

Information security controls for Small to Mid-sized Enterprises (SMEs)

DRAFT

30th September 2026

Contents

Introduction and scope	2
SME1 Accounts	2
SME2 Patching	3
SME3 Malware	3
SME4 Backups	4
SME5 People	4
SME6 Networks	4
SME7 Devices	5
SME8 Incidents	5
SME9 Internet	6
SME10 Physical.....	6
SME11 Servers	6
SME12 Inventory	7
SME13 Scams	7
SME14 Applications.....	7
SME15 Compliance	8
SME16 Privileges	8
SME17 Assurance	8
SME18 Suppliers	9
SME19 Monitoring	9
SME20 Governance	10
SME21 Cryptography	10
SME22 Knowledge	10
SME23 Insurance	11
SME24 Development	12

Introduction and scope

Small to Mid-sized Enterprises (SMEs) are organisations with up to about 250 people, including micro-SMEs ('solopreneurs') and tiny family businesses. As such, resources are tight, particularly in deep technical areas such as information or cyber security. However, all organisations rely on information. We all face information risks that deserve to be addressed. This document explains what and how.

The SME controls are drawn from numerous published SME information security guidelines. The SME controls recommended most often appear first in the list. However, the risks, control requirements and technologies vary markedly between SMEs, so it is your responsibility to determine:

- which controls would work for your SME;
- whether your existing controls are adequate or deserve improvement;
- what those intended improvements are, plus how, when and by whom they are going to be made.

To assist with that process, each SME control has:

- a convenient one-word **title**;
- a **summary** outlining the control in plain English;
- a **justification** briefly explaining why the control is even worth considering, the business benefits it is intended to deliver;
- **implementation notes** to help adopt the control in practice – either task your IT, cloud and other service providers to 'make it so' or tackle it yourself (your choice);
- a **reference** to the most relevant information security control from [ISO/IEC 27002](#) (mostly). The standard offers a page of advice on each control.

The SME controls are mutually supportive, collectively comprising a strong yet flexible and adaptable suite, hence there are numerous cross-references. Cybersecurity is a battle with many fronts.

Further guidance on information security controls is available from professional/trade bodies, peers, partners and suppliers ... plus those published guidelines mentioned earlier. You are not alone!

SME1 Accounts

Summary: allowing certain people to use computer systems means confidently determining who they are and what kind of access they are permitted, locking-out all others.

Justification: since most cybersecurity incidents involve inappropriate access to computer systems, data, applications and services, reducing that risk makes this an important control for organisations of all sizes. Requiring individuals to log-in to computer systems through their personal accounts is a fundamental control, underpinning most others. User accounts link system accesses, access rights and activities to individual people, reducing the possibility of inappropriate access such as hacking, scams [see [SME13](#)] or snooping. If properly configured, automated usage accounting typically records details of logins and certain activities in system security logs [[SME19](#)], providing valuable information for traceability and accountability purposes e.g. proving that someone was - or was not – logged-in to a system at the time a serious incident occurred. Individual user accounts with specified access rights can be protected to some extent using passwords, but **Multi-Factor Authentication (MFA)** markedly strengthens authentication and is recommended for important accounts and systems.

Implementation notes: most computer systems support individual user accounts with unique usernames and some form of user authentication – usually passwords and sometimes stronger approaches such as biometrics (e.g. fingerprints) and MFA (e.g. passwords plus biometrics plus geographic location). Stronger cryptographic authentication [[SME21](#)] is especially valuable for

privileged users [[SME16](#)] and for critical systems and services (e.g. those handling company accounts, financials, safety and compliance [[SME15](#)]). Default passwords should be changed when systems are installed since they are widely known among the hacker community. Access rights vary by system and are best configured for relatively stable user roles (e.g. ordinary user, administrator and manager) which are allocated to suitable individuals. Accounts and access rights are worth checking from time to time, according to how often roles, people and systems change, and the significance of various systems.

Primary reference: [ISO/IEC 27002](#) clause 5.15.

SME2 Patching

Summary: computer systems should be patched promptly when updates are released by the suppliers.

Justification: maintaining currency of computer systems reduces vulnerabilities caused by bugs and design flaws, as well as (often) improving functionality and enabling technical support. Delaying or skipping patches leaves systems vulnerable to attacks, failures and other incidents. The value and cybersecurity of unsupported or unmaintained systems decay over time, becoming liabilities.

Implementation notes: this control is especially valuable for business- or safety-critical systems connected or exposed to the Internet. Hackers and malware [[SME3](#)] can strike soon after patches are announced (so rapid patching reduces that risk) and can continue hunting for vulnerable targets for years (so even unsupported or legacy systems can be vulnerable). Severity ratings by suppliers and advisors can emphasise patches that are particularly valuable from a cybersecurity perspective, although they are naturally reluctant to disclose details that might aid adversaries and discredit their products. Furthermore, the manner in which systems are used, and hence the risks arising from the vulnerabilities, differ between SMEs. SMEs that produce or support systems should have internal arrangements to specify, generate, test and release patches or updates to supported customers, emphasising those with cybersecurity implications.

Primary reference: [ISO/IEC 27002](#) clause 8.8.

SME3 Malware

Summary: antivirus controls help protect against ransomware, viruses, Trojans and worms circulating extensively on the Internet.

Justification: computer servers, desktop computers, smartphones and other devices are vulnerable to malware attacks, with potentially serious and costly business and personal consequences. A ransomware infection, for instance, can prevent access to most if not all the SME's computer systems and services, severely disrupting business for an indeterminate period, perhaps indefinitely if recovery proves impossible. In addition to the business disruption, investigation and recovery costs, extortionate threats to disclose stolen information can devastate an SME's business and finances, even if covered by insurance [[SME23](#)].

Implementation notes: although antivirus software is not a total solution, it is a cost-effective part of the defence against malware. Frequent automated updates through an antivirus service can block new and variant forms of malware quickly. Working in conjunction with user authentication and access controls [[SME1](#)], security awareness [[SME5](#)], patching [[SME2](#)], network security [[SME6](#)], properly configured and maintained antivirus software substantially reduces but still cannot totally prevent malware infections. Therefore, incident responses [[SME8](#)] and immutable backups [[SME4](#)] are also necessary.

Primary reference: [ISO/IEC 27002](#) clause 8.7.

SME4 Backups

Summary: when things go wrong due to incidents, accidents and attacks, backups provide fallbacks – a safety mechanism that facilitates recovery and so keeps the business running with minimal disruption.

Justification: failure or loss of computer systems, networks, information services, devices, storage media and people disrupt dependent information processes and business activities. While small quantities of information may be recovered or recreated manually, that is slow and impracticable in most cases. Current, conventional technologies may be replaced more readily than legacy or custom equipment and specialist cloud or other information services, but thinking ahead and preparing suitable backup arrangements can save time and money in a crisis.

Implementation notes: regular data backups are the key control here, saving copies of digital data to other media and storing them safely – ideally off-line and away from the primary equipment. High-priority data that are business- or safety-critical, change frequently or would be needed urgently following a disruptive incident (such as ransomware [SME3] or a fire [SME10]) deserve to be backed up more frequently, secured more strongly and recovery-tested more often than lower-priority data. A suitable backup strategy [SME20] supported by backup policies, utilities, processes, access controls [SME1] and testing regimes should be prepared, implemented and maintained. In addition, consider backing-up other critical information resources such as computer hardware, power sources, network connections, cloud services, specialists with unique skills and knowledge (e.g. technologists, creatives, managers and accountants) and valuable paperwork (e.g. business records, contracts, licenses and agreements).

Primary reference: [ISO/IEC 27002](#) clause 8.13.

SME5 People

Summary: people qualify as information assets (requiring both protection and legitimate exploitation by the business) and information liabilities (threats to be guarded against e.g. hackers, fraudsters and careless or inept workers).

Justification: whereas cybersecurity is largely a technological concern, it is specified, designed, implemented, operated, managed, maintained and attacked by people.

Implementation notes: directing, supporting, enabling and encouraging workers (employees, contractors etc.) to act in the best interests of the organisation is, arguably, less of a challenge for tight-knit SMEs than for large organisations, but is required nevertheless. Controls include:

- defined roles and responsibilities [SME20];
- binding employment or service contracts;
- policies, procedures and work instructions clarifying obligations and expectations;
- awareness and training;
- management oversight, supervision and monitoring [SME19]; and
- disciplinary processes.

Primary reference: [ISO/IEC 27002](#) clause 6.

SME6 Networks

Summary: securing data, social and business networks requires a combination of technological and procedural or administrative controls.

Justification: few SMEs are totally isolated from and independent of the global Internet, either being directly connected themselves or reliant on third parties that are (supply chains are also networks). Most SMEs also use and depend on social networks for information and business connections. It is therefore appropriate to protect SMEs against significant network threats such as hackers, malware, social engineers and misinformation, actively maintaining secure and reliable network connections with trusted third parties.

Implementation notes: securing data networks involves controls such as firewalls and secure configuration of network routers, wireless networking and other devices (e.g. encrypting network traffic [SME21] and patching [SME2]) and cloud services [SME14]. Securing social networks is largely a matter of guiding workers on what they are expected to do, be wary of and avoid online [SME13], through acceptable use policies and awareness [SME5], with compliance monitoring [SME19, SME15], management oversight and direction [SME20, SME17]. Compliance [SME15] and assurance measures [SME17] are valuable information security controls for supply chains [SME18].

Primary references: [ISO/IEC 27002](#) clauses 8.20, 6.3 and 5.19.

SME7 Devices

Summary: securing computing devices is largely a matter of correctly configuring, using and managing their built-in security facilities

Justification: SMEs typically rely on computing devices such as desktop and portable computers, servers, smartphones, routers, firewalls, building management and industrial control systems, most of which are networked [SME6]. Whether they are purchased and owned by the SMEs or by workers and third parties, devices used by SMEs need to be both capable of being secured (i.e. designed and built for security [SME24]), and securely configured, used and managed in practice. Older equipment and low-quality consumer-grade devices can lack security facilities and technical support, increasing the security risks. A further risk arises from the connection and use of unauthorised (rogue) network devices without appropriate security.

Implementation notes: the security functions built-in to modern-day commercial-grade IT devices and networks [SME6] can generally be configured by non-technical users alone or with advice from the manufacturers and IT specialists. Furthermore, policies, procedures and monitoring can partially mitigate the risks from older, unsupported and rogue devices, including those identified when inventories are checked and updated [SME12]. A better approach is to prevent them becoming problematic e.g. by upgrading, retiring or replacing devices before they become obsolete, and by strengthening network security to block connections from insecure or rogue devices.

Primary reference: [ISO/IEC 27002](#) clause 8.9.

SME8 Incidents

Summary: even strong information security controls can only ever mitigate (reduce) risks, leaving residual risks that may eventuate.

Justification: appropriate advance preparations help to identify, contain/minimise, evaluate and resolve incidents more efficiently and effectively.

Implementation notes: preparing for information security incidents involves gathering and maintaining useful resources (such as incident management policies and procedures [SME5], reliable backups [SME4], resilient and responsive workers, and access to specialist advisors.

Primary reference: [ISO/IEC 27002](#) clause 5.24.

SME9 Internet

Summary: securing an SME's network includes but goes beyond a properly-configured firewall on the main Internet connection.

Justification: although the Internet is an invaluable source of information, commerce, support and information services, its global open-access nature is being actively exploited by a large number of hackers, fraudsters, criminals, spies and other adversaries. Without adequate security, any Internet connection opens the gate wide for attacks and loss of control of internal information.

Implementation notes: securing Internet connections primarily involves a combination of technical network security [SME6] and device security [SME7], authentication [SME1], cryptography [SME21] and worker vigilance [SME13]. To protect every connection, it is necessary to find out about all of them [SME12] and bring them all under control – no mean feat since there are so many possible connection methods and devices to secure.

Primary references: [ISO/IEC 27002](#) clauses 8.29, 8.21 and 8.23.

SME10 Physical

Summary: digital data security controls alone cannot entirely protect tangible computing devices, media and people from attacks and accidents such as fires.

Justification: unrestricted malicious physical access to computer and network devices, cables, storage media, workers and other information assets can bypass or disable most security controls over time, aside from simple theft and criminal or accidental damage. Just imagine having to explain the critical loss of a laptop or paperwork containing sensitive personal and valuable proprietary information, or a dangerous personal safety or environmental incident involving the loss of digital control of equipment, to the news media.

Implementation notes: a suitable blend of physical controls (such as barriers, locks, media safes and procedures) can substantially reduce the risks by avoiding or preventing most physical incidents, while detective and corrective controls (such as alarms, safety interlocks and uninterruptable power supplies) enable workers to respond effectively to the incidents that slip through the net.

Primary reference: [ISO/IEC 27002](#) clause 7.

SME11 Servers

Summary: many SMEs rely on networked servers providing file storage, application services etc. to workers and, via the web, to other Internet users. Protecting the information and services involves securing the servers both digitally and physically against deliberate and accidental threats potentially affecting all the users.

Justification: email, web and application servers are valuable yet vulnerable resources. Anyone specifying, purchasing, using, administering, monitoring and managing the SME's servers (whether employees or external cloud service providers) should ensure the associated risks to information confidentiality, integrity and availability are identified, evaluated and treated appropriately.

Implementation notes: server security controls primarily involve network and Internet security [SME6 and SME9], cryptography [SME21], prompt security patching [SME2], backups [SME4], physical security [SME10] and incident responses [SME8]. Security services offered by external suppliers should be compared to the SME's requirements, ideally before committing to binding arrangements or else during contract renegotiation since the details can change over time, and can have financial implications [SME18].

Primary reference: [ISO/IEC 27002](#) clause 8.27.

SME12 Inventory

Summary: preparing and maintaining lists or databases of the SME's information assets (such as computing devices, information content and knowledge) becomes ever more valuable as the business grows and changes.

Justification: securing unknown or unrecognised assets is difficult, at best. Once identified, important information concerning an SME's information assets (e.g. hardware and software versions, locations, owners and administrators) can be compiled and maintained, feeding the associated risk and security management processes e.g. patching [SME2].

Implementation notes: inventories should be designed, prepared and updated whenever information assets substantially change (e.g. when computer equipment or services are acquired, moved, reconfigured or disposed-of). Furthermore, periodic or prompted reviews and updates help management keep up with gradual and unauthorised changes, perhaps triggering investigations and security improvements in response to evolving or novel risks.

Primary reference: [ISO/IEC 27002](#) clause 5.9.

SME13 Scams

Summary: appreciation of the broad range of scams currently threatening SMEs is key to reducing the associated risks.

Justification: businesses and individuals generally are subject to numerous scams, hacks, attacks etc., most resulting in loss, damage, injury etc. For an SME, a ransomware incident, major fraud, serious accident or AI-enabled deception can be devastating, perhaps terminal.

Implementation notes: scams generally exploit vulnerable people, so informing and guiding workers about topical scams is the primary control, involving security awareness for all and targeted training where appropriate [SME5]. Management oversight [SME20] and monitoring [SME19], coupled with detective controls (e.g. log entries and alerts whenever security overrides are used) and assurance (e.g. reviews and audits of critical processes and records) can help detect and curtail incidents in progress [SME8]. Alert SME workers recognising and responding to the warning signs (e.g. by avoiding dubious activities and reporting their concerns to management) can reduce the number and severity of incidents that occur at all, and should be actively encouraged and supported by management. Liaise with suppliers, partners and customers to minimise supply chain vulnerabilities (e.g. how to authenticate invoicing and bank account changes) [SME18].

Primary reference: [ISO/IEC 27002](#) clause 5.7.

SME14 Applications

Summary: secure application software protects the information being processed, which in turn protects those who depend upon the information.

Justification: appropriate handling (communication, processing and storage) of digital data by applications (apps) is an essential part of cybersecurity. Procedural and other controls can only partially compensate for inherently insecure and vulnerable apps.

Implementation notes: there are security implications for app inputs, storage, processing and outputs (e.g. cryptographic validation [SME21], authentication and access controls [SME1]), as well as the manner in which apps are:

- specified, designed and developed [SME24];
- selected and authorised [SME20];

- obtained and installed on data networks [[SME6](#)], servers [[SME11](#)] and other devices [[SME7](#)];
- configured and used [[SME5](#)];
- managed, monitored [[SME19](#)] and supported;
- maintained and patched [[SME2](#)].

Primary reference: [ISO/IEC 27002](#) clause 8.26.

SME15 Compliance

Summary: information security controls can help an SME identify, comply and conform with applicable requirements such as those relating to information security, privacy, product and worker safety, financial accounting and reporting etc.

Justification: failure to comply with mandatory obligations or to conform with (satisfy or fulfil) relevant, reasonable and accepted requirements and expectations relating to information security can have serious consequences for any business or individual, including SMEs. Aside from enforcement actions and penalties, incidents may have adverse commercial implications such as reputational damage and brand devaluation.

Implementation notes: simply discovering and understanding compliance obligations and conformity expectations is a substantial challenge for SMEs, especially those with international business. Evaluating and addressing the associated risks and opportunities includes but extends beyond information security management, including aspects such as exposure, ethics and commercial implications. There may be opportunities to reject or negotiate unreasonable obligations and expectations but, once an SME is committed, various controls are appropriate to achieve and maintain compliance and conformity.

Primary reference: [ISO/IEC 27002](#) clause 5.36.

SME16 Privileges

Summary:

Justification: the powerful rights and permissions associated with privileged computer accounts can be used appropriately, securely and ethically, or not. Privileges often override or can be used to reconfigure, disable or evade system security controls, making them key targets for hackers and other adversaries intent on exploiting vulnerabilities without being detected and stopped.

Implementation notes: in all walks of life, ‘privilege’ is a restricted asset that is devalued if made too widely available. Controlling privileges in the information security context typically involves withholding privileges by default, only granting them to suitable, trustworthy and competent workers, apps, utilities etc. if necessary and justified, perhaps only for specified periods or purposes (e.g. user administration [[SME1](#)], backups [[SME4](#)] and patching [[SME2](#)]). The use or attempted access to particularly powerful privileges should be monitored [[SME19](#)] and logged routinely, ideally with alerts or alarms to notify relevant people of potentially inappropriate activities.

Primary reference: [ISO/IEC 27002](#) clause 8.2.

SME17 Assurance

Summary: ‘ensuring’ and being confident of anything (such as the suitability and adequacy of an SME’s information security arrangements) implies the need for assurance to reduce stakeholder uncertainties (risks).

Justification: without adequate and suitable assurance (ideally supported by meaningful enforcement actions if appropriate), various rules, obligations, requirements and expectations rely on the ethics and willing compliance, conformity and support of workers. The residual uncertainties (risks) can be reduced through assurance.

Implementation notes: assurance involves checking, testing, reviewing and auditing activities to obtain and evaluate relevant information. In the information security context, that includes controls such as event logging, automated alerts and alarms, routine monitoring of key risk and security parameters [SME19] plus investigations or studies prompted by, or intended to detect and address, significant incidents, vulnerabilities and other issues. Assurance is also key to supply chain security [SME18], risk and security strategies, investments, continual improvement/maturity etc.

Primary reference: [ISO/IEC 27001](#) clauses 9.2 and 9.3.

SME18 Suppliers

Summary: information security controls are appropriate to mitigate unacceptable risks to information within and concerning supply chains.

Justification: in addition to products (goods and services) and money, information relating to and flowing through supply chains and networks is subject to risks of concern to those directly involved. There are inevitably tensions between them when sharing and evaluating information, relying on mutual openness or transparency, honesty, credibility and consistency. Protecting this valuable yet vulnerable information is often an underappreciated part of managing business relationships, supporting supply chain resilience, product security and commercial opportunities.

Implementation notes: mitigating risks to the confidentiality, integrity and availability of supply chain information that are unacceptable to SME stakeholders and supply chain partners implies the need for appropriate information security controls. In addition, the information can be of interest and value to third parties such as competitors and criminals intending to cause disruption and exploitation, and is vulnerable to accidents, delays and errors. Identifying, evaluating, treating and monitoring these information risks requires collaboration between those involved on risk and security management, including assurance [SME17].

Primary reference: [ISO/IEC 27002](#) clause 5.19.

SME19 Monitoring

Summary: tracking parameters, metrics and other information pertinent to information risk and security management gives SME management the basis for identifying, reacting to, minimising and ideally averting business issues.

Justification: the lack or inadequacy of pertinent, up-to-date and accurate information increases uncertainty (risk). Identifying, monitoring, evaluating, reporting and acting on information can mitigate the risk. Monitoring and reacting appropriately to issues with important, dynamic or otherwise risky business activities, systems, processes, controls etc. is an integral part of business administration and security management.

Implementation notes: with limited resources and other priorities, SMEs need to be smart about information risk and security monitoring, for example focusing selectively on the most significant, dynamic or risky aspects relating to core business objectives. Automating routine data collection, analysis and reporting of key security metrics can help, provided the associated requirements are properly specified and duly satisfied in practice. A complementary approach is to watch for and investigate anomalies that can indicate or give early warning of hidden issues, events and incidents. Relative to larger organisations, SMEs have the advantage of closer relationships between workers

(implying shorter paths and quicker information flows) but the disadvantage of less capability to focus on specific, detailed issues such as information risk and security. Designing, operating and maintaining appropriate risk and security monitoring is a governance responsibility [[SME20](#)].

Primary reference: [ISO/IEC 27001](#) clause 9.1.

SME20 Governance

Summary: instituting appropriate information security governance arrangements is a crucial part of SME management.

Justification: proactively directing and controlling the organization's information risk and security arrangements supports sound corporate governance, effective organizational management and sustainable business success. SME managers and other stakeholders cannot reasonably claim to be ignorant of significant information risks and security issues (such as noncompliance with privacy, safety or tax laws [[SME15](#)]) since they are collectively responsible for appropriate governance, and personally accountable for individual failings.

Implementation notes: although some governance arrangements emerge naturally as an SME is formed and grows, proactively designing and implementing appropriate mechanisms (such as defined roles, responsibilities, reporting lines, accountabilities and policies [[SME5](#)]) supports organisational development, maturity and security. It reduces information risks arising from unreliable, slow, inaccurate and irrelevant internal information flows, misunderstandings, gaps and conflicts, inadequate emphasis on core business objectives etc.

Primary reference: [ISO/IEC 27001](#) clause 5.3.

SME21 Cryptography

Summary:

Justification: several important cybersecurity controls protecting the integrity and confidentiality of computer systems, networks and data involve cryptography. Well designed, operated and managed cryptography can provide strong, reliable security, but these are complex controls that tend to decay over time and fail-unsecure, and therefore need to be managed carefully.

Implementation notes: cryptography is a complex field, the domain of competent technical specialists. SMEs are largely reliant on encryption and cryptographic authentication functions within computer devices [[SME7](#)], applications [[SME14](#)] and network services [[SME6](#)] from suppliers [[SME18](#)]. Nevertheless, there are strategic decisions and technical choices to be made between cryptographic algorithms, technologies and supporting processes (e.g. securing communication, storage and processing of sensitive data, and being especially discreet with secrets, perhaps even avoiding the use of IT completely [[SME1](#)]). As an example, the emergence of quantum computing is driving the adoption of quantum-safe algorithms, requiring a systematic approach to identify and upgrade or replace traditional pre-quantum cryptographic mechanisms [[SME12](#)].

Primary reference: [ISO/IEC 27002](#) clause 8.24.

SME22 Knowledge

Summary: sharing knowledge on information security matters with third parties can be valuable, provided the associated information risks are addressed.

Justification: information security is such a broad, complex and dynamic field that SMEs can benefit from specialist advice from competent and knowledgeable colleagues at little to no cost.

Implementation notes: professional social networks [[SME6](#)], special interest groups, trade bodies, suppliers, advisors, academic studies and surveys can provide knowledge (information, insight, guidance and support) concerning information risks and security controls, strategies, tools, incidents etc. However, the sensitive nature of this field is such that professionals can be reluctant to disclose much except perhaps to trusted colleagues [[SME5](#)], and can struggle to distinguish factually accurate information from conjecture, supposition and marketing scams [[SME13](#)].

Primary reference: [ISO/IEC 27002](#) clause 5.6.

SME23 Insurance

Summary: insurance cover is an example of a corrective or post-incident control that partially mitigates the losses and costs incurred by clients suffering claimable events.

Justification: pooling of risks and insurance premiums allows insurers to indemnify clients, paying to offset certain losses and costs associated with specified types of incident or claim. Insurance can be cost-effective for serious, rare and unpredictable incidents where the risks cannot be sufficiently mitigated by other controls.

Implementation notes: forms of insurance relevant to information risk and security include:

- cyber-insurance – covers costs and losses arising from cybersecurity incidents such as malware and ransomware infections and hacks;
- business interruption insurance – covers costs and losses relating to business interruptions caused by various incidents;
- professional indemnity and technology errors and omissions insurances – cover individuals and companies providing professional advice, services and other products against third party claims for negligence, intellectual property theft etc.;
- fidelity insurance provides cover for dishonesty by employees such as fraud, theft and embezzlement;
- directors and officers liability insurance – indemnifies directors and officers against claims relating to their statutory obligations towards the SME, and their personal accountability for unwise management decisions;
- property, vehicle and other types of insurance – can provide limited cover e.g. compensation for theft or accidental damage to IT hardware in the office, at workers' homes or while travelling;
- self-insurance – refers to paying for incidents from company reserves, a low-cost but risky approach since serious or repeated incidents can exhaust reserves.

The descriptions above are generic and simplified. The terms and conditions in insurance policies (contracts) specify, in explicit detail:

- the actual cover and exclusions;
- associated client obligations e.g. to operate various security controls, avoid unnecessarily exposing assets to compromise, and disclose pertinent factors;
- commercial aspects such as the premium, excess and sum insured;
- legal aspects such as applicable laws and dispute procedures.

Some insurers can also provide or engage specialist forensics and support services to help clients investigate and resolve incidents, perhaps in conjunction with the authorities.

Primary reference: [ISO/IEC 27102](#).

SME24 Development

Summary: information security relating to various forms of development revolves around defining, prioritising and satisfying business requirements for risk mitigation.

Justification: while it can be tempting for an SME that only uses off-the-shelf software to disregard this control, development-related information risks are not limited to applications [SME14]. There are information risks associated with various business, product, market, workforce and process developments for instance, plus information services (such as Internet and cloud computing) and professional services (such as IT, accounting, human resources and legal services). Rapid advances in AI and quantum computing are topical examples of technological developments with significant risk and security implications.

Implementation notes: this control is clearly relevant to SMEs that commission and develop software or information systems. For other SMEs and other forms of development, addressing information risks should be a routine and well-practiced part of relevant business activities such as:

- identifying information risks and specifying information security objectives for processes and commercial relationships;
- considering information risk, security and related aspects when choosing between and acquiring various products and approaches;
- encouraging or requiring suppliers, customers and partners to address information risks for the benefit of entire supply chains [SME18];
- preferentially adopting secure computing and communications protocols, information systems, services etc.;
- keeping abreast of technological and other developments with risk and security implications, perhaps even driving innovation in this area through projects and collaborations.

Primary reference: [ISO/IEC 27002](#) clause 8.25.

Queries, criticisms and suggestions to improve this draft are welcome.

Please email me Gary@isect.com or
participate in the debate through the free [ISO27k Forum](#).

This guideline comes to you free of charge thanks to our sponsor:
the [Cybersecurity Hyperglossary](#). Talk straight. Cut the jargon!