
# Information risk catalogue

By Gary Hinson

27th January 2024

**Summary**

This generic catalogue is a brainstorming tool to help identify information risks - an important prelude to their analysis and treatment in the business context. Please don't be overwhelmed by its length! The list of **over 200 information risks** is *deliberately* wide-ranging to prompt creative thinking, and yet it is not totally comprehensive. For one thing, multiple risks can coincide. Simply imagining the permutations and combinations is mind-blowing! While some may *seem* far-fetched, risks just like these have caused real-world incidents within living memory. By all means focus on the risks most relevant to your specific context, and get to work on evaluating and addressing the most significant ones as soon as possible … but don't completely discount or ignore the remainder. Remember that 'improbable' is not 'impossible', just as 'probable' is not 'certain'. Risk management is risky!

## Definitions

I define **information risk** as 'risk pertaining to information', where:

- **Risk** is the possibility of threats exploiting vulnerabilities to cause incidents with adverse impacts;
- **Pertaining to** means to or involving;
- **Information** includes all forms and formats of information such as computer data and knowledge.

*Most* but not *all* risks to information constitute information *security* risks that involve the compromise (loss or reduction) of its confidentiality, integrity and/or availability, below anticipated or required levels – although the requirements are seldom defined or quantified beyond vague categories (*e.g*. top secret, secret, commercially confidential, public).

**Hinson tip**: although often described as risks, missing, dysfunctional or failed controls are conceptually distinct from the risks that the controls are supposed to mitigate. While weak or missing preventive controls, for instance, may fail to prevent incidents, detective and corrective controls may yet save the day *if* threats act on vulnerabilities. The risk is indicated in that final clause. Having said that, the possibility of controls failing is itself a risk that generally is counteracted by further 'layers' of control, including up-front resilience engineering, assurance measures and incident responses. Some of these constitute management or process controls: it's not all about information security!

## Purpose and audience for this document

This document lays out a deliberately wide range of information [security] risks as a reminder or prompt of the kinds of issues potentially worth considering in information risk analysis. The process of risk analysis is creative and expansive in nature (*e.g*. contemplating the myriad ways and times at which incidents can occur), as well as analytical and systematic (*e.g*. breaking down 'information risk' into its constituent parts for greater insight).

**Hinson tip**: some of the entries in this catalogue are compound *i.e*. they mention multiple threats, vulnerabilities and/or impacts relating to an information risk. That's life! Take malware risks, for instance: there is a tremendous variety of viruses, worms, Trojans, ransomware, spyware and so on.

The main idea is to provide the creative spark that lights fires under risk analyses, risk assessments, risk workshops and the like. It is all risk-related, more specifically "information risk" as defined above.

Despite the length of this paper, this is *not* a comprehensive or complete risk catalogue. As expressed here, many of what I call 'information risks' are in fact scenarios involving clusters of related risks. With decades of experience and a lifelong fascination with the topic, I have particular incidents or situations in mind behind them all. Since your background, experience, interests and perspective certainly differs, you should be able to identify further risks.

There may be particular circumstances that affect your organisation, its business situation, location and circumstances, including some that previously have or might have caused 'situations', events, incidents or disasters, plus those that present novel and perhaps emerging concerns for the future.

## Tags

I have *arbitrarily*[1] categorised the information risks using the following colour-coded hashtags[2]:

- #Confidentiality risks lead to incidents that typically result in information being revealed inappropriately, leading to the potential for consequential losses (*e.g.* exploitation of the information by third parties) and various harms.
- #Integrity incidents can render information, systems, people and organizations unreliable, inaccurate and outdated, leading to incidents such financial losses, reputational damage, brand devaluation and compliance issues.
- #Availability incidents limit, slow or prevent required, relevant, high-quality information being readily available for legitimate business activities. This can slow or interrupt dependent activities and processes, reduce the quality and nature of decision making, threaten safety *etc*.
- #Other incidents may not directly or primarily affect the confidentiality, integrity or availability, such as those relating to or arising from the *mis*management of information risks**.**

## About the author

I am Dr Gary Hinson PhD MBA, an information security specialist with a lifelong interest in the human, technological and commercial aspects of both protecting and exploiting information.

Originally a research scientist, my professional career stretches back to the mid-1980s as a practitioner, manager and consultant in the fields of IT system administration, information security and IT auditing for multinationals in several industries.

As a freelancer, I research, write, debate, consult, audit, mentor and teach, mostly on ISO27k - the ISO/IEC 27000 information risk and security management standards - and information security metrics.

Browse these websites for more:

- IsecT.com concerns my freelancing/consulting business
- SecAwareBlog.blogspot.com is my blog … which Google refuses to index
- SecAware.com is a source of security policies, ISO27k templates and awareness content
- ISO27001security.com has information on the ISO27k standards, plus free templates and tools
- SecurityMetametrics.com offers guidance on the P.R.A.G.M.A.T.I.C. security metrics method
- linkedin.com/in/garyhinson/ has my professional profile and interests.

[1] You will probably doubt, dispute or disagree with some of the tags, thinking of different incidents, situations and outcomes. Being human, I have made mistakes. By all means contact me to put me right, or ignore or correct the tags as you wish. This catalogue is simply a creative prompt, a starting point for your risk management remember. Knock yourself out.

[2] Some incidents may harm the confidentiality, integrity *and* availability of information, or may involve any of those aspects depending on precisely what occurs.

# Information risk catalogue

- ☐ Accidental inappropriate and/or unauthorised disclosure of sensitive proprietary or personal information due to human error *e.g.* a worker emailing a spreadsheet or scanned document attachment containing sensitive information, or attaching the wrong file or selecting the wrong recipient, causing embarrassment or worse, leaving logged-in systems unattended, failing to redact the correct information appropriately or releasing an unredacted version by mistake, catching a glimpse of someone's underwear; #Confidentiality
- ☐ **A**dvanced **P**ersistent **T**hreats – extended and extraordinarily intense, targeted, well-planned and competently-executed incidents involving spies/spooks, malware, social engineering, deception, burglary, coercion *etc*. perpetrated or supported, tolerated, resourced and enabled by governments for national security, commercial or political reasons, or by other highly competent and resourceful adversaries for their own reasons (*e.g.* organised criminal gangs/networks, pressure groups, extremists, terrorists, evil corporations); #Confidentiality #Integrity #Availability
- ☐ Advances in technology, tools and techniques rendering old controls and existing security arrangements relatively inefficient, ineffective, costly or obsolete; #Integrity
- ☐ Aggregation, cross-referencing and deep analysis of information obtained from disparate sources, possibly dubious and of uncertain quality; #Confidentiality #Integrity
- ☐ **A**rtificial **I**ntelligence 'feeding on its tail': generative AI outputs of dubious quality being used to train further AI systems; #Integrity
- ☐ Autocorrect mistakes; #Integrity
- ☐ Bad advice, possibly deliberate (misinformation/disinformation, social engineering, fraud, inept or inappropriate decision support) but more often simply inept; #Integrity
- ☐ Bad decisions, errors of judgment and the like – particularly those with significant or material consequences (which may not become evident until later on) and unintended consequences (*e.g.* inappropriate metrics leading to counterproductive changes); #Integrity
- ☐ Bad metrics *e.g.* low value, insufficiently linked to reality, unclear meaning or purpose, readily manipulated or faked; #Integrity
- ☐ Bad, incompetent or fraudulent research *e.g.* inappropriate, inept or biased sampling of members of a population, leading to false and misleading survey conclusions; #Integrity
- ☐ Bias, discrimination and prejudice; #Integrity
- ☐ Bit errors, where individual binary bits are flipped or remain stuck despite the intended data communications and processing (*e.g.* cosmic rays, thermal or electrical noise, chip manufacturing defects); #Integrity
- ☐ Black ops, false-flag and similar underhand techniques to conceal the true nature and perpetrators of incidents; #Integrity
- ☐ Bribery and corruption, inappropriate/coercive lobbying, physical threats and other forms of social manipulation; #Integrity

- ☐ Bugs – all manner of software coding errors affecting all kinds of program creating vulnerabilities, constraining or negating technical controls and exposing IT systems to attacks, errors, unreliability, performance/capacity issues and other concerns, events, issues, limitations or incidents; #Integrity
- ☐ Camouflage and deception *e.g.* masquerading as an authorised person in order to gain unauthorised access to or control over valuable information, such as fake boss/business email compromises; typo-squatting; phishing, vishing, smishing *etc.*; #Integrity
- ☐ Carelessness, negligence, slapdashery; #Confidentiality #Integrity #Availability
- ☐ Casual/amateur or directed/professional theft of sensitive information from offices, data centres, archive stores, libraries, workers' homes, vehicles or bags, hotel rooms, conference/training facilities *etc.*; #Confidentiality
- ☐ Classical ransomware attacks in which legitimate users are simply locked out of their systems *e.g.* by disabling all their accounts; #Confidentiality #Availability
- ☐ Coincidences such as coincident discoveries, inventions or phrasing, whether genuinely chance events or false claims; #Other
- ☐ Coincident or unexpected failures, issues or events involving information *e.g.* discovery of additional vulnerabilities, threats or impacts, perhaps as a result of unanticipated incidents, zero-days *etc.*; #Confidentiality #Integrity #Availability
- ☐ Collisions of messages on shared links *e.g.* overloaded data networks or voice/radio circuits; #Integrity #Availability
- ☐ Complexity, conflicts and other issues relating to IT systems, hardware, firmware, middleware, software *etc.* plus various information processes/activities, interactions, laws/regulations *etc.*; #Integrity #Availability
- ☐ Compliance or conformity failures relating to laws and regulations around information *e.g.* financial reporting, safety systems, environmental hazards, privacy …; #Integrity
- ☐ Conceptual differences, flaws and misunderstandings *e.g.* basing systems, processes or organisations on inaccurate, incomplete or out of date models of the world; #Integrity
- ☐ Conflicting rules, expectations, policies, directives, instructions *etc.*, either generally or under specific circumstances; #Integrity
- ☐ Conflicts, disagreements, misunderstandings, mistranslations and misinterpretations in general relating to communications in various formats, languages, situations, levels of formality, media *etc.*; #Other
- ☐ Confusion and doubt – clouded thinking leading to uncertainty, the possibility of error and perhaps a reluctance to commit to or initiate the appropriate responses, activities *etc.*; #Integrity
- ☐ Consensus and "group-think" where individual perceptions, decisions and actions are modified, coerced or subsumed by the social group and context in which they are expressed *e.g.* deferring subserviently and inappropriately to a strong/charismatic/powerful leader, going along with and failing to challenge the prevailing wisdom; #Integrity

- ☐ Conspiracies *e.g.* restrictive trade agreements, cabals, monopolies/duopolies/oligopolies; #Integrity
- ☐ Contradictions in general, whether differences of opinion, alternative interpretations or conflicting facts; #Integrity
- ☐ Control bypasses, shortcuts, evasion, reconfiguration, disablement *etc.*; #Confidentiality #Integrity #Availability
- ☐ Controls that fail silently, subtly, unexpectedly or in unanticipated fashion; #Confidentiality #Integrity #Availability
- ☐ Controls that simply don't function as intended, wholly or partially, perhaps failing occasionally or under exceptional conditions; #Confidentiality #Integrity #Availability
- ☐ Corruption or loss of strategies, plans, metrics and other valuable business information; #Availability
- ☐ Covert mechanisms such as cheat codes, backdoors, trapdoors, magic packets *etc*. allowing certain controls to be overridden or disabled; #Confidentiality #Integrity #Availability
- ☐ Crypto-ransomware attacks in which users' data are strongly encrypted; #Confidentiality #Availability
- ☐ Cultural conflicts within or beyond the organisation, leading to ineffective and inefficient working practices, perhaps exposing or causing information security or privacy issues; #Integrity #Availability
- ☐ Cyberattacks using credential stuffing, malware, SQL injection, cross-site scripting *etc.*; #Integrity
- ☐ Cybercriminals, hackers or spooks targeting confidential information for financial gain, identity theft, espionage or other reasons, using methods such as phishing, malware/APTs, hacking and coercion; #Confidentiality
- ☐ Cybertage (deliberate sabotage, damage or destruction of computer data, systems, devices, equipment, networks, cabling, power supplies, air conditioners, or IT security controls such as intruder or fire alarms *etc.*) by malicious insiders, outsiders, both (collusion) or unknown perpetrators; #Availability
- ☐ Damage, loss, compromise, theft or duplication of authentication/security tokens and devices such as passports, ID cards, staff passes, smartphones, keys *etc*. leading to further incidents; #Confidentiality #Integrity #Availability
- ☐ Deceit, lies, half-truths and 'alternate realities', especially if expressed convincingly; #Integrity
- ☐ Defection of invaluable knowledge workers to competitors, taking their brains with them!; #Availability
- ☐ Degradation of information quality and quantity *e.g.* fading of printed or written materials, loss of cited content and context; #Availability
- ☐ Delayed identification of incidents, perhaps indefinite; #Other
- ☐ Delays and interruptions to information services causing temporary inability to access information; #Availability

- ☐ *Deliberate* generation and leakage, disclosure or publication of misleading, inaccurate, incomplete, out-of-date or entirely fabricated information with the express intention of misleading others for commercial, political, criminal or other reasons (misinformation/disinformation); #Confidentiality #Integrity
- ☐ Delusions and hallucinations including those afflicting AI systems as well as influential/powerful people and their followers *e.g.* the social phenomenon known as 'outrage' – genuine but irrational/excessive fears of cell towers, vaccinations *etc.*; #Integrity
- ☐ **D**enial **o**f **S**ervice attacks, whether intentional or accidental *e.g.* due to misconfiguration, capacity constraints, unanticipated peak loads, bugs and flaws, testing; #Integrity #Availability
- ☐ Dependencies in general *e.g.* cryptographic dependence on randomness, algorithms and implementation details; widespread reliance on various approaches, tools, individuals and organisations; #Confidentiality #Integrity #Availability
- ☐ **Dependencies** in general, where multiple things, people, systems, organisations need to collaborate, cooperate and work effectively together, but are fragile or unreliable in fact; #Availability
- ☐ Design flaws – unrecognised or unresolved mistakes in the architecture and design of systems, processes, activities and arrangements; #Integrity
- ☐ Design flaws in systems, applications and processes/activities involving information; #Confidentiality #Integrity #Availability
- ☐ Destructive or disruptive cyberattacks typically involving malware plus escalation of privileges and other hacks; #Availability
- ☐ Difficulties and costs to obtain sufficient reliable, accurate, timely information, hence a tendency to accept and use low-quality information that is more readily available; #Availability
- ☐ Disaffected workers who plan to join competitors or set up in competition with the organisation; #Confidentiality #Integrity #Availability
- ☐ Disclosure, revelation or other compromise of the credentials *(*passwords, private keys, biometrics, SIM cards …) used to identify and authenticate individuals, systems, applications *etc.*; #Confidentiality #Integrity
- ☐ Discovery and eDiscovery of compromising/incriminating internal corporate information … or difficulties discovering information from adversaries *e.g.* cyber criminals accused of incidents; #Integrity
- ☐ Disinformation – the *deliberate* provision of misinformation intended to mislead others; #Integrity
- ☐ Disruptive events in general, including natural and human activities *e.g.* pandemics, strikes, protests, traffic jams, security/safety incidents; #Availability
- ☐ Distraction and reduction of cognitive capabilities due to personal problems such as addictions, debts, mental illness, relationship issues, grievances, coercion and other/conflicting interests or pressures; #Integrity #Availability
- ☐ Diversionary tactics *e.g.* distraction theft/pickpocketing, dummy moves/feints/side-steps, chaff; #Integrity

- ☐ Double-bluffs and other manipulative psychological/social engineering techniques exploiting a target's misunderstandings; #Integrity
- ☐ Employment disputes or incident involving intransigent, belligerent, difficult workers; #Confidentiality #Integrity #Availability
- ☐ Errors in strategic, tactical or operational decisions and activities *e.g.* errors of judgment, following suboptimal strategies, analysis-paralysis, inappropriate allocation of resources; #Integrity
- ☐ Ethical failures, especially if they are noticed, causing further concerns and adverse consequences such as disreputation, distrust and brand devaluation; #Integrity
- ☐ Excavators accidentally (or even deliberately?) ripping up network and power cables, water lines, fuel lines *etc.*; #Availability
- ☐ Exceptions *i.e.* unusual situations in which controls are deliberately relaxed or overridden, generally for compelling business reasons. Aside from the risk of someone being misled or coerced into inappropriately reducing controls, there may be other adverse consequences such as further transactions or activities also passing the disabled controls; #Integrity
- ☐ Excessive or inappropriate creativity – hallucinations, wild theories or claims, refusal to evaluate or accept more rational fact-based explanations, unfounded conspiracy theories generated or propagated by workers, social groups or systems including AI; #Integrity
- ☐ Excessive or inappropriate responses to relatively minor information security incidents *e.g.* taking business systems offline for detailed and lengthy forensic analysis even if there is virtually no prospect of prosecutions, taking numerous related systems down just in case a malware infection or hack has spread following an identified incident; #Availability
- ☐ Excessive/inappropriate/unnecessary conservatism and unreasonable resistance to or unwillingness to accept/embrace change, including stubbornness, arrogance, political interference, lack of vision/foresight, unwillingness to learn and improve; #Other
- ☐ Excessively lax, tight, rigid, inappropriate, difficult or otherwise costly security controls; #Confidentiality #Integrity #Availability
- ☐ Excessively tight, strict or laborious access controls making legitimate use of information impossible, too hard, too much effort, too slow, too costly *etc.*, causing impediments and delays to the business and perhaps other effects (*e.g.* causing people to rely instead on lower quality information that is more readily/cheaply available); #Confidentiality #Integrity #Availability
- ☐ Excessively tight, strict or laborious access controls leading workers to evade, disable or erode them *e.g.* passwords on sticky notes; #Confidentiality
- ☐ Exploitation of metadata such as traffic analysis, file sizes and dates, classification or other tags; #Confidentiality
- ☐ Exposure or revelation of vulnerabilities to threats, allowing adversaries or accidents to exploit or trigger them; #Confidentiality #Integrity #Availability
- ☐ Extortion, blackmail or revenge involving the threatened or actual revelation, corruption or destruction of information; #Integrity

- ☐ Extreme pressure creating excessive stress, exacerbating fragility/limited resilience, with people, teams, business units, organisations and even entire nations and populations operating 'on a knife edge', sub-optimally, and perhaps acting irrationally; #Integrity #Availability
- ☐ Facilitating or encouraging illegal, unethical, inappropriate, or socially unacceptable activities; #Integrity
- ☐ Failure to deliver on promises, guarantees, offers, expectations, contracts and agreements; #Other
- ☐ Failure to recognise, evaluate and respond in an appropriate and timely manner to shifts in the risk landscape such as new/emerging risks, increasing/decreasing threat levels, newly discovered or currently exploited vulnerabilities, or changing business use of and dependence on information; #Other
- ☐ Failure to take risks that fall within management's risk tolerance and appetite, for whatever reason *e.g*. incorrectly analysed and evaluated, biased decision-making, personal prejudices or limitations such as timidity and undue caution (perhaps due to prior incidents), or a genuine and realistic appreciation of the true magnitude of the risk based on experience and expertise ('gut feel'); conversely, gung-ho attitudes, lack of stability, inability to focus and complete important things, lack of strategic thinking and planning, short-term-ism and excessive risk-taking; #Other
- ☐ Failure to uphold or fulfil explicit or implicit contractual obligations, commercial or employment agreements, codes of practice, standards, reasonable and ethical expectations *etc*.; #Other
- ☐ Failures of information-related security controls and arrangements; #Confidentiality #Integrity #Availability
- ☐ Falsification, fakery, counterfeiting and piracy – the illegitimate production, distribution and passing-off of copied products, materials and information that masquerades as and so appears to come from legitimate producers or sources; #Integrity
- ☐ Financial losses if information is inappropriately modified or destroyed, *e.g*. ransomware; #Integrity
- ☐ Forgotten passwords, phrases and other important secrets; #Confidentiality #Availability
- ☐ Fragility in general *e.g*. undue reliance on single points of failure, operating too close to safety, technology, capacity, financial, support or other limits; #Integrity
- ☐ Fraud, misappropriation *etc*., including malicious collaboration between groups of people (breaking divisions of responsibility) ; #Integrity
- ☐ Fundamental flaws and mistakes in the design, implementation, operational use or management of crypto-systems *e.g*. non-random key generation, obscure technical or mathematical/statistical vulnerabilities, re-use of **O**ne **T**ime **P**ads, predictability of sequence numbers, nonces or seed; #Confidentiality #Integrity
- ☐ Fundamental misunderstandings about information risk and security such as the myopic focus on IT/cyber; #Other
- ☐ **G**arbage **I**n **G**arbage **O**ut – undue reliance on inaccurate, incomplete and perhaps maliciously crafted information inputs to a processing system, producing erroneous outputs; #Integrity

- ☐ Governance issues or failures *e.g.* provision of insufficient resources or of inappropriate structures and reporting arrangements, to manage the organisation's information risks adequately; #Confidentiality #Integrity #Availability
- ☐ Gradual accumulation of information errors and volumes of information degrading information processing services, IT systems and networks, processes *etc*. over time, reducing remaining capacity, performance and the ability to recover information from systems, backups and archives; #Availability
- ☐ Gradual degradation of information quality through the accumulation of errors and omissions, misinformation, inaccurate inferences, presumptions and conclusions *etc*.; #Integrity
- ☐ Gradual or sudden loss of information due to natural causes - accidents, disasters, floods, fires, pestilence, mould, exposure to sunlight, insect infestation, rat or squirrel damage to cables, mice nesting inside IT equipment …; #Availability
- ☐ Hackers, crackers, cybercriminals and their nefarious activities; #Confidentiality #Integrity #Availability
- ☐ Hardware, software, system or service failures affecting IT equipment, storage media, network connections, cloud services, security controls *e.g.* as a result of power issues, overloads, obsolescence, mould or vermin infestation, fires, floods, misconfiguration, system self-protection *etc*.; #Availability
- ☐ Health and safety issues or incidents adversely impacting workers' capabilities, motivation and competence, such as tiredness, stress, overload, burnout, mental illness, distraction/inability to concentrate …; #Availability
- ☐ Human errors and mistakes damaging or destroying information such as people accidentally deleting files, misconfiguring IT systems or destroying valuable contracts, agreements, invoices, receipts, instructions …; #Availability
- ☐ Human errors *e.g.* typos, accidental deletion or overwriting of data … and many others; #Integrity
- ☐ Idiocy – limited comprehension and cognitive capabilities or capacity, increasing the frequency and/or severity of inappropriate decisions, responses, outputs *etc*. and reducing the ability to recognise and respond appropriately to inaccurate, misleading, out-of-date or patently false information; #Other
- ☐ Illegitimacy in general; #Integrity
- ☐ Illicit, illegal, unethical or excessive surveillance, monitoring, snooping, voyeurism …; #Confidentiality
- ☐ Implausible deniability where a person, department, business unit or organisation was patently aware of a significant, reportable incident but failed to do so, claiming *not* to have known about it or their obligation to disclose it; #Integrity
- ☐ Inability or delayed access to information needed for legitimate and appropriate business purposes due to the access controls *e.g.* forgotten password, lost encryption key; #Confidentiality #Availability

- ☐ Inability to make legitimate *use* of and benefit from available information *e.g*. inadmissible or forensically unsound evidence, 'ultra' secrets, use of personal information other than for explicitly consented purposes; #Availability
- ☐ Inadequate capacity and performance of an IT system, network, services or process resulting in delays, interruptions or complete failure to operate; #Availability
- ☐ Inadequate identification, analysis and treatment of information risks *e.g*. discounting, ignoring or failing to address legitimate risks appropriately, sufficiently and in good time; #Other
- ☐ Inadequate investment in information and information sources, IT, systems, networks, technologies, people, expertise *etc*.; #Other
- ☐ Inadequate, inappropriate, incomplete, incompetent or otherwise untrustworthy testing, reviews, audits or other assurance measures, placing undue confidence and reliance on the assurance gained; #Integrity
- ☐ Inappropriate 'fear of the unknown' and resistance to change – increasing the risk associated with stasis or slow responses; #Other
- ☐ Inappropriate and illegitimate use of information provided/obtained for legitimate purposes; #Confidentiality #Integrity
- ☐ Inappropriate beliefs *e.g*. mistaken attribution of incidents, failure to identify the true causes or reasons for particular occurrences; #Integrity
- ☐ Inappropriate defaults, particularly those that persist into production or that are readily reinstated *e.g*. by an accessible reset button or function; #Confidentiality #Integrity #Availability
- ☐ Inappropriate disclosure or theft (industrial espionage) of strategies, plans, budgets, management reports, metrics, risks, controls and other secret or sensitive information – the organisation's proprietary/business information, or personal information and third-party information in its care; #Confidentiality
- ☐ Inappropriate, poor quality, unreliable or missing metrics or other management information, leaving management operating in a vacuum and seemingly inept management in general; #Integrity #Availability
- ☐ Incidents caused by, and not identified and avoided/prevented/mitigated due to, naïveté, inexperience, inappropriate trust *etc*.; #Confidentiality #Availability
- ☐ Incompetence, ignorance, laziness, misguidedness and the like – people not earning their keep and conforming to requirements, including those who assume false identities, fabricate qualifications, conceal criminality, flaunt, bend or break the rules *etc.*; #Confidentiality #Integrity #Availability
- ☐ Incorrectly classified and prioritised incidents *e.g*. ramifications misunderstood; #Confidentiality #Integrity #Availability
- ☐ Inept innovation *e.g*. continuing to spend on 'legacy' dead-end technologies while failing to invest adequately in more promising approaches, thereby accumulating 'technical debt'; #Other
- ☐ Inept IT/OT change and configuration management, version control, patching *etc*.; #Confidentiality #Integrity #Availability

- ☐ Information or sensory overload, where a system, network, person, organisation *etc*. is deliberately or accidentally flooded with so much information (*e.g*. spam, amplification attacks, errors in network interfaces, a flood of alerts) that information services and processes falter or fail, causing delays and outages, loss of valuable information and perhaps more serious incidents; #Availability
- ☐ Information ownership doubts, challenges, disputes and disagreements, plus related concerns about ethics, control, exploitation and value; #Integrity
- ☐ Insider threats of all sorts – bad apples on the payroll, on the premises or closely involved with the business; people who exploit information gained at work, and other opportunities, for personal or other reasons to the detriment of the organisation and third parties; #Other
- ☐ Insufficient creativity, motivation, dynamism and buzz relative to competitors including start-ups (important for online businesses); #Other
- ☐ Interception of sensitive information in transit (during communication) using line taps and monitors, compromised comms servers and services; #Confidentiality
- ☐ Interference, meddling, disrupting and discrediting *e.g*. submitting malicious product reviews, spreading false rumours about an organisation or individual; #Integrity
- ☐ Intolerance, over-assertiveness and aggressive behaviour; #Confidentiality #Integrity #Availability
- ☐ Issues created by changes involving information, systems *etc*. *e.g*. incompatibilities between operating systems, middleware and application programs resulting from/discovered following patching or upgrades, inadequately specified, planned and prepared changes, inept implementations, and unexpected complications relating to or leading on from the change process; #Integrity
- ☐ Issues within closed-source, secret or undisclosed details of the inner designs of various complex technologies such as cryptographic modules and authentication systems; #Confidentiality #Integrity #Availability
- ☐ Lack of creativity, blinkered thinking, inappropriate constraints, failure, inability or refusal to think outside-the-box, lack of freedom and ambition or drive to succeed; #Other
- ☐ Lack of sufficient, up-to-date, accurate knowledge, appreciation and understanding of complex and dynamic situations; #Other
- ☐ Leakage of sensitive information to third parties via common business partners or intermediaries, through social media, job ads, casual conversations *etc*.; #Confidentiality
- ☐ Legal liability for incidents that result in the loss, disclosure or corruption of information, particularly in industries subject to strict laws and regulations concerning the confidentiality and/or integrity of information *e.g*. finance, healthcare, government and defence; #Confidentiality #Integrity
- ☐ Lip-service - claiming to be doing something (such as securing information) while actually doing nothing or something else; #Integrity
- ☐ Logical errors, fallacies, inappropriate heuristics (conceptual short-cuts) ; #Integrity

- ☐ Loss or lack of assurance, trust and confidence in the organisation's security, privacy and business continuity arrangements, its systems and people; #Integrity
- ☐ Lousy defaults such as well-known passwords that system administrators sometimes neglect to change after installation, or accessible 'factory reset' functions/triggers; #Confidentiality #Integrity #Availability
- ☐ Machiavellian people (especially managers) with personal agendas who scheme and manipulate systems, people/organisations and situations to their personal advantage to the detriment of others; #Confidentiality #Integrity #Availability
- ☐ Malware incidents – viruses, worms, Trojans, ransomware *etc*.; #Integrity
- ☐ Management or governance failures *e.g*. short-termism (planning horizons limited to a manager's anticipated tenure and bonus periods), inappropriate risk tolerance or appetite levels; #Confidentiality #Integrity #Availability
- ☐ Manipulation of strategies, plans, metrics/management information or other important operational information and data, whether intentional or not, one-off or ongoing/systematic; #Integrity
- ☐ Mechanical issues *e.g.* sensor, software/firmware programming or actuator failures on automated systems such as robots and **C**omputer **N**umerically **C**ontrolled machine tools, fan or air conditioning failures leading to equipment overheating; #Availability
- ☐ Misappropriation, malfeasance …; #Integrity
- ☐ Misattribution and false accusation, particularly if that leads to any form of harm to the alleged perpetrator; #Integrity
- ☐ Mis-classification – including misclassification of risks; #Integrity
- ☐ Misconfiguration of information systems, accidental or deliberate; #Confidentiality #Integrity #Availability
- ☐ Misdirection – deliberately misleading others into inappropriate conclusions, decisions and activities/responses; #Integrity
- ☐ Misidentification of people, applications, systems, messages *etc*.; #Confidentiality #Integrity
- ☐ Misinformation – inaccurate, incomplete, out of date or otherwise low-quality information provided or passed-on innocently, unknowingly, unwittingly; #Integrity
- ☐ Misinterpretation, such as mistakenly attributing certain effects to specific causes; #Integrity
- ☐ Misleading, inaccurate or out-of-date information about the status of suppliers, partners, customers, supplies, products, services, legislation, finances, IT systems, relationships, risks, controls *etc*.; #Integrity
- ☐ Misunderstandings by the transmitters and/or receivers of information ('Chinese whispers'), some stemming from language and cultural differences; #Integrity

- ☐ Moles, sleepers and plants – people deliberately placed within an organisation by an adversary for various nefarious purposes, or insiders 'turned' through bribery and corruption, coercion, radical idealism, opportunism or whatever, typically to commit industrial espionage (*e.g.* theft of confidential information) or sabotage/cybertage (*e.g.* interfering with systems, controls, parameters, relationships, strategies, plans *etc.* in order to slow or interrupt production services, compromise product quality, undermine brands and so cause commercial disadvantage; #Confidentiality #Integrity #Availability
- ☐ More significant risks and additional concerns relating to *particularly* sensitive information such as access credentials, trade secrets, financial and personal information (especially medical and sexual); #Confidentiality
- ☐ Natural disasters such as floods, fires, earthquakes, eruptions and sinkholes that damage, destroy or result in critical IT infrastructure, systems, services *etc.* being taken out of service, making important information unavailable for a period, perhaps indefinitely; #Availability
- ☐ Negotiations of all kinds – business-to-business, organisation-to-worker, boss-to-staff, organisation-to-regulator, government-to-nation, system-to-system …; #Other
- ☐ Noncompliance with mandatory obligations, legislation, contractual terms *etc.*; #Other
- ☐ Nonconformity with discretionary requirements, policies, responsibilities, expectations *etc.*; #Other
- ☐ Obsolescence leading to unreliability, costs to maintain adequate services and (often) security issues (*e.g.* reliance on old, unsupported, insecure versions of Windows); #Availability
- ☐ Operating beyond design constraints *e.g.* overheating, overdue maintenance, excessive stress, inappropriate applications; #Availability
- ☐ **O**perational **T**echnology, **I**ndustrial **C**ontrol **S**ystems or **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition incidents causing production outages, unsafe operating conditions, equipment malfunction, environmental damage, loss of materials, loss of efficiency, costly delays …; #Availability
- ☐ Other harmful events, accidents, incidents or disasters involving loss of confidentiality – a catch-all confidentiality risk; #Confidentiality
- ☐ Other harmful events, accidents, incidents or disasters involving use of inaccurate, incomplete, misleading or out-of-date information for business purposes – a catch-all integrity risk; #Integrity
- ☐ Other harmful events, accidents, incidents or disasters involving non-availability or loss of important, valuable information – a catch-all availability risk; #Availability
- ☐ Over-abundance of information (excessive volumes, high rates of change, substantial duplication, poor quality, misinformation, propaganda *etc.*) leading, misleading or manipulating people into behaving inappropriately, making bad decisions, ignoring/failing to notice and react to genuine issues *etc.*; #Availability
- ☐ Over-ambitious, unrealistic, unreasonable 'stretch' targets, goals, objectives, expectations, demands *etc.*; #Other
- ☐ Overloading of information services, systems, communications links, people, links *etc.* leading to unexpected/unpredictable delays, unreliability and distrust; #Integrity #Availability

- ☐ Overreliance on assertions, claims, promises and guarantees; #Integrity
- ☐ Overreliance on flawed assurance measures such as certifications, self-assessments, reviews and audits; #Integrity
- ☐ Paranoia – extreme, unreasonable, irrational and unrealistic fears; #Other
- ☐ Partial (temporary or permanent) loss of information *e.g.* workers forgetting, mis-remembering or misinterpreting things, accidental deletion of data from an application such as a database, spreadsheet or email system, deliberate deletion of what turns out to be irreplaceable data in order to recover storage space; #Availability
- ☐ People failing to read and understand the fine details, relying on summaries and skim-reading, leaping to false conclusions; #Integrity #Availability
- ☐ People, groups or organisations 'gaming the system', seizing opportunities to take advantage for selfish reasons *e.g.* strikes, obstinate or passive-aggressive behaviours such as working-to-rule; #Integrity
- ☐ Perfectionism *e.g.* a reluctance to start implementing valuable controls against extant risks until fully analysed and a complete architectural solution is 'finished' – by which time it may be too late; #Other
- ☐ Phishing, spear-phishing, whaling, vishing and other social engineering attacks and scams, particularly those compromising trusted, privileged and powerful insiders; #Confidentiality #Integrity #Availability
- ☐ Physical 'kinetic attacks' typically involving weapons, explosives, guns, missiles, mortars, bombs, electromagnetic pulse systems, tanks *etc.*; #Availability
- ☐ Physical disasters such as major storms, bush or city fires, floods and tsunamis destroying or degrading facilities, IT equipment, storage media and people; #Availability
- ☐ Physical lockouts due to excessive security or safety controls; #Confidentiality #Availability
- ☐ Power cuts, brownouts, surges, spikes *etc.*; #Availability
- ☐ Ransomware attack involving the theft and actual/threatened disclosure of sensitive information, in addition to encrypting vital corporate data and thereby preventing access to IT systems, decimating trust in IT, cybersecurity *etc.*; #Confidentiality #Integrity #Availability
- ☐ Reduction in business effectiveness or efficiency; #Integrity
- ☐ Reputational damage *e.g.* problems with information services that erode the trust or increase distrust by owners, customers, suppliers, regulators and the workforce, leading to brand devaluation and other adverse impacts *e.g.* limited commercial options, increased regulatory oversight; #Integrity
- ☐ Reverse-engineering of systems, applications, cryptographic functions *etc.* based on competent, painstaking analysis; #Confidentiality
- ☐ Ridicule leading to a loss of credibility and reputation *e.g.* for making outrageous claims or patently false or self-serving predictions; #Other

- ☐ Rogues, loose-cannons – people, apps, systems, organisations *etc*. that are unpredictable, unreliable and liable to bend or break rules (though not necessarily for bad reasons); #Confidentiality #Integrity #Availability
- ☐ Side-channel and back-channel attacks exploiting unintended mechanisms to pass or extract sensitive information from otherwise secure units such as cryptographic subsystems, modules, devices or organisations *e.g*. power consumption monitoring, Alternate Data Streams, microdots, remote command-and-control mechanisms; #Confidentiality
- ☐ Snooping, stalking and grooming of vulnerable targeted individuals; #Other
- ☐ Social distancing, isolation, exclusion, marginalisation; #Other
- ☐ Social, societal and cultural factors, social media, social interaction and influence generally; #Confidentiality #Integrity #Availability
- ☐ Spies and spooks – interpret these *extreme* information risks as you will; #Confidentiality #Integrity #Availability
- ☐ Spoofing – falsely purporting to be something, someone, somewhere *etc*. *e.g*. IP/DNS spoofing, caller identity spoofing, GPS/location spoofing, website spoofing (phishing), counterparty spoofing …; #Integrity
- ☐ Static discharge, lightning, inept handling and inadequate protection of static-sensitive devices; #Confidentiality #Integrity #Availability
- ☐ Strategic errors due to poor quality information, such as automating the wrong things or in the wrong ways; #Integrity #Availability
- ☐ Stress, burnout, overwork … leading to people making mistakes, errors of judgment, slip-ups *etc*. and under-performing; #Confidentiality #Integrity #Availability
- ☐ Stretching or embellishing the truth, elaborating on details, creatively joining-the-dots or plugging-the-gaps, creative fictions expressed as reality; #Integrity
- ☐ Subordination, politics and power-play – where low social status reduces the credibility, motivation and ability of individuals and groups to influence, make decisions and act, relative to those with higher status and power (both formal and informal); #Other
- ☐ Supply chain disruptions, incidents, breaches, perturbations, uncertainties *etc*. at any point upstream/downstream, including logistics, affecting or involving information, IT systems, services, support, maintenance, reliability, trustworthiness *etc*., especially in tightly-coupled just-in-time business networks; #Confidentiality #Integrity #Availability
- ☐ Surrogation – where a metric becomes the primary focus of attention and effort, rather than whatever is supposedly being measured (*e.g*. feedback ratings), or more generally where something or someone substitutes or stands in for another but provides inferior service, lacks experience *etc*.; #Integrity
- ☐ System administrator lockouts due to lost/forgotten passwords *etc*., or caused deliberately by brute force 'credential stuffing' attacks; #Confidentiality #Availability
- ☐ Technical failures or issues that corrupt data, applications, systems, communications, processes, messages, transactions *etc*.; #Integrity

- ☐ Temporary or permanent damage to/loss of valuable information storage media, either physically (*e.g*. stolen, discarded, destroyed) or logically (*e.g*. hacked, corrupted, infected); #Availability
- ☐ Theft and inappropriate exploitation of intellectual property such as sensitive proprietary or personal information (*e.g*. piracy, extortion) by insiders, outsiders or both (collusion); #Confidentiality
- ☐ Toxic (bad, nasty, unethical, oppressive, coercive, aggressive or dysfunctional) corporate or workplace or team cultures *e.g*. where the 'tone at the top' is off-key and counterproductive; #Confidentiality #Integrity #Availability
- ☐ Tunnel vision – a myopic or obsessive focus on something specific to the exclusion of other factors, aspects, goals, risks *etc*.; #Other
- ☐ Unappreciated/unrecognised inappropriate access to sensitive information, possibly over the medium or long term *e.g*. stealthy interception or bugging of various communications, systems, networks, offices, vehicles, homes …; #Confidentiality #Availability
- ☐ Unauthorised access to IT systems, networks, people, stored data, paperwork, files, backups, archives *etc*. by workers, visitors, intruders, onlookers, maintenance or cleaning or security staff, inspectors or auditors, out-of-hours/shift workers *etc*.; #Confidentiality
- ☐ Unauthorised and/or inappropriate modification, destruction or replacement of information, such as unauthorised changes to source code, compilers, libraries, modules, external functions and services, agreements, policies, procedures, contracts *etc*.; #Integrity
- ☐ Unauthorised, inappropriate or untimely disclosure of information through websites, emails, social media, text messages, phone calls, physical/verbal release *etc*.; #Confidentiality
- ☐ Unavailability of sufficiently-skilled, qualified, competent, experienced, capable and motivated people to complete necessary information-related activities within required timescales and budgets; #Availability
- ☐ Uncertainty and unpredictability generally – essentially anything less than absolute guaranteed certainty leaves some margin of possibility and the potential for harm *i.e*. residual risk; #Other
- ☐ Uncritical thinking, passively and naively accepting and believing information that may be partly or completely untrue and misleading; #Integrity
- ☐ Undue reliance and uncritical acceptance of job applicants' CVs, qualifications, claimed identities, suitability *etc*., and the converse *i.e*. candidates accepting positions based on misleading information about the organisation, job, responsibilities/expectations, manager, team, terms and conditions of employment *etc*. provided in job ads and interviews; #Integrity
- ☐ Undue reliance on fallible people (especially knowledge workers/professional specialists, creatives and lynch-pins such as founders and executives) who may leave or fail to perform adequately for reasons such as resignation/retirement, incompetence, accidents, overload/exhaustion, sickness/disease, addictions, self-interest, poaching by competitors, kidnapping, demotivation, redundancy or dismissal; #Availability
- ☐ Unduly constrained options *e.g*. when various possibilities are discounted irrationally, inappropriately or unnecessarily, or for personal rather than business reasons; #Other

- ☐ Unowned risks for which nobody is accountable and nobody believes themselves responsible; #Other
- ☐ Unreliability and unpredictability of IT systems, networks and/or people and organisations providing important information services, or in general – particularly uncertainties about what might or might not actually happen at some point under various circumstances, due to the combination of complexity, limited analysis and control, and seemingly/inherently random factors; #Availability
- ☐ Untrustworthy, fraudulent or compromised agents, intermediaries/middle-men, facilitators, advisors *etc*. - individuals, organisations or systems that fail to perform competently, fairly and in the interests of both parties as anticipated; #Confidentiality #Integrity #Availability
- ☐ Unwelcome and perhaps unrecognised errors affecting the completeness, accuracy or timeliness of information at any points in the course of communications (formulation, coding, transmission, carriage, reception, decoding and use) ; #Integrity
- ☐ Unworkable, unreasonable or unenforceable policies, procedures, laws, regulations, recommendations or expectations; #Other
- ☐ Vagueness in general – insufficient precision, accuracy, veracity, credibility, definition *etc*. (and yes there are indeed several examples in this very catalogue!); #Other
- ☐ Various situations (events, incidents, occurrences, attacks, infections, thefts, exploitations, mistakes, outages …) 'flying under the radar' *i.e*. going unrecognised, unnoticed, unappreciated or simply being ignored *e.g*. low-and-slow hackers or spies patiently grooming or probing a target over a long period, accumulating potentially useful information while building trust; #Availability
- ☐ Victims - vulnerable workers who are weak, withdrawn/meek, cognitively-challenged and easily (mis)led or coerced and exploited by others (insiders or outsiders); #Confidentiality #Integrity #Availability
- ☐ War, terrorism, extremism (whether declared openly or covert) and social disorder/disobedience *e.g*. riots, looking, violence, widespread noncompliance leading to a crackdown by the authorities, Marshall law; #Confidentiality #Integrity #Availability
- ☐ Whistleblowers – risky for them, risky for the organisation, risky all round!; #Confidentiality #Integrity
- ☐ Workers whose personal objectives and values do not adequately align with and support, enable or further the achievement of legitimate corporate objectives; #Confidentiality #Integrity #Availability
- ☐ Zero-day exploits compromising IT systems though previously unrecognised and as-yet unpatched bugs, flaws or operational issues; #Confidentiality #Integrity #Availability
- ☐ Zombie apocalypse/alien invasion … hinting at totally unanticipated left-field incidents, plus those superficially considered but then totally discounted and effectively ignored due to the belief that they will *never* happen and/or the inordinate costs and difficulties of addressing them (whether true or not); #Other

## Document history

This catalogue started out as a shorter checklist of information risks I prepared to help clients through the risk identification phase of risk analysis. Clause 6.1.3c) of ISO/IEC 27001 glibly advises readers to "apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system". That requirement begs more questions than it answers *e.g.*:

- What is "information security risk"?
- What is the "information security risk assessment process"?
- How does the process "identify risks"?
- What is supposed to be "in scope" of the ISMS – is that the information, the information security risks, or something else?
- What is the "scope" of the ISMS anyway?

I appreciate that's just me nit-picking at loose language as usual but look again: can *you* tell from the standard how risks are to be identified? I can't. My clients can't. It's not entirely obvious.

The information risk checklist I published to through ISO27k Toolkit in **November 2023** divides 80 generic information risks into those primarily affecting confidentiality, integrity or availability … plus an intriguing category of "other" information risks. Some of those others affect confidentiality, integrity *and* availability in various combinations. Some can affect confidentiality, integrity *or* availability depending on the nature of the incidents that play out. A few cause impacts that don't obviously relate to confidentiality, integrity or availability, at least not directly. Various risks affecting the information risk management process, for example, are hard to categorise. Are "knowledge gaps" and "limited creativity" about the non-availability of information? Hmmm, not really. How about the risks of failing to identify risks that later eventuate, or compliance/conformity risks? Um.

So, that set me thinking and led to this more elaborate catalogue released at the end of **January 2024**.

ISO/IEC 27002:2022 uses a handful of labels to tag and categorise information security controls. I have used a similar approach here by labelling the risks with 4 tags. If maintaining confidentiality is the main concern in a given situation (such as when developing the security design for an application system to handle persona, corporate or national secrets), risks tagged with #Confidentiality are probably worth considering. If data or system integrity is an important driver (a safety-critical or financial system, for example), browse or work your way systematically through the catalogue looking for #Integrity risks.

With over 200 risks in the catalogue, simply selecting by tags will generate a lengthy list … so you need to apply some commonsense rationalisation if you need a shortlist – perhaps picking out just the "key risks" or "cyber risks" (whatever that means to you), or risks not already under consideration in your risk assessment process. I cannot shortlist, characterise, quantify, evaluate or assess your information risks for you. I can barely even guess at the impacts of incidents that might be caused if the risks eventuate, and I have little knowledge of the relevant threats and vulnerabilities. Of course, if you engage me, I will gladly help you explore and figure things out. How about a remotely facilitated risk workshop or training session? An independent review and critique of your risk assessment report maybe? Something else? Let's talk!

Finally, if this checklist has inspired or annoyed you, if it is valuable in your work, if you spot duplications, errors and omissions, or have better ways to express things, *please* send me an email. *Your* information can help reduce *my* information risks. Thank you, good bye and good luck.

## Copyright



## Disclaimer

This is a *generic* list of information risks. It is incomplete and inaccurate. As provided, it is not definitive, comprehensive or suitable for any organisation, project or situation, not even IsecT Ltd, without customisation and interpretation. It is merely intended to stimulate creative thought. Use, adapt or ignore this information at your own risk … and don't come running to me with your broken leg.