*e.g.* hackers or malware targeting the platforms, operating systems, applications and network services that the SME relies upon).
- Technological **and** other types of risk to or involving information. The adaptive approach includes but extends beyond IT. Classical cyber security controls alone cannot protect all forms of valuable information against all manner of threats – power cuts, floods and fires for instance.
- Novel incidents that are rare or have yet to occur: these are obviously the hardest to predict and control against, but factors such as heavy dependence on particular information, IT systems, business relationships *etc.*, and strong branding, advertising and promotion increase the organisation's exposure, vulnerability and hence risk.

Find more examples in appendix D.

Now knit those two perspectives together to identify significant risks relating to the most valuable information assets:

- Incidents usually involve the compromise of **C**onfidentiality, **I**ntegrity and/or **A**vailability – the classic CIA triad. Read all about this in appendix A.
- Of all the things that *might* happen, which ones scare us the most, and why? What about our stakeholders?
- Take into account both the chances of various incidents occurring and their severity when they do. Rare but potentially devastating incidents cannot be ignored.
- If it helps, consider the associated threats (causes), vulnerabilities (inherent weaknesses) and impacts (business consequences).
- Keep *brief* notes as a record of the risk assessment.

Given how tough it would be to project and quantify probabilities and impacts, subjectively comparing risks relative to each other is generally adequate for the purposes of the adaptive approach. **Iterative risk analysis** (appendix E) and **qualitative risk analysis** (appendix F) are two pragmatic, low-cost, rough-and-ready methods.

Every run through the cycle of 4 steps is another opportunity to review and update the risk assessment, so avoid analysis paralysis. It is more important to press ahead and tackle significant information risks *now* than to understand them in excruciating detail, at some later point.

If you and your colleagues are already familiar with a particular risk analysis method, perhaps even one from a different domain (such as financial, engineering, business continuity or safety risk management), you may be able to adapt and apply it in this context. The combination of probability with impact is fundamental to managing all types of risk.

Step ⓑ – pick an information risk to work on next

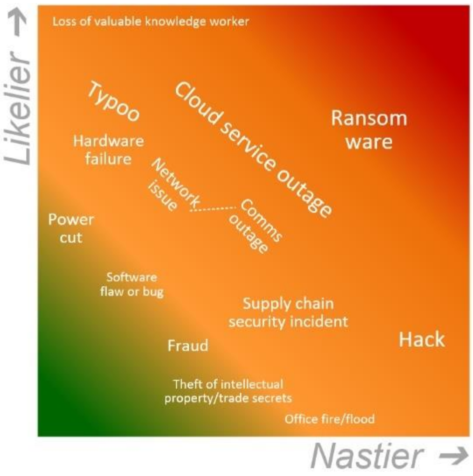
If you find information security overwhelming, pay attention!

With such limited resources and competing priorities, SMEs have little option but to concentrate our efforts by focusing.

The obvious question then is: focus on what?

The adaptive approach revolves around information risks, so this step involves considering the risks identified in the previous step, then picking on something that clearly needs to be taken forward – not everything right now, just the most urgent or most promising issue at this point.

For micro-businesses especially, focusing on the biggest risks one-by-one is a legitimate and powerful way to make real progress.



Risks towards the red corner of the **PIC** are clearly of most concern, making them obvious priorities for active risk-reduction or risk-avoidance. However, an SME may struggle to tackle them immediately, particularly when first adopting the adaptive security approach … so there may be good business reasons to work on less significant risks first, building up the capabilities, expertise and confidence. Deliberately deferring action on significant risks is a tough management decision, and another opportunity for management to reconsider the resources and priorities in this area.

Orange-zone risks across the middle diagonal of the **PIC** are often the most numerous. It may help to link-together related risks, addressing each cluster in turn. For example, mitigating malware-related information risks may require improvements to antivirus, backups and security awareness, involving coordinated efforts from both IT and HR. Again, this might be too much to tackle at once, so stagger the improvements over a few months.

Finally, risks towards the green corner of the **PIC** are of lesser concern and can probably be more-or-less ignored (accepted) … but don't forget that those situations may in fact occur and even minor incidents may coincide, accumulate or be worse than we predicted. Therefore, general-purpose controls such as incident management, backups and resilience are applicable across the entire risk spectrum. At some point (preferably early-on), someone needs to focus on those controls.

It is important to remain overtly business-focused in this step, providing management the information, latitude and support to make sound business decisions. Information risks must be understood in relation to other business risks and concerns. They all need to be well-managed, reasonably consistently. From your individual perspective, information risks may be paramount, but senior management may be even more concerned about markets, products, competitiveness, commercial strategy, compliance, technology, personnel, finances, health and safety, continuity, culture, succession planning, innovation or who-knows-what.

Look for opportunities to align and integrate information risk and security with the business as a whole. Can information security reduce market, product or commercial risks, opening-up business opportunities? Is it feasible to incorporate security improvements into IT projects and cultural change initiatives?

Step © – determine the approach

This analytical step involves exploring the chosen information risk/s and possible risk treatment options in sufficient detail to decide what to do.

There are four generally-accepted ways of treating risks, depending on where they fall on the spectrum:

1. **Risk avoidance** – not doing *extremely* risky red-zone things. Normally we only do things that have some purpose and value, so if we don't do them in order to avoid excessive risk, we forgo that value. We may avoid taking on risks (*e.g.* withholding valuable information from untrustworthy third parties), avoid increasing risks (*e.g.* not dropping our guard with long term partners), or stop risky activities (*e.g.* pulling out of business arrangements that have become unduly threatening to our interests).
2. **Risk reduction through security controls** - most risks are 'mitigated' in some fashion using technological, procedural or physical controls (also known as measures, countermeasures, safeguards *etc.*). Most controls have a specific purpose (*e.g.* antivirus controls attempt to spot and block malware infections) while some others are general-purpose (*e.g.* resilience and backups). Multi-purpose controls (*e.g.* backups, policies and procedures) can address several risks at once, and as such are often more valuable but less effective than single-purpose controls.
3. **Risk sharing**[1] - some risks can be shared by customers, owners, communities, teams *etc.*, who undertake to deal with them or accept the consequences (defined liabilities). For example, insurers undertake to compensate the insured if particular situations occur, *provided* the insured has taken reasonable/specified steps to reduce the risk. People willingly provide their personal information, *provided* recipients promise to take care of it.
4. **Risk acceptance** - all the remaining risks are said to be accepted, whether deliberately and expressly[2], or not. We accept risks that were only partially treated by other means (*e.g.* where the controls are not entirely effective and reliable, or where situations we intended to avoid occur anyway, or where our attempted quantification was inaccurate, perhaps because things changed unexpectedly) plus risks that were ineptly or inappropriately treated (*e.g.* risks we didn't even identify as such, due to limitations or flaws in the early stages of the risk management process).

Thorough analysis is clearly a lot of work, especially if we decide to research and analyse data on likelihoods and impacts of various information risks, and explore the costs and benefits of various potential controls. So, a quicker, simpler, more pragmatic approach is to shortcut the risk analysis by adopting 'typical' security controls. Even without explicitly tackling their information risks, most organisations already have some controls in operation. It may be cheap and easy to adopt a few obvious candidates for a quick-start or step-up in capability.

> Generic frameworks such as ISO/IEC 27001 and NIST CSF can prove worthwhile. They typically address a significant proportion of the information risks commonly faced by organisations simply by suggesting commonplace information or cybersecurity controls. However, most are aimed at larger organisations with more resources.

The following table outlines a range of information security controls specifically for SMEs, broken down according to the size of organisation. **These are merely generic suggestions to consider.** They may or may not be appropriate for *your* SME. In particular, there is no point investing in controls against acceptable, negligible or non-existent risks, and you may face unusual information risks not addressed by these controls. This is not a shopping list!

Appendix B lists *numerous* SME security standards and other resources offering further guidance.

[1] This is termed 'sharing' not 'transferring' because some risk persists (*e.g.* insurers may yet refuse or reduce claims or go bust), plus whoever decides to share risks remains accountable for that decision if it doesn't work out.

[2] Management can legitimately decide to retain and do nothing about risks, opting to take their chances. Normally, this is a sensible option only for risks with trivial impacts and insignificant business consequences. However, flagrantly disregarding rare but devastating incidents is a bet-the-farm decision, tightrope walking without a safety net. Tread carefully.

Micro	Small	Medium
Governance, strategy, policies, plans …		
Notionally set side sufficient finances, time and other resources to tackle the main information risks in a reasonable timeframe. Lightly documenting your existing risk and security arrangements is a good place to start.	Manage and monitor expenditure on information security within budgets. Justify budget requests and proposals in business terms, and argue for a fair allocation. Prioritise controls that address the highest risks to get the most security benefit for your investment.	Emphasise multi-purpose controls that address multiple risks. Distinguish capex (more significant **cap**ital **ex**penditure *i.e.* investments) from opex (routine **op**erational **ex**penditure). Clarify management's accountability for resourcing and priorities allocated.
Commit to making fundamental security improvements, starting with a written list or plan for the present month and brief daily security tasks. Pick out and focus on just a *few* (less than 4!) top priority short-term, information security controls or improvement initiatives.	Plan security improvements as a series of quarterly phases stretching about a year ahead, with monthly or fortnightly team meetings to check/measure and direct further progress.	Prepare a set of options for management, including the governance and management arrangements and an overall multi-year programme.
Leverage free or low-cost security resources including built-in tools, apps or online services and information. Use basic office apps such as Google Workspace or Microsoft 365 to administer information risk and security-related documents - policies, reports, approvals, contracts *etc*.	Use online collaboration and document management tools such as Google Drive, OneDrive, Box and SharePoint. Introduce DocuSign, Acrobat or similar apps for electronic signatures on authorisations, contracts *etc*.	Adopt some form of Document Management System: structuring, filing, indexing, searching, retrieving, maintaining and authorising risk and security-related information is easier with automation.
Prepare a basic, generic, lightweight information security policy covering important controls such as passwords, patching, antivirus, backups *etc*. Review and update it every year or so.	Prepare an overarching security policy mandated by the CEO supported by topic-specific policies covering aspects such as identification and authentication, access control, background checks and incident management. Review and update the set annually.	◀ That plus … A suite of security procedures, checklists, forms, guidelines *etc*., plus awareness and training materials, maintained quarterly and reviewed as a whole annually.
HR/personnel elements, awareness, training, motivation		
Seek reputable and competent suppliers for security and privacy around IT, HR, websites, finances, payments, compliance *etc.* Seek recommendations or referrals from trusted peers.	Develop and provide security and related services in-house, where more cost-effective than commercial suppliers. Consider appointing a virtual or fractional CISO, preferably someone to train-up, mentor and support a suitable employee to take on the role at least part-time.	Consider the need for an Information Security Manager, CISO or similar senior role, leading a small team of competent experts. Bolster corporate risk and security services, drawing selectively on external expertise only where necessary for specified assignments (*e.g.* audits).

Micro	Small	Medium
Prepare and circulate basic security awareness materials such as an ‘acceptable use policy’. Demonstrate your commitment to security (walk-the-talk, bring it up in meetings and conversations). Talk through security with new recruits.	◀ That plus … Prepare more comprehensive risk and security awareness content and make it readily accessible for all workers, particularly any new/changed policies. Liaise with HR on security aspects of onboarding and disciplinaries.	◀◀ Those plus … Train risk and security specialists, plus new starters including temps. Test to validate knowledge transfer, understanding and fulfilment of responsibilities. Ensure the disciplinary process can handle information incidents, forensics *etc.*
Keep information risk and security in mind. Make sure everyone is not merely aware of current threats such as phishing and malware, but is actively spotting and responding to potential attacks. Facilitate and encourage prompt reporting of concerns and incidents. Provide advice and guidance on topical issues and priorities.	Inform, engage and motivate workers on information risk and security policies, controls, concerns *etc*. Develop a basic security awareness program providing regular updates *e.g*. through emails, newsletters, posters, agenda items for team and management meetings *etc*. Bring things up in conversation, note them in reports *etc*.	Develop a structured, rolling/continuous security awareness and training program. Plan a sequence of topics or focal points. Use multimedia. Promote the security culture consistently, walking-the-talk, demonstrating management’s interests and concerns at every opportunity. Measure and reward awareness and proactivity.
Information risk and security management including cyber		
Choose a reasonably private and secure home office, or at least an area that can be easily cleared of potentially sensitive and valuable information, devices *etc*. when not in use or visitor call.	Rent a shared/temporary office space or buy a small office supplementing home working, with secure facilities to store and process information.	Invest in dedicated, branded offices with suitable facilities to access, process, secure and archive information, and identify alternative locations in case of an office fire, flood or other disaster.
Identify critical data and assets (*e.g.* customer information, financial records, trade secrets). Identify basic security vulnerabilities (*e.g*. minimal cyber resources and skills in-house), threats (*e.g*. compliance failures, malware, pressure from customers) and impacts (*e.g*. fines, loss of custom). Talk this through as a team – or in front of the office mirror!	◀ That plus … Conduct and document a more thorough risk assessment, concerning a wider range of threats, vulnerabilities and impacts. Run risk and security workshops tapping-in to the collective wisdom.	◀◀ Those plus … Utilise available resources for risk assessment such as online tools and benchmarks. Review incident records for clues about longstanding, widespread or serious as-yet-unresolved issues. Introduce quantitative risk analysis methods for greater insight where it makes sense.
Schedule, proceduralise and if appropriate script or automate regular security tasks. Add diary entries as reminders of regular/routine activities such as: checking backups, antivirus and other important controls; spotting changing risks; patching …	◀ That plus … Work with relevant heads/leaders to ensure required regular and *ad hoc* activities are scheduled/planned, resourced and completed. Increase scripting and automation.	◀◀ Those plus … Work with relevant internal and external resources to improve the routine and *ad hoc* activities, automating extensively and minimising inefficiencies and inconsistencies

Micro	Small	Medium
Minimise powerful administrator access to IT systems unless workers have both the need and the competencies to avoid security breaches. Encourage the use of password managers and multi-factor authentication. Pay special attention to securing email, financial, managerial and administrator accounts.	Adopt roles such as system, risk or asset owner. Adopt multifactor authentication for all trusted, privileged or important accounts, logins, apps, services *etc.* if possible, plus a password manager app. Review and update access rights periodically, especially after workers leave or change roles, and more frequently for important systems.	Facilitate and support proactive and timely management of roles, responsibilities, privileges, access rights, permissions *etc*. by the relevant business managers, plus independent checks on important systems. *Insist* on strong multifactor authentication as a rule, wherever possible, plus an enterprise-scale password manager app. with centralised management & recovery.
Basic security logging with occasional checks *e.g*. react to backup failures within a week at most.	More detailed security logging with alerts/alarms for significant events, plus response procedures and daily checks (*every* day!).	Automate security monitoring and alerts, escalation paths, planned incident management, and hourly or contemporaneous checks 24x7.
Develop a sensible backup schedule *e.g*. quarterly off-site data backups and weekly cloud backups. Test[3] recovery *at least* once a year. Where possible, cross-train and share key security tasks among workers, or at least document them so someone can pick up the pieces if workers leave or fall sick.	Develop a sensible backup strategy with full image and differential backups, both on- and off-site. Test recovery quarterly and before significant IT changes. Train-up or contract with suitable deputies providing cover and support for documented security procedures.	Extend the backup strategy with high-availability RAID/mirroring and long-term archival arrangements. Exercise to improve and test to prove recoverability, before *and* after significant IT changes. Build a competent team of information risk and security professionals.
Reduce the volume of data online by deleting apps and data if no longer required, or moving it to offline archival storage. 'Spring clean' your cloud and local storage at least once a year. The less available, the less there is for someone to steal, hold to ransom or disclose.	Provide secure archival facilities plus policies and procedures to take information safely offline, or systematically identify and archive/delete/purge redundant information. Standardise apps and services. Restrict the ability to install or access apps/services other than those sanctioned as secure, necessary and appropriate. Review/audit to identify and deal with unauthorised apps, services, network traffic *etc*.	Constrain or charge business units for online storage capacity, encouraging them to reduce the amount of information remaining online. Archive/delete/purge periodically. Use the funding to risk-assess and proactively manage the security of additional apps *e.g*. build a security test lab. Actively manage local storage including USB devices, and cloud storage, as well as corporate network drives.
Enable automated patching of systems, devices and applications. Check every few months that *everything* is fully patched and up to date - no exceptions. Retire or replace any that are no longer actively supported by the suppliers and cannot be updated.	Centralise patch management including prioritisation of urgent security patches addressing exposed and exploited vulnerabilities, plus patch coverage/version monitoring. Regularly scan networked systems and applications for known vulnerabilities using suitable tools. Isolate and plan to replace any unsupported systems.	Invest in proactive threat and vulnerability management, including commercial penetration testing if justified. Promptly risk-assess, test and install relevant security patches for operating systems, applications and firmware on all devices. Replace/upgrade aging systems well *before* they become obsolete. Hunt down and address any exceptions.

[3] Use a suitable test environment. **Do *not* try restoring backup data to a production system just in case it fails!**

Micro	Small	Medium
Pay attention to security for network perimeter controls such as switches and routers *e.g.* only acquire current, supported products and keep them fully patched. If possible, share risks with broadband/comms providers through service agreements.	Maintain a dedicated server room or at least a lockable cupboard or rack unit for network devices. Pay special attention to cabling *e.g.* physically labelling and securing the cables against accidental damage, vandalism or theft. Keep records about network routes, devices, addresses *etc*.	Secure networking and comms devices in the server room or another protected area. Hire or train-up a network administrator to address network security controls at all levels of the stack from physical to users.
Incident and business continuity management		
Think through responses to common incidents *e.g.* ransomware, power cut, network/comms outage, IT failure.	Plan and document responses to a broader range of incidents, in conjunction with those who would be involved.	Prepare and maintain incident response policy, procedures, team, tools, playbooks *etc.*, drawing on existing resources plus good practice advice.
Run a desktop exercise roughly once a year, simulating the recognition, response and resolution to a serious incident.	Establish basic business continuity arrangements. Run periodic incident management/disaster recovery exercises involving the entire organisation.	Establish a comprehensive business continuity approach. Run quarterly exercises, covering all major IT systems and services (at least) in the course of each year.
Assurance and maintenance		
Ask a trusted, competent person - possibly someone from a peer or partner organisation - to review and comment on your information risk and security arrangements. Offer to reciprocate if appropriate. Repeat occasionally *e.g.* every few years.	Review information risk and security arrangements as appropriate In addition, train-up one or more internal auditors temporarily seconded from the business, or use contractor/consultant auditors, to conduct internal audits of the information risk and security arrangements regularly *e.g.* annually.	Beef-up the assurance measures including reviews, tests and audits to reassure senior management that things are working well. Develop an internal audit program concerning who audits what, how and when. Consider penetration testing and external audits if appropriate, including formal security certification.
Subscribe to vendor security advisories and alerts from CERT *etc.*	Subscribe to security advisories, alerts, journals, blogs, podcasts, newsletters *etc.*	◀ That plus … Encourage the team to complete security training courses and attend or speak at security conferences
Accept that, although it may not be possible to make continuous steady progress due to competing priorities, it will take sustained effort to achieve results.	Measure and report key metrics to senior management annually, demonstrating progress made and future plans. Update and collaborate with sympathetic peers as much as possible, taking an interest in their challenges too.	◀ That plus … Add more frequent regular management reports plus *ad hoc* specials such as post incident reviews, audits, cybersecurity updates and new security policy, strategy or investment proposals. Coordinate security plans and projects with peers and specialists.

Step ⓓ – make it so

Having identified and evaluated information risk and decided what to do, the next step is obviously to do it.

Normally this means implementing or strengthening certain information security controls to mitigate unacceptable information risks, but don't forget that risk sharing and risk avoidance may also require action:

- If risks are to be shared with others, there is usually some form of notification, negotiation and agreement on the terms and conditions. This may be formalised through commercial contracts (such as insurance or outsourced security operations), contract clauses (such as defined responsibilities and liabilities for suppliers, partners, customers and employees) or some other evidence of their acceptance (such as a website visitor clicking to agree/opt-in to a privacy policy, dropping a record in the log).
- If risks are to be avoided (*e.g.* by not starting, slowing down, halting or reversing excessively risky business activities), the associated business changes may need to be driven through, especially if there are substantial drawbacks or costly consequences for the business. Assurance checks may be appropriate to follow-up and confirm to management that the risky situation is, in fact, fully and permanently resolved.

A well-defined security implementation plan can help enormously, especially if there are lots of things to do and people involved. Include plenty of contingency in the plans and track its consumption from the very instant things *start* to overrun or over-spend. Don't wait until all the planned time and budget are gone before dipping into the contingency set-aside: by then it's probably too late to make changes necessary to get back on track.

While addressing security is vital, so are other business priorities and competing demands. A balanced approach to resourcing is necessary. However, don't let the need for immediate action on other priorities overshadow the very real threat of cyberattacks (such as ransomware) and physical disasters (such as storms or earthquakes) which could happen at any moment - possibly even right now while you are reading these words. Addressing security alongside other needs requires a realistic assessment of the remaining, untreated risks and the potential consequences of inaction.

In short, time is of the essence.

A note about security tools and services: technologists, generally, love our abbreviations and acronyms. Marketers have latched on to the idea of selling security products with catchy labels such as EDR, SIEM, MS and *aaS. Many commercial security products are aimed primarily at large or very large and mature organisations with deep pockets and sprawling networks. More modest and in some cases free security technologies may be of value to SMEs with particular needs. Either way, clarify the business and security objectives before even evaluating, let alone selecting and acquiring tools, to avoid wasting time and money on dead-ends.

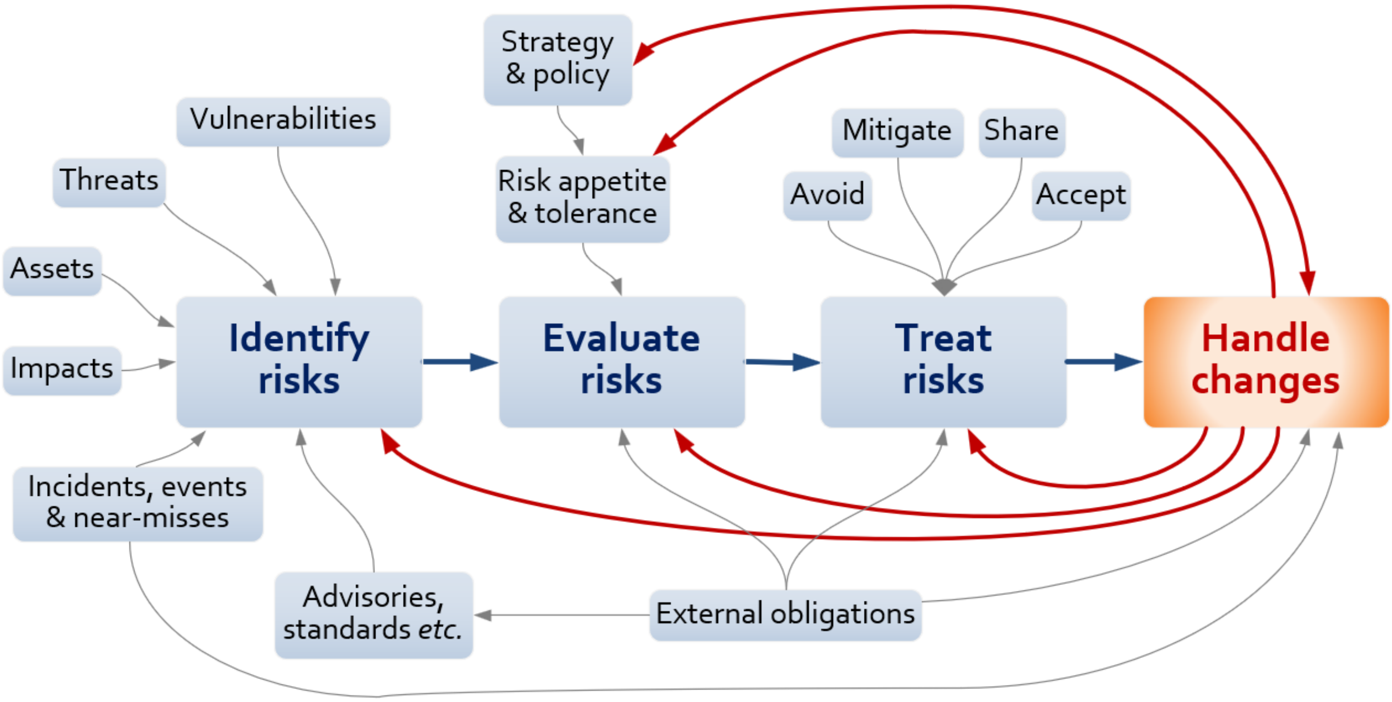
Deliverables from phase ④

A functional approach to manage information security, proven by completing the first few laps of the cycle. By now, you should have knocked over one or two of your biggest information risks.

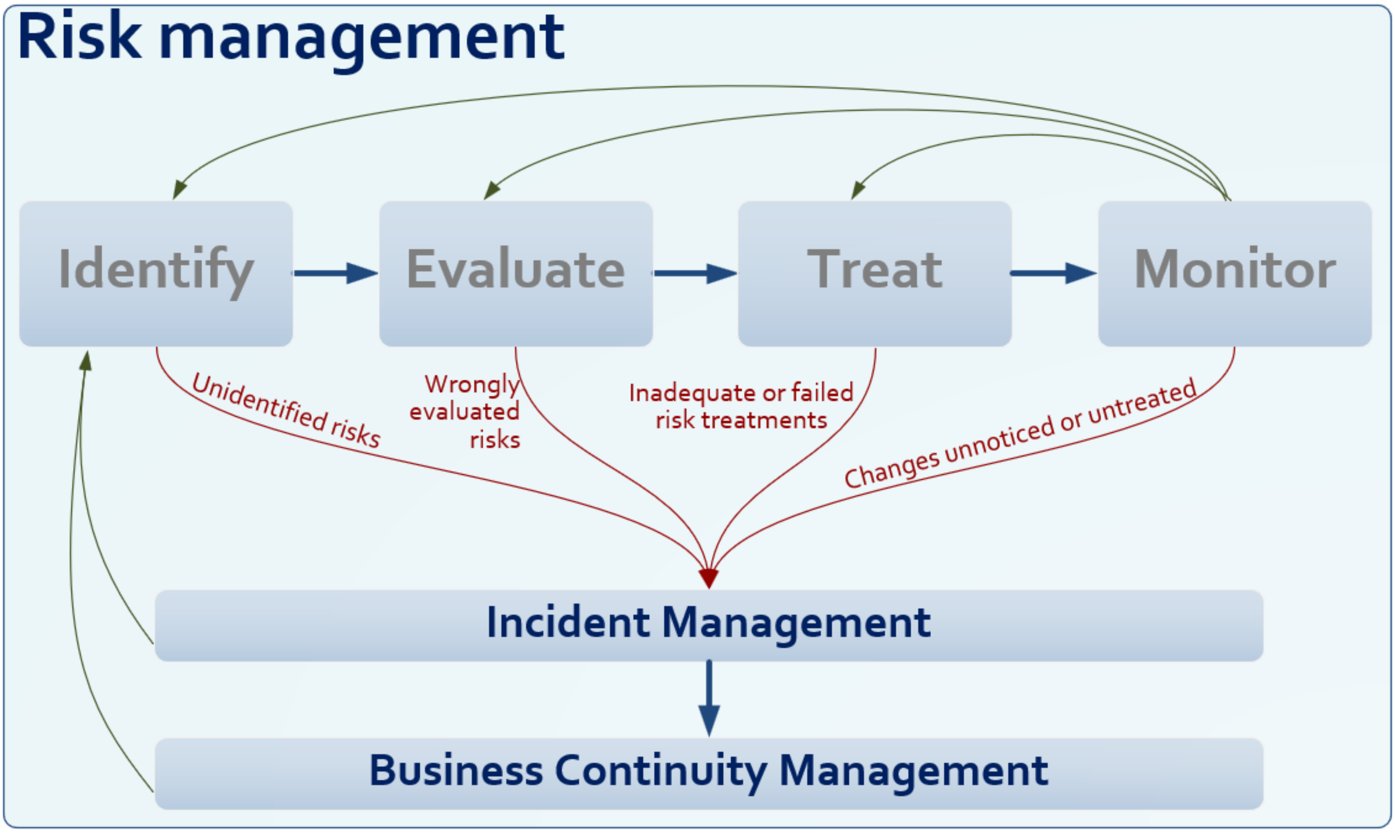
Phase ⑤ – M^4 (Monitor, Manage, Maintain, Mature)

As with the earlier phases, phase ⑤ remains strongly business-aligned. The information risk and security management arrangements now operating *must* continue to serve the needs of the SME.

Aside from continuing to cycle through the information risks, there are several information flows, feedback loops and links to other business activities to manage. For starters, given the need to track and respond to both gradual and step changes in the business, technology, risk and compliance contexts, **change** management is important:



Similarly, the possibility of significant **incidents** causing serious harm to the business means further aspects to manage:



Business **value** (benefits less costs) should be driving decisions, including opportunities to drive changes. Is there **value** in automation and tools to support the management of information, information risk and information security? Alternatively, how can the manual processes and activities be made more efficient and effective, more **valuable**?

Keep tracking value-added. Identify security wins and celebrate them. Be honest about security fails, learn the tough lessons … and do something positive about them!

Various **metrics** can be designed to quantify and record progress - in particular, measures relating to the objectives defined in phase ② plus the implementation status of risk treatments initiated in phase ④. 'Security maturity' **metrics**, for instance, concern the organisation's general capabilities in this area, covering aspects such as:

- Residual (current) risk levels.
- Security effectiveness and efficiency.
- Organisational resilience.
- Compliance and conformity.
- Readiness, reactions or responsiveness to changes – including changes driven by **management** or naturally occurring (*e.g*. the evolving corporate culture), as well as those imposed on the SME from elsewhere.
- Trustworthiness plus trust or confidence …

Assurance is an important part of phase ⑤ and can contribute to previous phases as well. Assurance involves putting arrangements in place to provide **management** with reliable information and guidance concerning the status of information risk and security by:

- Gathering suitable evidence through reviewing, testing, checking and auditing practices.
- Sound analysis and evaluation of the information, drawing sensible conclusions such as the root causes of any identified issues.
- Making sensible suggestions, proposals or recommendations to address the issues and make improvements.

Once things have settled down, here are some strategic development ideas to squeeze even more value from your adaptive information risk and security management approach:

- **Manage** changes, planning improvements for compliance, business developments, evolving threats, new technologies *etc.* Review and update strategies, plans, policies, procedures *etc.* to remain relevant, address the evolving objectives, mitigate current and future risks, exploit new technologies, tools and services, and support/enable changing business requirements. Explore strategic and tactical options.
- Integrate or at least align the information risk and security strategy and approach with other areas of the business such as risk, continuity, compliance, IT, privacy, operations, finance …
- Scale-up, learn and **mature**:
  - Identify and seize or engineer improvement opportunities (hinting at strategic development). Find even more ways to support and enable the business to develop and thrive, not just survive *e.g*. new business opportunities, partnerships and services; systematically identifying then improving or replacing or simply dropping controls that do not earn their keep.
  - Rather than simply reacting to things, become more proactive. As information risk and security is brought under management control, that releases resources to push ahead with other activities.
  - Identify and tackle further pain-points, including relatively minor but persistent annoyances such as cultural issues (suggesting root cause analysis and concerted, sustained effort).
  - Improve management information and assurance. Put more effort into checks, tests, reviews, audits. Reassure stakeholders that information risks are being proactively managed, generating value. Offer suitable evidence to substantiate that *e.g*. strategies, metrics.

Being able to demonstrate added value and successes is an important way to secure more support and resources, and to direct attention to the most/least valuable aspects, giving the objectives and metrics additional significance.

- Improve supply chain security **management**:
  - Work with your upstream suppliers, partners and downstream customers with the aim of 'levelling' the information risks throughout the entire supply network.
  - If everyone achieves broadly the same level of security, the risks are shared evenly, whereas if any player has fallen behind, they may drag the team down with them.
  - Coordination and collaboration with other organisations when things are going well will pay dividends when issues or incidents occur. This is a sadly under-valued resilience and business continuity measure, and a business opportunity for SMEs who are truly on-the-ball.
- Spread the good news! Write for and present to local small business groups, chambers of commerce, industry forums, national or international organisations (such as the Institute of Directors), online communities (such as the ISO27k Forum) and social media. Share useful lessons on information risk and security, celebrating the progress you have made, supporting and encouraging others.
- Head towards certification:
  - Drift or drive into conformity with ISO/IEC 27001, Cyber Essentials *etc.*, where that makes good business sense (*e.g.* if customers request or demand it, if it offers competitive advantage, or if obliged by laws and regulations) …
  - … which implies preparing and being ready to move ahead at pace, since deadlines to respond to sales enquiries or tenders, achieve compliance *etc.* are generally short. Being proactive on information risk and security puts an SME in a stronger, more confident position.
  - Exploit the business value of the systematic approach and demonstrable security improvements through marketing and promotion (*e.g.* "Hey look at us: we're *certified* secure!").

Deliverables from phase ⑤

The main deliverable from this phase is intangible *i.e.* the organisation is competently managing its information risks using the chosen risk treatments to bring them within a tolerable level, resulting in an acceptable frequency and severity of information security incidents, breaches, compliance failures *etc*. This can be demonstrated by security metrics and assurance such as certification.

Conclusion

Implementing an appropriate information risk and security management approach, even at a micro-level, significantly improves an SME's security posture or status – not just the appearance of security, but the actuality. It involves identifying, analysing and systematically reducing the probability and/or impact of various information risks, increasing management's control.

Information risk and security management is an ongoing process, requiring continuous adaptation and improvement leading to maturity. It is perfectly acceptable and understandable to start out with the fundamentals and adopt more sophisticated arrangements gradually over time, at a pace that suits the business. The adaptive approach

> *"Security is very similar to health. If you don't exercise, if you eat badly, if you don't sleep, you're probably going to get ill … If you don't have good governance, if you don't think about your risks, if you don't make your users aware, if you don't have good technical controls, you're going to have an incident. You don't need to be amazing at this, you don't need to be incredibly fit but you've got to do the basics to help protect information."*
>
> Steve Townsley,
> Head of Information Security,
> Mercedes F1

Appendices

Appendix A: backgrounder on concepts

This appendix gives a broad introduction to and overview of information risk. There is a lot of ground to cover here so this is quite lengthy, despite being quite superficial. Several key terms of art are defined in the glossary.

Incidents (happenings, events, accidents, attacks, crises …) involving information typically cause or involve a loss of or reduction in its:

- **Confidentiality** – unauthorised/inappropriate disclosure or revelation or exposure of sensitive information;
- **Integrity** – incomplete, inaccurate or out-of-date information; and/or
- **Availability** – information cannot be accessed and used for its intended purposes, for a while or indefinitely.

Those are the primary effects. However, incidents can also have secondary adverse effects such as a loss of or reduction in:

- **Compliance** with legal, regulatory or contractual obligations – increasing the possibility of penalties such as fines and additional supervision;
- **Conformity** with and satisfaction of personal, corporate or societal requirements, including ethical expectations;
- **Access** to information *e.g.* it may take longer or be more difficult to acquire sufficient, appropriate data for various purposes;
- **Information management** capabilities *e.g.* the legitimate owners of information may be unable to secure it, restrict/permit access to it, determine who can use and how and when *etc.*, or may feel it is not even worth attempting to do so due to losing confidence in security;
- **Quality** *e.g.* AI systems may hallucinate, offering factually inaccurate but plausible information, or advisors may give misleading, inappropriate, inaccurate or incomplete advice;
- **Flexibility** *e.g.* it is costlier, harder, more complicated and takes longer to plan, execute and test/validate/accredit changes to a secure IT system or process;
- **Reliability** and **trustworthiness** *e.g.* it may be unclear or uncertain whether information is sufficiently correct, complete, current and controlled following an incident, particularly if the exact nature and sequence of events cannot be ascertained;
- **Understanding** of information *e.g.* due to translation or transcription errors, inadequately-explained or ineptly-expressed concepts, cultural and comprehension issues;
- **Utility** *e.g.* information that is no longer considered sufficiently trustworthy, complete, accurate and up-to-date for its intended purposes may be unusable.

Furthermore, incidents may lead to an increase in:

- **Information processing**, **communication** and **storage** – aside from overheads caused by the operation of security controls, security logs typically store pertinent information for later analysis, and some incidents involve the deliberate or accidental accumulation of 'junk' data obscuring events;

- **Delays** – slowing down dependent decisions, activities or processes while necessary information is obtained and verified;

- **Complexity** – increasing controls for a system or process makes it more complicated, adding 'moving parts' that all need to function properly and interoperate smoothly; and

- **Uncertainties** and **risks** of further incidents – once an incident such as a ransomware attack or privacy breach occurs, that may increase the probability and/or impacts of further incidents.

Ultimately, incidents destroy **value**. As a consequence of various incidents, information is worth less to its legitimate owners and users, and perhaps more to adversaries or competitors. Furthermore, incidents drive up losses and costs such as:

- The **direct** loss of asset value *e.g*. theft and misuse of intellectual property or trade secrets, or reputational damage and brand devaluation;

- **Consequential costs** due to disruption or prevention of downstream business activities *e.g*. urgent revision or suspension of commercial plans to launch new products;

- Costs associated with **managing**, **investigating** and **resolving** incidents *e.g*. attempting to resume control and regain customer trust, loyalty and custom;

- The full **lifecycle costs** of various controls – from specification and design through to their operation, management and maintenance;

- **Opportunity costs** – other potentially beneficial investments or activities are delayed, curtailed or prevented due to the lack of funds and other finite resources, including management and staff attention and energy; and

- **External impacts** *e.g*. privacy breaches adversely affect the lives of the individuals whose personal information is compromised.

In the business context, it makes no sense to spend a fortune on reducing trivial incidents. Conversely, targeted investment to avoid, prevent or contain the damaging effects of significant risks is entirely justified, even necessary. Therefore, we really need to **analyse** and **quantify** risk in order to invest appropriately, especially given limited/finite resources.

Incidents fall on a notional **impact** or damage scale from zero (having absolutely no adverse effect on the organisation at whatsoever) to catastrophic, maybe even existential. Incidents also vary in **likelihood** from never or extremely rare to commonplace or continuous. **Risk** is a *combination* of *both* **impact** *and* **likelihood**.

Although historical data and trends may give us clues about both aspects, the information is often limited and unreliable, particularly in the case of novel or as yet unrecognised incidents. The analysis can be complicated if we take into account the **distribution** or range of impact and likelihood values, and compounding factors such as incidents occurring at 'the worst possible time' or 'in the worst possible way'. Coincident and widespread incidents are particularly challenging both to assess and to treat – as we saw recently in the case of COVID-19.

In short, the best we can do in in reality is to **estimate** information risks with some margin for error.

One way to estimate and compare the **likelihood** of various incidents is to explore the **threats** (external factors that impinge on the SME) and **vulnerabilities** (inherent weaknesses within the SME and its information systems and processes), thinking particularly about information, digital data, IT systems, networks, information processes and activities.

Take an SME's financial management, for example. If the SME uses paper ledgers, calculators or IT systems ranging from Excel up to sophisticated server or cloud-based financial management systems and services:

- Relevant **threats** include accidents and mistakes, misunderstandings, data-entry errors, design flaws and programming errors (bugs), fraud and misappropriation, plus hacks and malware. Although they may be less common, more extreme threats, such as office fires/floods and intrusion or manipulation of systems by well-resourced criminal gangs and government agencies cannot be ignored.
- Relevant **vulnerabilities** include management's reliance on the computer systems and services plus information values and feeds from third parties (such as tax rates and rules for coding expenses, and information from the banks and payment services), dependence on software suppliers plus network services and electricity. Diverse vulnerabilities such as complexity and change may make some financial systems riskier than others – but offsetting that, there may be benefits such as harnessing Artificial Intelligence for decision-support.

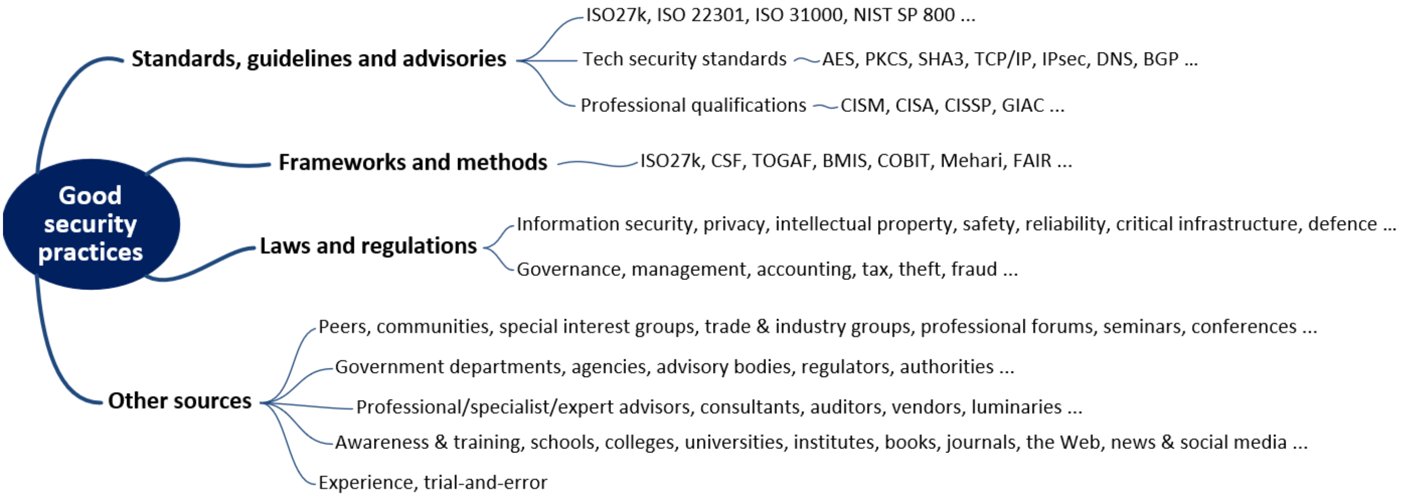
An effective way to estimate and compare the **impact** of potential incidents is a systematic business continuity management process, **B**usiness **I**mpact **A**nalysis. BIA focuses particularly on 'serious incidents' or 'disasters' that could cause 'significant' damage, costs and disruption to 'the business' (mostly its operational or production activities, particularly those relating to its core business – healthcare for a dentist or doctor's clinic, professional services for an IT, advisory or consulting business, education for a school or college …), on the basis that they are probably among the greatest risks and hence priorities for management. However, BIA may down-play or disregard gradual or widespread risks such as human errors, mistakes and accidents that account for numerous mostly minor incidents that collectively represent a drain on society and the economy.

Furthermore, the **costs** and other implications of various security controls vary widely: some are more-or-less free, while others are extraordinarily expensive to acquire, implement, use, monitor, manage and maintain. Some (such as password length and complexity criteria) are generally configurable and can be 'dialled-up or -down' in strength to reflect changing risks, whereas others (such as **P**ublic **K**ey **I**nfrastructures) are relatively inflexible once implemented. Likewise, the **effectiveness** varies: few controls are totally 100% effective and utterly reliable, while most are somewhat effective and some have dubious effect or are highly unreliable, perhaps even counterproductive (costing more than they save). In addition to quantifying risks, it helps to compare the value of various controls as part of the security decision-making process, but again net value (defined as benefits less costs) is tricky to determine or indeed measure.

Underlying all of this is the troublesome issue of **uncertainty** which makes predicting the future inherently difficult and error-prone, especially in novel, complex and dynamic situations. Uncertainty makes it difficult to figure out exactly what might or might not happen, how and when, especially over the medium to long-term appropriate for investing seriously in information security. Uncertainties make it tricky to design and apply controls, and in some circumstances dangerous to rely upon them working as intended. We are talking about messy real-world business situations here, not the nice clean theoretical models and academic studies under laboratory conditions. Consider the practicalities of dealing with the information risks facing Anne, Anil, Alison and Andy, the audiences we had in mind while preparing this guideline: their SME businesses are simply three notional examples plucked from the millions out there.

Given how difficult it is to predict information risk and manage information security, it is tempting to ask why bother? That brings us to **risk tolerance**, **risk aversion** and **risk acceptance**. An SME's owners/investors/creditors, managers, directors, employees and supply chain partners may each have differing perspectives, desires or fears about risk, including information risk. The most risk-averse over-emphasise the effects making them extremely uneasy about ignoring or failing to address risks that are of little concern to more risk-tolerant individuals. Conversely, risk-seekers may actively seek out and willingly take substantial risks, particularly if they believe there is sufficient chance of making a fortune or succeeding in some other way. Finally, risk-ignorants are unaware or fail to appreciate the reality of the risks they face: a classic example is a distracted or blasé worker absent-mindedly clicking a link in a phishing email, then disclosing their username and password to the phishers, without even realising they have been duped.

Appendix B: a cooks' tour of SME guidance on information security


Good security practices
Standards, guidelines and advisories
ISO27k, ISO 22301, ISO 31000, NIST SP 800 ...
Tech security standards
AES, PKCS, SHA3, TCP/IP, IPsec, DNS, BGP ...
Professional qualifications
CISM, CISA, CISSP, GIAC ...
Frameworks and methods
ISO27k, CSF, TOGAF, BMIS, COBIT, Mehari, FAIR ...
Laws and regulations
Information security, privacy, intellectual property, safety, reliability, critical infrastructure, defence ...
Governance, management, accounting, tax, theft, fraud ...
Other sources
Peers, communities, special interest groups, trade & industry groups, professional forums, seminars, conferences ...
Government departments, agencies, advisory bodies, regulators, authorities ...
Professional/specialist/expert advisors, consultants, auditors, vendors, luminaries ...
Awareness & training, schools, colleges, universities, institutes, books, journals, the Web, news & social media ...
Experience, trial-and-error

Standards and other reference sources

- ISO/IEC 27000 - overview and glossary for the ISO27k standards - free!
- ISO/IEC 27001 - formal information security management system specification
- ISO/IEC 27002 - a page explaining each of the 93 controls in ISO/IEC 27001 Annex A
- ISO/IEC 27003 - explains the formal requirements in ISO/IEC 27001 (2013 version – update in progress)
- ISO/IEC 27004 - how to design and use information security metrics
- ISO/IEC 27005 - techniques to analyse/assess & treat information risks
- ISO SME information security guide – ISO's guide for medium-sized organisations to adopt ISO/IEC 27001
- Pragmatic ISMS implementation guide – free guidance on implementing ISO/IEC 27001 for medium to large organisations
- DIN SPEC 27076 – German IT security standard for SMEs
- ISO 31000 - risk management, in general
- ISO/TS 31050 - improving organisational resilience, extending ISO 31000
- NIST Cyber Security Framework small business quick start guide - free!
- ISO27k Forum, ISO27k FAQ & ISO27k Toolkit - free, all free!
- ISO 27001 ISMS Handbook: Implementing and auditing an Information Security Management System in small and medium-sized businesses by Cees van der Wens (paperback ~US$40 from Amazon)
- The ISO website is the official source of information on ISO and ISO/IEC standards
- The ISO27001security website describes each of the ISO/IEC 27000-series standards, both published and in preparation, and offers free resources for implementers including this guideline and the ISO27k Forum

Methods, models and mechanisms

Alignment, adoption or conformity with conventional information security approaches may be an SME business goal, particularly if we are under pressure from customers or the authorities to standardise and demonstrate maturity in this area. The number of guidelines means plenty of choice with lots of well-meaning advice but can be bewildering – so the table below succinctly summarises and compares *some* of them, purely for your awareness.

The ticks indicate – roughly – which controls are covered. The colour-coded headings *suggest* guidance that may be suitable for micro, small and medium-sized organisations respectively. This classification, and the whole table in fact, is a generic and subjective assessment: *your* SME may well value any of the controls, any of the guidelines, or something else entirely.

These are not mutually exclusive options, in other words it is OK to pick and choose whichever controls are appropriate for the business, given its unique circumstances, and particularly its information risks. However, please bear in mind that the governance and management arrangements described by some of the guidelines may not work effectively unless fully implemented. Structured incident management and assurance activities such as reviews and audits, for instance, are typically required to drive continuous improvement of the security management arrangements: omit those and things are more likely to decay and fall apart than to build into a thing of great beauty and elegance.

Note: the **value** column shows the balance of benefits *typically* achieved less the associated costs but that is highly subjective and context-dependent – a rough indication at best, so please don't rely entirely on our assessment. Naturally, it makes business sense to adopt **H**igh-value controls, but the **M**edium and even **L**ow-value ones may be worthwhile. Furthermore, the table is not comprehensive: other controls and variants may be required and may offer *even better* value.

Security controls	Value	NIST SME quick-start	NCSC Small biz guide	ACSC Essential 8	Belgian small guide	Victoria law	CERT NZ	IASME cyber essentials	ENISA SME sec guide	Singapore Cyber Essentials	CIS criticals	ISO SME guide	ISO/IEC 27001
Identification, authentication & access control inc. MFA, default passwords & accounts	M	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Backups	H		✓	✓	✓	✓	✓		✓	✓			✓
Patching/updating, vulnerability management	M			✓	✓	✓	✓	✓		✓	✓		✓
[Mobile/portable] Device & media security & home working	M		✓			✓	✓	✓	✓	✓			✓
Incident detection, response & management, business continuity, recovery, resilience & contingency	M	✓				✓	✓		✓		✓		✓
Malware/antivirus	H	✓	✓		✓			✓		✓	✓		✓
Network security: firewalls, segregation, redundant links	M				✓		✓	✓	✓		✓		✓
Cloud, web & browser security	M						✓	✓	✓	✓	✓		✓
HR/personnel security, background checks, roles & responsibilities & reporting lines, accountability, health & safety, awareness, training, competences, culture *etc.*	M					✓			✓	✓	✓	✓	✓

Security controls	Value	NIST SME quick-start	NCSC Small biz guide	ACSC Essential 8	Belgian small guide	Victoria law	CERT NZ	IASME cyber essentials	ENISA SME sec guide	Singapore Cyber Essentials	CIS criticals	ISO SME guide	ISO/IEC 27001
Assurance: reviews, checks, tests, oversight/supervision, audits, certification	M							✓			✓	✓	✓
Physical security	L	✓			✓				✓	✓			✓
System administrator rights	H			✓	✓			✓		✓			
Apps inc. Office	L			✓						✓	✓		✓
Change management, version control, authorisation & record-keeping, asset inventory	M										✓	✓	✓
Compliance with applicable & relevant laws & regulations *e.g*. privacy & data protection	L						✓				✓		✓
Governance & risk/security management, policies, asset ownership, classification, performance & capacity *etc*.	L	✓										✓	✓
Logs, alarms, alerts	M						✓			✓	✓		✓
Social engineering, phishing, BEC & fraud controls	H		✓			✓	✓						
System security, hardening, configuration	M					✓				✓	✓		✓

Security controls	Value	NIST SME quick-start	NCSC Small biz guide	ACSC Essential 8	Belgian small guide	Victoria law	CERT NZ	IASME cyber essentials	ENISA SME sec guide	Singapore Cyber Essentials	CIS criticals	ISO SME guide	ISO/IEC 27001
Third party & vendor risk & security management, contracts, agreements, outsourcing, pro services	L								✓		✓		✓
Email security	M									✓	✓		✓
Intellectual property, licensing	L							✓		✓			✓
Knowledge sharing	L								✓				✓
Cryptography: encryption, authentication, hashing, keys …	L												✓
Insurance	L							✓					
Secure software engineering, development, implementation & maintenance	L												✓

ACSC - Australian Cyber Security Centre

The Australian Government’s Essential eight reduces cyber security to a simple, short checklist of just 8 arbitrary controls. It is aimed at getting organisations started on the process of securing their information.

Arguably, that’s better than nothing … but naturally we believe this SME guideline is better still. In particular, the risk-based approach gets around the danger of implying that ‘just doing these 8 things’ makes any organisation secure, since the risks and hence security needs vary widely between organisations.

Belgium – Centre for Cybersecurity

The Centre for Cybersecurity Belgium is Belgium’s national authority for cybersecurity, supervising, coordinating and monitoring application of the Belgian government’s cyber security strategy. Their CyberFundamentals Framework, developed to satisfy the requirements of NIS 2, is “a set of concrete measures to protect data, significantly reduce the risk of the most common cyber-attacks, and increase an organisation's cyber resilience”. The CyberFundamental starting level Small is intended for micro-organisations and other SMEs with limited technical knowledge.

CERT - Computer Emergency Response Teams

A coordinated global network of government-backed organisations assists businesses in crisis, typically due to cyber security incidents such as malware, hacks and privacy breaches. Many CERTs offer guidance specifically for SMEs which comprise a majority of their clientele, since larger organisations generally have their own incident response arrangements. An example is this set of 11 security tips for SMEs on the Own Your Online website from CERT NZ.

CIS - Center for Internet Security

CIS describes itself as “an independent, nonprofit organization with a mission to create confidence in the connected world.” CIS promotes 18 critical security controls and offers free methods, tools and hardened operating systems to analyse risks and improve IT system security - albeit primarily for large, mature US organisations.

Defining Reasonable Security encourages business leaders to address rhetorical questions such as what is the scope of our mission, obligations and stakeholders? Do we know what is connected to our systems and networks? Do we know what is, or is trying to, run on our systems and networks? Do we understand the data on our systems and the relative sensitivity? Are we limiting and managing the number of people who have privileges on our systems and networks? Have we established processes for reviewing the health of our networks, training employees and recovering from possible breaches? What are our gaps and what risks do they pose? The CIS guide covers 6 areas: know your environment, account and configuration management, security tools, data recovery, security awareness, and business processes and outsourcing.

DFS – New York State Department of Financial Services

DFS offers a cybersecurity program template (outline) to help small licenced financial services businesses with less than 20 people comply with the DFS Cybersecurity Regulation.

It covers: IT asset inventory; cybersecurity risk assessment; third party service providers; access privileges and management, including MFA and VPNs; data retention and disposal; cybersecurity awareness training; incident response and reports; and 15 policy areas.

ENISA - the European Union agency for cybersecurity

ENISA has been assisting SMEs particularly since COVID struck. Their SME Cybersecurity Guide recommends working on 12 areas: cybersecurity culture, training, third party management, incident response planning, systems access, device security, network security, physical security, backups, cloud, online security and knowledge sharing.

Among others, ENISA also offers guidance on NIS 2 compliance for the critical infrastructure sectors, including the few SMEs that are directly in-scope of NIS 2, and the far larger number in the supply chains for critical infrastructure organisations in Europe.

European DIGITAL SME Alliance

Small Business Standards is an association representing European SMEs' interests in standardisation at the European and international levels.

DIGITAL SME is a member of SBS representing ~45,000 European digital SMEs.

The SME Guide on Information Security Controls covers 16 areas: asset management; information classification; policies; incident management; access control; network security; vulnerability and threat management; malware; backups; remote working; awareness; privacy *etc.*

GCA – Global Cyber Alliance

This nonprofit organisation offers Cybersecurity Toolkit for Small Business consisting of "a series of toolboxes, each with tools and reference materials that address a specific cybersecurity area" – namely: ICT devices and applications; passwords and two factor authentication; updates, patches and vulnerability management; email authentication and brand monitoring; phishing and malware prevention; data backups and recovery.

"Each tool is organized and described in a way that makes it as easy as possible for people with limited cybersecurity knowledge to understand the risks and select the right tools. The tools were selected because they address the highest standards in cybersecurity recommended by the Center for Internet Security, the UK's National Cyber Security Centre (NCSC) and Australian Cyber Security Centre (ACSC)."

IASME - Information Assurance for SMEs consortium

Based in the UK, the IASME consortium works through an international network to advise and certify organisations in cyber security, counter fraud, risk management and governance. Its standards are affordable and achievable for SMEs. Certification (either by verified self-assessments or technical audits) is an option for SMEs that are looking to provide assurance regarding their cyber (IT and network) security arrangements, perhaps to qualify for UK government work.

IASME Cyber Baseline concerns technological security measures applicable to every business. The standard (free!) has mandatory requirements across 8 core disciplines (organisation, assets, secure architecture, people, managing access, technical intrusion, backups and resilience) plus a further 5 discretionary guidelines (planning information security, legal and regulatory landscape, physical and environmental protection, policy realisation and secure business operations).

IASME Cyber Essentials concerns defences against the most basic types of cyber attack that an SME will face. It supposedly represents the UK government's minimum requirements for cyber security. Organisations seeking certification self-assess their status against 5 security controls, and their responses are verified by qualified assessors. Cyber Essentials Plus increases assurance through auditing *i.e.* a technical assessment and verification of the implemented controls.

IASME Cyber Assurance - builds on the essential controls of IASME Cyber Baseline or Cyber Essentials, providing assurance as to the privacy and data protection measures taken by an SME. There are two levels to the standard. Level one focuses on the management of physical and human resources, physical security and data protection requirements alongside incident response when things go wrong. Level two requires independent auditing of the processes for additional assurance.

ICO - UK Information Commissioner’s Office

The ICO is the UK government watchdog for privacy and related matters. It handles privacy registrations, complaints, breaches *etc*. and dispenses advice on privacy - such as a privacy notice generator tool and other privacy guidance for SMEs.

ISO - International Organisation for Standardization

ISO is an independent, non-governmental, global organisation that develops and publishes international standards covering various aspects of technology, engineering, industry and business. These standards ensure consistency, safety, interoperability and quality in products, services and management systems across the globe - thousands of ISO standards touching everyday aspects of modern life.

ISO publishes numerous standards concerning information security, business continuity, risk management and related areas, some developed in conjunction with the International Electrotechnical Commission, Cloud Security Alliance, ISACA and others:

ISO/IEC 27001:2022 - defines requirements for scoping, planning, implementing, maintaining and continuously improving an Information Security Management System. The standard offers a set of 93 generic information security controls to be used as a checklist, ensuring that nothing important gets forgotten. Although it is intended to apply to all organisations, in practice ISO/IEC 27001 is often seen as overkill for SMEs … but the fundamental principles (such as the systematic risk-based approach) are sound and proven, underpinning adaptive SME security.

ISO/IEC 27001:2022 - Information security management systems - A practical guide for SMEs is a new (2024) handbook from ISO, supporting SMEs developing and implementing ISO/IEC 27001 information security management systems.

ISO 22301:2019 - similarly defines requirements for planning, implementing, maintaining and continuously improving a Business Continuity Management System. The purpose of a BCMS is to identify risks, prepare for emergencies, continue essential business activities if possible, and if not recover as soon as possible from disruptive events to the organisation.

ISO 31000:2018 - a framework of generic processes for managing all kinds of risks affecting your organisation, systematically again.

London Cyber Resilience Centre

The Cyber Resilience Centre for London is one of nine UK regional centres helping SMEs and third-sector organisations (charities, voluntary and community groups) reduce their vulnerability to cyber-crime. Among other resources, they offer leaflets on: staff training; strong passwords; 2 step/multi-factor authentication; phishing; patching/software updates; and backups.

NIST - National Institute for Standards in Technology

NIST is a federal agency within the US Department of Commerce providing, promoting and maintaining measurement and technology standards. NIST technical standards are well respected and used globally, not just in the US. They are good practices, de-facto building blocks for organisations to adapt to their specific needs.

CSF - Cyber Security Framework - the original NIST CSF was released in 2014 to guide organisations on the comprehension and communication of risk. A decade later, ‘quick start guides’ were added to highlight content designed for various types of organisation, including SMEs.

Special Publication 800 series - the SP-800 series is a large and growing collection of guidelines, frameworks and controls supporting the US Federal Government’s cyber and information security needs. NIST SP 800-53, for instance, provides a comprehensive and popular catalogue of security and privacy controls. The SP-800 standards are well-written, actively maintained and free of charge. Although they are intended for large organisations, the quality and depth of coverage makes them valuable in-depth references.

NCSC – UK National Cyber Security Centre

The NCSC matured from the Information Assurance wing of GCHQ, becoming the UK's technical authority on cyber security, supporting UK plc to become safer and more secure. NCSC guides and resources support SMEs undergoing information security initiatives such as the one outlined in this guideline or the IASME approach.

Information for… is a hub of collected knowledge and resources tailored to different types of organisations.

Small Business Guide: Cyber Security offers practical advice for SMEs, micro and small organisations specifically. The guidance promotes just five actionable (and free!) steps to engage with cyber security and protect against cyber security issues commonly faced by SMEs: backups, malware prevention, securing portable devices, password security and avoiding phishing. With written guides, videos and infographics, there's something here for everyone.

10 steps to cyber security promotes: risk management, engagement and training, asset management, architecture and configuration, vulnerability management, identity and access management, data security, logging and monitoring, incident management and supply chain security. Although intended for larger organisations, the principles are relevant to SMEs, possibly as maturity objectives.

Exercise in a box is a versatile free toolkit for a safe environment in which to simulate a cyber security incident eventuating in your business. It is designed to be used by someone who is not a cyber security subject matter expert, offering a choice of 14 scenarios to exercise and improve your incident response capability.

Singapore Cyber Security Agency

The Cyber Security Agency's cybersecurity certification scheme recognises organisations with good cybersecurity practices protecting their operations and customers against cyber-attacks.

Cyber Essentials is a cybersecurity certification for SMEs that are embarking on their cybersecurity journey. Given limited IT and/or cybersecurity expertise and resources, Cyber Essentials prioritises cybersecurity measures needed to safeguard IT systems and operations from common cyber-attacks. The Cyber Essentials mark recognises organisations that have put in place good cyber hygiene measures.

Cyber Trust is a cybersecurity certification for organisations with more extensive digitalised business operations. It is targeted at larger or more digitalised organisations facing greater risks. The Cyber Trust mark reflects a risk-based approach to guide organisations to understand their risk profiles and identify relevant cybersecurity preparedness areas required to mitigate these risks. It distinguishes organisations with good cybersecurity practices and measures that are commensurate with their cybersecurity risk profile.

Victorian Legal Services

Law firms in the Australian state of Victoria are, in effect, expected by the authorities and clients to achieve or exceed minimum cybersecurity expectations – a mix of IT system/technology and procedural/behavioural security controls.

Despite being pitched at SME law firms, basic controls such as security updates, user authentication, access controls, backups, training and incident response are worthy of consideration by *all* organisations.

Unusually, the guidance covers controls against phishing or business email compromise attacks involving fraudulent changes to payee bank details.

It also specifies *unacceptable* cyber security practices that could constitute professional misconduct *e.g.* failing to install security updates and patches or available software updates, failing to enable automatic updates or manually check for updates at least fortnightly.

Training courses

There is a cottage industry offering information security and cybersecurity training and individual certification schemes, feeding the global demand for competent and qualified professionals. Aside from technical, in-depth training offered for security specialists and engineers, business-focused courses and qualifications such as SABSA and CISM are worth considering to bridge the gaps between commercial realities and theoretical niceties. General business degrees and MBAs are arguably even more beneficial than cybersecurity or IT qualifications for smaller SMEs, since they can always contract with specialist consultants and advisors or simply take advantage of the huge amount of information available on the Web, most of it free.

SME security advice in languages other than English

French: ANSSI - France’s national cybersecurity agency - published a simple set of 13 questions concerning basic information controls typically used by SMEs *e.g*. backups, software updates, antivirus …

German: DIN SPEC 27076 is a free German standard from Germany’s Association of Small and Medium-Sized Businesses (BVMW), Federal Office for Information Security (BSI), Institute for Standardization (DIN) and others. The standard lays out the Cyber Risk Check process for assessing/auditing micro and small organisations for the presence of basic cybersecurity controls (responsibilities for information security, backups, firewalls *etc*.), through a set of ~50 questions. The German government will subsidise up to 50% of the cost for consultants to generate Cyber Risk Check reports with prioritized security improvement recommendations.

Hint: Google Translate and similar facilities can machine-translate English content such as this guideline into other languages and *vice versa.* Yes, even Latin.

Appendix C: information risk and security workshop

Organise a workshop, team meeting or exercise to consider the organisation's information risks, explore its security improvement goals, talk things through collectively and agree priorities for action:

1. **Goals:** what do we want to achieve - raising awareness of the key threats? Identifying specific vulnerabilities in our IT systems? Brainstorming solutions to bolster our defences? Clarifying the goals helps design a focused and productive workshop.
2. **Who to invite:** collaboration is key! Involve relevant stakeholders, decision-makers and specialists. Invite professional advisors, consultants and contacts if appropriate. Diverse perspectives should address a wider range of information risks.
3. **Book the workshop:** find a comfortable distraction-free space with whiteboards, markers and sticky notes to encourage active participation. Schedule the workshop with enough lead-time for everyone to attend, hopefully.
4. **Identify a facilitator** – someone suitable to guide the discussion towards a productive outcome - possibly you if you have enough expertise in this area (information risk, security *and* workshopping!) and can lead without dominating the debate. If not, find someone better, perhaps a consultant or business mentor. Decide how to capture the debate and any issues or decisions: do you need a scribe or will memories be sufficient?
5. Prepare an **agenda** along these lines:
    a. **Introductions**: something lightweight to set the scene, introduce key concepts and objectives, and clarify the workshop's expected outcomes.
    b. **Information risks**: brainstorm risks such as phishing, malware, privacy breaches *etc*. Categorize or plot them according to their relative likelihood and impact. Touch on the associated threats and vulnerabilities without getting bogged-down in the details or terms. Encourage everyone to share their ideas and concerns – including doubts about the arrangements, the risks and assertions made. Park any discussion about security controls until the next item …
    c. **Security controls**: review existing information security measures in relation to the risks, identifying any priorities for improvement. Again, actively encourage everyone present to engage in the process while respectfully considering others' perspectives, concerns and wishes.
    d. **Action plan/next steps**: prepare a rough plan with tasks and responsibilities across the organisation and realistic timescales. Invite all those responsible to acknowledge that the plan is a reasonable starting point, subject of course to resourcing, other activities, priorities and changes – important details that have yet to be determined.
6. **Promote the workshop:** emphasise the business value of addressing information risks. This might seem technical to some, or perhaps a compliance issue to be left to the lawyers, whereas framing it as a business imperative for the entire SME engages everyone. Let colleagues know this workshop will equip them with the knowledge to protect themselves, their work and, ultimately, the entire organisation plus its supply chain. Keep it simple and engaging, avoiding jargon. Spark their curiosity with some thought-provoking questions such as "What *is* our most valuable information?", "What are our main information dependencies?" or "How secure are our remote and home working practices?" to pique interest and get people talking. Send out reminders a few days ahead.
7. **Hold the workshop** then circulate workshop notes and the action plan as a draft for comment. It may not be 'done' but recognise and celebrate progress made!
8. **Organise follow-up activities** if appropriate *e.g.* meeting reports/notes, further workshops, focus groups, security reviews and studies, planning/budgeting meetings …

Appendix D: information risks

‘Information risks’, meaning ‘risks relating to or involving information’, are all around us. Incidents (commonly tagged ‘cybersecurity’ by journalists) frequently hit the news headlines. However, you may not appreciate just how diverse and challenging they are. Here are some example information risks to set you thinking …

Confidentiality risks: attacks by cybercriminals, hackers or spooks; evasion or disabling of access controls; inappropriate disclosure, interception or theft of sensitive information; inappropriate/unethical/illegal exploitation of intellectual property; inappropriate surveillance; leakage of sensitive information via third parties; … plus other unauthorised and inappropriate access to or release of sensitive information.

Integrity risks: bad advice, bad decisions; bias, discrimination and prejudice; bribery and corruption, including IT system/data corruption; bugs; change management/change and version control issues; communications errors; compliance or conformity failures; damaging cyberattacks; deceit, deception; delusions, hallucinations, excessive creativity, logical errors, fallacies; design flaws; ethical failures; falsification, fakery, counterfeiting and piracy; fragility; fraud; malware infection; misattribution. misclassification, misdirection, dis/misinformation, misinterpretation, misunderstanding, misleading, mistranslation; inaccurate, incomplete or out-of-date information; stretching the truth, bending the rules; unauthorised modification, destruction or replacement of information; zero-day exploits; … plus other causes of inadequate accuracy, completeness, relevant and timeliness of information.

Availability risks: corruption or loss of valuable/vital business information; cybertage – sabotage of IT equipment, media or data; defection of knowledge workers to competitors; delays and interruptions to information services; denial-of-service attacks plus unintentional disruptions; dependencies; destructive cyberattacks and other seriously disruptive incidents; gradual or sudden loss of information; hardware, software, system or service failures; health and safety issues/incidents; human errors and mistakes; inadequate capacity and performance resources; natural events and accidents; physical attacks involving the use of destructive weapons against people and facilities; power cuts, brownouts, surges, spikes *etc*.; unrecognised, unnoticed or unappreciated incidents; unreliability and unpredictability in general.

Other risks: advanced malware from spies and spooks; breaches of contracts, agreements and understandings, broken promises; carelessness, negligence, thoughtlessness; changes in the risk landscape, technologies, business *etc*.; collisions, conflicts and delays in overloaded networks or systems; covert backdoors or loopholes; exploitable architectural or design flaws; inability to access and use/administer systems, data, facilities, people *etc*.; inadequate risk management *e.g*. excessive risk-aversion, unowned risks; incompetence and negligence; ineffective controls; inept or incompetent information security management and governance failures; information overload; insider threats; knowledge gaps; limited creativity, lack of innovation; loss or theft of security tokens and passwords; misconfiguration, misidentification and misuse of information; noncompliance and nonconformity; overload, stress, burnout; paranoia, irrational fears and anxieties; perfectionism and procrastination; personal issues affecting cognitive capabilities, recall, performance and judgment; rogues; security control failures; social engineering, social factors, social media and social interactions; supply chain issues, breaches, incidents, disruptions …; toxic cultures, dysfunctional relationships; underinvestment; unforeseen/unexpected events and challenging situations; unreasonable resistance to change; untrustworthy partners; unworkable rules, requirements or expectations; vagueness and uncertainty in general; war, terrorism and extremism; … others, including unknown unknowns!

Protecting against *all* those risks simultaneously is extremely challenging … so it makes sense to identify and prioritise ‘key risks’ from this long and yet still incomplete list.

Appendix E: iterative risk analysis

This risk analysis process or method blends risk, security, incident and problem management, creatively combining imaginary with actual data and concerns:

1. Imagine you have experienced a 'typical' incident affecting whatever [information] asset/s you are risk-assessing - such as a physical incident affecting the office. Consider various types of incident of differing scales and importance *e.g*. an office break-in, vandalism, professional hit, insider theft, fire, flood ... whatever. For now, pick out whatever type/s of incident seems most likely and/or damaging for further consideration - not least, real incidents that have occurred (this analysis might follow an actual incident for maximum reality!). Start exploring the associated threats, vulnerabilities and impacts, using information about actual incidents under similar circumstances to inform your analysis - or wing-it using common sense. This step initiates the risk analysis, clarifying the asset/s and risks of most concern. Press ahead ...

2. Following this imaginary incident, how would you know what had occurred? What indications would there be of the incident? How soon would it be discovered? When, by whom and how? Consider the possibility of gradual/non-obvious incidents (*e.g*. overloaded smouldering power cables, or where everybody is busy and assumes someone else is responsible), deliberately concealed incidents (*e.g*. worker thefts) and incidents with little if any indication (*e.g*. intellectual property theft - spying). This prompts you to think about detective controls *e.g*. alarms, warnings, indicators ...

3. What would your immediate reactions be? What would you do first? Who would need to be involved? What would you need to make that work well? Use the incident scenario to explore/improve your incident response plans and preparations. Consider a desktop walk-though or an exercise to check them out more realistically.

4. How would you investigate and resolve the incident? Again, consider who, what, when, how, why ... What information and skills would be essential or most valuable for the investigation (*e.g*. records, logs, CCTV footage, forensics, fire investigators)? Also, what could/would you do to minimise the damage and get things back to normal ASAP? What would be the priorities for the business? This step extends/deepens your exploration of the incident response, including the corrective controls and a little Business Impact Analysis for good measure.

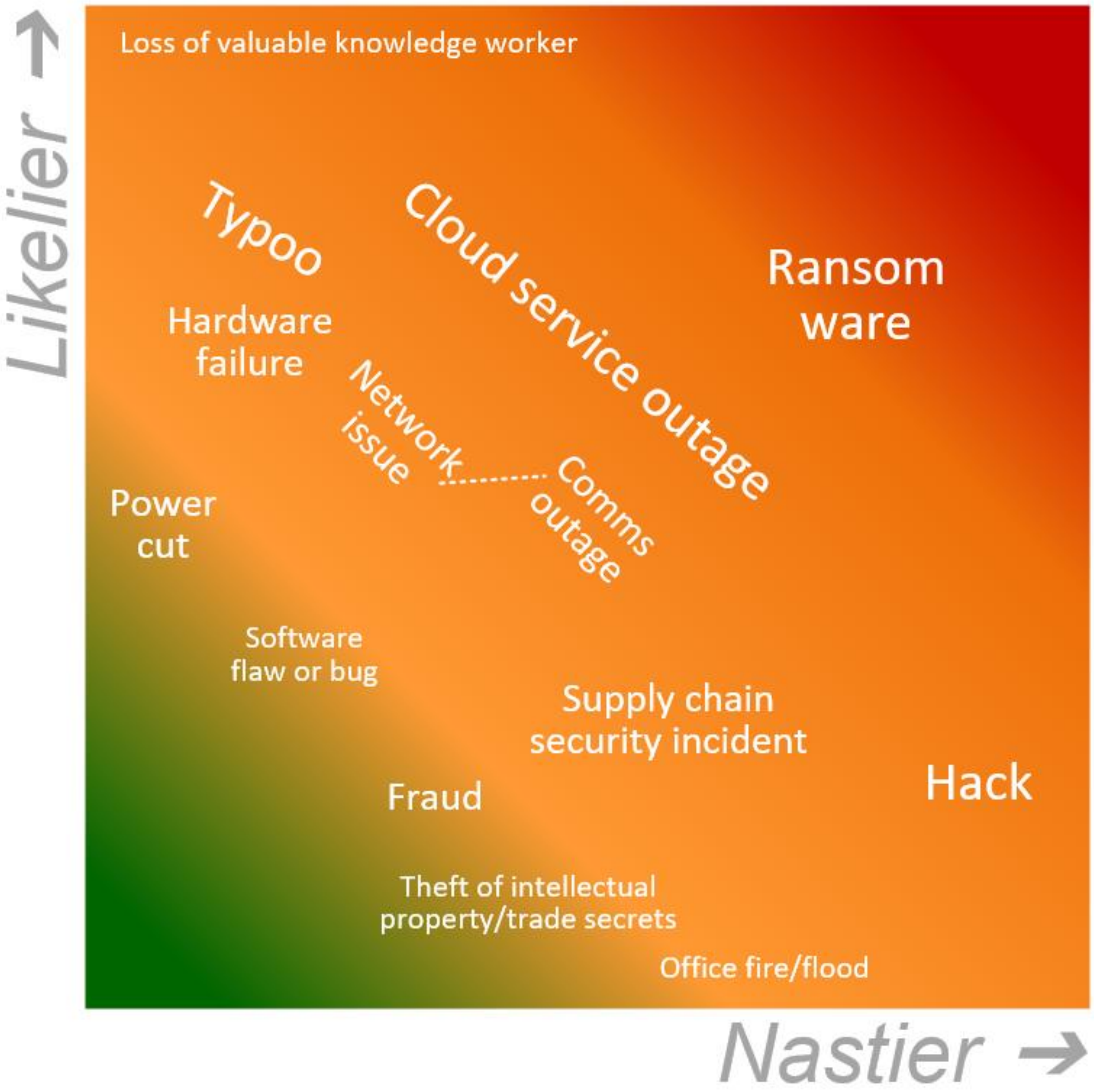
5. Thinking back to step 1, is the incident worrying enough to improve the preventive controls? What else can/should be done to prevent the incident and others affecting the same asset/s, reducing the threats, vulnerabilities and/or impacts. Estimate how much disruption and cost this imaginary incident would have caused, roughly - minor expense and inconvenience, big trouble, expensive repairs, compliance penalties, business failure, death and destruction, cataclysm ...? Apart from workers and the organisation/business itself, who else would/might have been materially affected (*e.g*. other residents of the same burnt-out building; customers; authorities; passers-by)? How long would these problems persist? Given even an approximate frequency of occurrence of this particular incident or of similar incidents (*e.g*. once a day, once a week, once a year, once a decade ...), this assessment may be enough to justify investing in implementing or improving cost-effective preventive controls, or at least consider the possibilities, pose other questions and gather more info to firm-up the details, particularly for large/unusual investments or where the benefits are marginal or dubious.

6. Lather, rinse, repeat. Pick other possible incident scenarios, assets, *etc.* on each run through the cycle. Risk management is a never-ending quest for perfection, particularly as things keep changing and risks can never be totally eliminated. Keep on knocking-over the biggest risks, time after time.

Appendix F: qualitative risk analysis PIC

This intuitive method simply involves identifying and then plotting risks relative to each other on a colour-coded **P**robability-**I**mpact **C**hart. Although this can be done by someone working independently, a team effort such as a risk and security workshop can increase the range of risks considered, tease out issues and concerns, deepening and generally improving the quality of the analysis. Thought and debate are essential parts of this, arguably even more valuable than the PIC itself which is merely a way to capture and share the analysis.

Here is an example **PIC** plotting an SME's information risks according to their relative likeliness (probability) and nastiness or business significance (impact).



Note: this **PIC** is merely a generic illustration of the approach for inspiration: your SME's information risks undoubtedly differ.

Appendix G: example registers

Example risk register

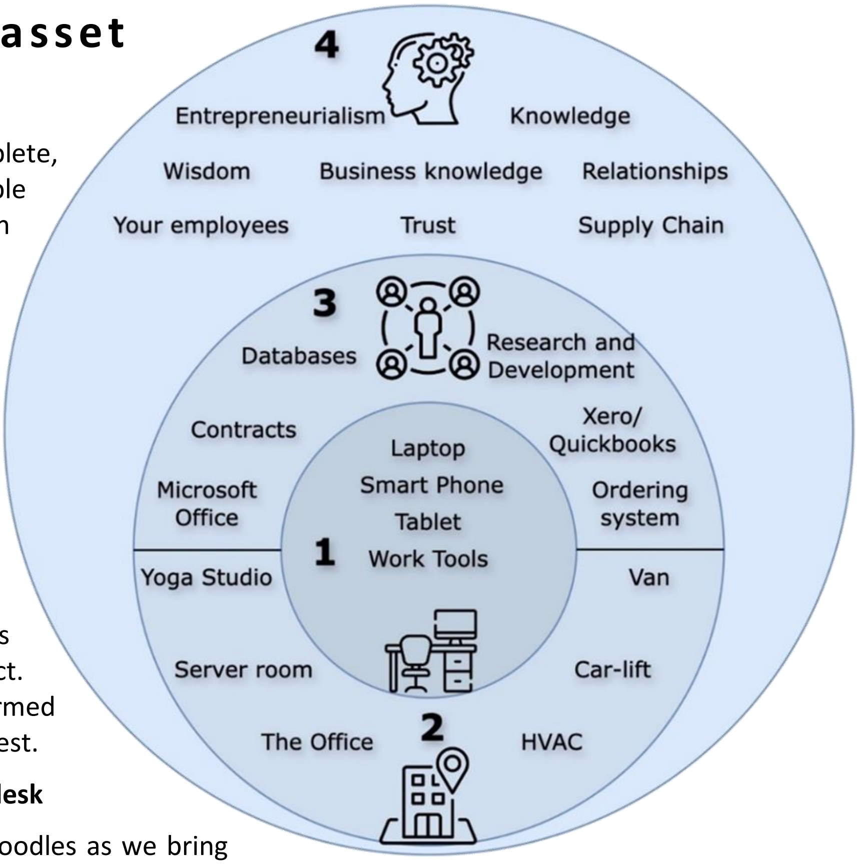
Compiling and maintaining a risk register, list or database is a helpful way to collate and manage risks and controls. Your SME may already have something, perhaps covering commercial, health-and-safety, financial or other risks. Incorporating all manner of risks into a consolidated master risk register has the benefit of comparing and contrasting the risks on an even basis according to their relative likelihoods and impacts, and facilitating their management as a complete, prioritised set. If that is a step too far, developing an information or cyber risk register may be a worthwhile pilot.

Here is a simple example of an **information risk register**. In the form of a spreadsheet, you can add as many rows and columns as you need, define parameters, add statistics, develop macros for sorting and colour-coding *etc.* Other example registers follow if a more comprehensive approach is needed … but remember these registers are primarily a decision-support tool for risk management. However much you try, you can never completely eliminate the uncertainties behind risk, so don’t get carried away with the technology!

					Risk level				
ID	Title	Owner	Likelihood	Impact	Raw	Current	Treatment[4]	Checked	Comments
R1	Ransomware	IT Mgr	H	H	H	H	M & S	2024 Jan 16	Phishing remains a concern
R2	Intellectual property theft	CEO	M	H	H	M	M	2024 Jan 16	Intense competition can flare up if relations with unethical peers deteriorate
R3	Loss of key workers	HR	M	H	H	M	M	2024 Jan 16	Retention, training, profit sharing
R4	Errors, mistakes	CEO	H	M	H	L	A & M	2024 Jan 16	Always a possibility ☺
R5	Hacks	IT Mgr	M	M	M	L	M	2024 Jan 16	Network & system security controls
R6	Power cuts	Property mgt	L	H	M	L	M	2024 Jan 16	Cloud services, laptops & mobile access
R7	Comms failure	Telco	M	M	M	L	S	2024 Jan 16	Comms contracts & diverse comms options
R8	Major storm/flood	Property mgt	L	H	M	L	A & X	2024 Jan 16	Located away from riskiest areas

[4] M = Mitigate; S = Share; A = Avoid; X = Accept

Example information asset register



An asset register is a reasonably complete, accurate and up to date account of the valuable items owned by the organisation or placed in its custody. When the business seeks to protect, exploit and enhance the assets, it helps enormously to know details such as what and where they are, who owns them, and how much they are worth - even if ours is a micro-SME whose main assets are an old laptop and a well-used smartphone!

Information assets aren't entirely physical or technological: intangible information content such as intellectual property, trade secrets, strategies and brands can be as valuable, sometimes far more valuable in fact. Again, understanding the assets enables informed decisions about what controls will serve us best.

Come with me on a virtual journey at your desk

Scribble down some notes, mind-maps or doodles as we bring our first asset register into being:

1. Picturing our SME as a machine, point at all the different parts and consider what they contribute to the whole. Start with the things we use every day at our workspace - laptop, phone, notebook, internet router … What do we need to keep the machine working? What pieces would we miss the most if they were broken, and why is that?
2. Zoom-out for a broader view of our workplace - premises, power and comms cables. What are the infrastructure services that fuel the machine?
3. Now zoom out even further to visualise the relationships between the SME and other parties, such as the banks holding our financial assets, and data centres in the cloud holding some of our information assets. Who are they? Where?
4. Lastly, zoom back down to ground level to think about the real talent that exercises all these assets – us and our team! Our knowledge, business acumen, expertise and experience are intangible information assets that fuel and lubricate the machine. For many SMEs, our creative and innovative capabilities are our crown jewels, our unique business advantages that others cannot readily steal or replicate.

If we capture everything important in this mental model we've made, we'll have an asset register – a starting point at least. Some examples follow …

Example *information* asset register

ID	Description	Location	Owner	Controls	Retention	Classification	Checked	Comments
D1	Proposals, project costings	Google Drive	Project leader	Password, biometrics	To end of contract (if awarded)	Company confidential	2024 Jan 10	
D2	Contracts	Google Drive	CEO	Password, biometrics	End of contract +5 years	Client confidential	2024 Jan 10	
D3	Client documentation	Google Drive	Client	Password, biometrics, encryption	To end of contract	Company confidential	2024 Jan 10	Includes client-supplied content & deliverables (draft & final)
D4	Internal materials	Google Drive	Project team	Password, biometrics, encryption	To end of contract or indefinite	Company confidential	2024 Jan 12	Drafts, templates, research materials, project plans, reports. policies, procedures *etc*.
D5	Deliverables	Google Drive	Project leader	Password, biometrics, encryption	To end of contract +1 year	Company confidential	2024 Jan 12	Final/accepted deliveries to clients
D6	Business contacts	Smartphones	All	Password, biometrics	Indefinite (dynamic)	Personal	2024 Jan 13	Contact details for employees and various third parties
D7	Brand	Public	CEO	Marketing	Indefinite	Company confidential	2024 Mar 12	Client feedback, reviews, perceptions, focal points …
D8	Contracts, notice of award, notice to proceed	Red folder	CEO	Lockable cabined in private office	In perpetuity	Company confidential	2024 Jan 10	

Example *hardware* asset register

ID	Description	Serial number	Owner	Key controls	Checked	Comments
H1	Dell XPS 15	2551333950	A.D. (co.)	Fingerprint, antivirus, firewall, cable lock	2024 Jan 17	Windows Defender, Avast Antivirus - Free
H2	Apple MacBook Pro	AX1124D21	C.C. (co.)	Fingerprint, antivirus, firewall, encryption	2024 Jan 17	
H7	Dell 7010	A-CSD-SSS-2171	CEO	Encryption, backup regime	2024 Jan 17	
H8	CISCO small business router	CD-112a-000124	Co.	Basic firewall	2024 Jan 17	Outdated, insecure, needs replacing

Example *software* asset register

ID	Description	Purpose	Value	Supplier	Controller[5]	Version	Support	Checked	Comments
S1	AWS - IAM	User and access management	H	AWS	A.D.	Cloud	Yes	2024 Feb 12	IAM = Identity and Access Management
S2	AWS - S3	Data storage	H	AWS	A.D.	Cloud	Yes	2024 Feb 12	S3 = Simple Storage Service
S3	Dropbox	Cloud storage and digital signatures	L	Dropbox	C.C.	Cloud	60%	2024 Feb 12	Maintenance limited to security updates
S4	Workspace	Office apps	H	Google	C.C.	Cloud	90%	2024 Feb 12	Gmail, Meet, Drive, Docs, Sheets

[5] Typically, the person or group with administrator/full access

Example *compliance* register

In a similar fashion, this example shows a basic compliance register listing an SME's main **L**egal, **R**egulatory and **C**ontractual obligations relevant to information risk and security:

ID	Title	Type	Authority/owner	Evidence of compliance	Compliant	Checked	Comments
C1	Privacy Act	L	National Privacy Commission	Certificate of registration	100%	2024 Jan 17	
C2	Labor code	R	Department of Labor and Employment	Certificate of registration	80%	2024 Jan 17	Changes since last registration to be checked and notified prior to next
C3	eCommerce Act	L	Department of Trade and Industry	Certificate of registration	100%	2024 Jan 17	
C4	Sales contract XYZ1	C	CEO	Contract manager & client checks	70%	2024 Jan 17	Delayed deliveries caused by client issues: records kept
C5	Employment contracts	C	CEO	Review annually at bonus time	90%	2024 Jan 18	A last resort: maintaining cordial staff relations is business-critical

Appendix H: glossary

- **Accountability**: the possibility of being sanctioned by an authority for failing to fulfil obligations to them.
- **Assurance**: monitoring, checks, reviews and audits to increase confidence in the arrangements.
- **Authentication**: confirming that something is authentic, true, real.
- **Availability**: able to be used for legitimate purposes.
- **Awareness & training**: complementary techniques to help people understand, become more competent, learn new skills …
- **BIA** (**B**usiness **I**mpact **A**nalysis): in business continuity management involves exploring the possible causes of serious operational disruption.
- **CIA (C**onfidentiality, **I**ntegrity, **A**vailability**) triad:** security is largely about protecting these 3 characteristics.
- **Compliance**: fulfilment of legal, regulatory or contractual obligations – increasing the possibility of penalties such as fines and closer supervision.
- **Confidentiality**: secrecy, sensitivity.
- **Conformity**: satisfaction of informal personal, corporate or societal requirements, including ethical expectations.
- **Consequential costs:** costs incurred indirectly and/or subsequently as a result of, or triggered by, an incident.
- **Control**: a means to prevent inappropriate or unwanted activities, actions and outcomes, while permitting or facilitating the converse.
- **Cyber**: generally refers to IT, especially computer systems or devices connected to or accessible from the Internet.
- **Data**: generally means digital/computer data, but can mean other forms of information such as results from a research study.
- **Direct costs:** costs and losses directly incurred, caused by and attributable to an incident.
- **Distribution:** mathematical description for the spread of data points on a graph *e.g*. a 'normal' distribution is the familiar 'bell curve'.
- **Event**: generally a small, insignificant occurrence that may signal or accumulate/build into an incident.
- **Externalities**: effects outside/beyond the boundaries of a system, organisation or situation affecting third parties, perhaps society at large.
- **Governance**: overall arrangements to direct, monitor and control the organisation's activities.
- **Impact**: the adverse consequences of an incident on the affected party or parties – the harm, damage, costs.
- **Incident**: a serious event that causes substantial impacts.
- **Incident investigation**: exploring the nature, timeline and causes of an incident, mostly to learn what went wrong so it can be fixed.
- **Incident management**: planned, systematic activities to prepare for, investigate, contain, recover and learn from an incident.
- **Incident resolution**: that part of incident management involving containing and stopping any further damage resulting from an incident.
- **Incident response:** the process and team called-on to deal with (investigate and resolve) incidents.
- **Information**: an expression of knowledge that has meaning and value.
- **Information management**: the planned collection/creation, storage, organisation, analysis, use and control over information, overall.
- **Information processing**: communicating/sharing/analysing information by any means using IT, mentally or mechanically (remember slide rules?).
- **Integrity:** completeness, accuracy, relevance, timeliness and reliability or trustworthiness, or the lack of disruptive forces, errors, omissions *etc*.

- **Lifecycle cost**: ‘concept to coffin’ investments and costs incurred during the entire life of a system, control *etc*., from specification to retirement.
- **Likelihood:** probability, possibility, potential.
- **Medium-sized organisation**: an SME with up to about 250 employees.
- **Micro-organisation: a** tiny SME with a handful of employees, perhaps just the 1 (owner-operator, sole trader).
- **Opportunity cost**: given limited finances or other resources, investing in some things means not investing in others, losing out on their benefits.
- **PIC** (**P**robability **I**mpact **C**hart) or **PIG** (**P**robability **I**mpact **G**raphic): see appendix F.
- **PKI** (**P**ublic **K**ey **I**nfrastructure): a cryptographic system involving complementary pairs of keys, one of which is public while the other must remain private.
- **Policy**: objectives and rules laid out and mandated by management.
- **Privacy**: confidentiality and control of personal information, plus other aspects such as dignity, personal space, choices.
- **Quantify**: measure, determine the amount.
- **Recovery**: getting back to normal following disruption or interruption.
- **Reliability:** the extent to which something (such as a system, network, person or control) can be trusted to perform as expected or required.
- **Resilience:** robustness, stability, dependability, continuity …
- **Responsibility:** expectation of an individual *e.g*. to ensure that an asset is properly protected and legitimately exploited.
- **Risk:** the probability that bad things might happen, coupled with the consequences. “The effect of uncertainty on objectives” (ISO 31000).
- **Risk acceptance:** living with, rather than mitigating, sharing or avoiding, a risk. May be an explicit decision, implicit or by default/ignorance.
- **Risk assessment & risk analysis**: systematic study of risk in more or less detail (these similar terms are inconsistently defined and used).
- **Risk aversion:** a general reluctance to accept, or fear of, risks.
- **Risk tolerance:** a general acceptance or desire to take risks.
- **Security**: the probability that incidents will not happen, or if they do, they will not be bad.
- **Small organisation**: an SME with up to about 50 employees.
- **SME**: **S**mall to **M**edium-sized **E**nterprise (includes micros).
- **Threat**: something hazardous or dangerous, capable of impinging upon and harming the object of analysis *e.g*. a person, process or system.
- **Trust**: the implicit anticipation or expectation that something or someone will act in and protect/promote the trusting party’s best interests.
- **Trustworthiness**: the extent to which something or someone is truly worthy of being trusted - an integrity property.
- **Uncertainty**: the inability to predict future events with total accuracy and precision. Increases markedly with complexity and time horizon.
- **Utility**: usefulness (adjective). Supplier of electricity, phones, water, waste disposal *etc*. (noun).
- **Value:** a measure of how much something is worth to its owners, possessors, competitors, adversaries, society *etc*.
- **Vulnerability:** inherent weakness or flaw in something that, if exposed, might be exploited by various threats leading to adverse impacts.

Appendix I: about the ISO27k Forum

Since 2006, the **ISO27k Forum** has grown into a supportive and friendly global community of *more than 5,000* information security professionals, most of whom are actively using the ISO/IEC 27000-series information security standards.

The Forum is a **practitioners' group** with a *practical* focus. We mostly discuss matters of interest and concern to those interpreting and applying the ISO27k standards in genuine real-world situations.

Forum members are generally interested in information security standards, willing to help promote the standards more widely and discuss information security management standards, practices, methods *etc*. We are CISOs, ISMs, CROs, compliance managers, information risk and security consultants, IT/cybersecurity specialists, security analysts, incident responders, students, academics and researchers. A few of us are involved in the standards bodies and committees responsible for developing and maintaining ISO27k and other standards – but please don't hold that against us!

The Forum is a self-help ISO27k-user community that thrives on proactive involvement of its members. We are encouraged to ask on-topic questions, raise concerns, discuss challenges, offer answers, share tips, debate topical issues and so forth. Sharing is important to us or, as one of our members put it:

"We are a TEAM – **T**ogether **E**veryone **A**chieves **M**ore".

This SME guideline is an example of what the community achieves through selfless collaboration and teamwork – one of several goodies offered *for free* in the ISO27k Toolkit.

To join the Forum, please apply through www.iso27001security.com/html/forum.html It is also free. No charge.