Information risk checklist

November 2023 Release 1

Gary Hinson, IsecT Ltd.

This generic checklist supports the risk identification phase of an ISO/IEC 27001 **I**nformation **S**ecurity **M**anagement **S**ystem's information risk management process. **It is simply a starting point, a stimulating but incomplete and potentially inaccurate or misleading prompt that needs to be interpreted or adapted according to the situation.** Think outside the box! Get creative! For further guidance, a more detailed and comprehensive version can be purchased through SecAware.com.

Confidentiality risks

- ☐ Attacks by cybercriminals, hackers or spooks
- ☐ Evasion or disabling of access controls
- ☐ Inappropriate disclosure, interception or theft of sensitive information
- ☐ Inappropriate/unethical/illegal exploitation of intellectual property
- ☐ Inappropriate surveillance
- ☐ Leakage of sensitive information via third parties
- ☐ Other unauthorised and inappropriate access to or release of sensitive information

Integrity risks

- ☐ Bad advice, bad decisions
- ☐ Bias, discrimination and prejudice
- ☐ Bribery and corruption, including IT system/data corruption
- ☐ Bugs
- ☐ Change management/change and version control Issues
- ☐ Communications errors
- ☐ Compliance or conformity failures
- ☐ Cyberattacks
- ☐ Deceit
- ☐ Delusions, hallucinations, excessive creativity, logical errors, fallacies
- ☐ Design flaws
- ☐ Ethical failures
- ☐ Falsification, fakery, counterfeiting and piracy
- ☐ Fragility
- ☐ Fraud
- ☐ Malware infection

- ☐ Misattribution. mis-classification, misdirection, dis/misinformation, misinterpretation, misunderstanding, misleading, mistranslation
- ☐ Inaccurate, incomplete or out-of-date information
- ☐ Stretching the truth, bending the rules
- ☐ Unauthorised modification, destruction or replacement of information
- ☐ Zero-day exploits against previously-unrecognised and as-yet-unpatchable bugs or flaws
- ☐ Other causes of inadequate accuracy, completeness, relevant and timeliness of information

Availability risks

- ☐ Corruption or loss of valuable/vital business information
- ☐ Cybertage – sabotage of IT equipment, media or data
- ☐ Defection of knowledge workers to competitors
- ☐ Delays and interruptions to information services
- ☐ Denial-of-service attacks plus unintentional disruptions
- ☐ Destructive cyberattacks and other seriously disruptive incidents
- ☐ Gradual or sudden loss of information
- ☐ Hardware, software, system or service failures
- ☐ Health and safety issues/incidents
- ☐ Human errors and mistakes
- ☐ Inadequate capacity and performance
- ☐ Natural events and accidents
- ☐ Physical attacks involving the use of destructive weapons against people and facilities
- ☐ Power cuts, brownouts, surges, spikes *etc*.
- ☐ Unrecognised, unnoticed or unappreciated incidents
- ☐ Dependencies plus unreliability and unpredictability in general

Other information security risks

- ☐ **A**dvanced **P**ersistent **T**hreats, spies and spooks
- ☐ Collisions, conflicts and delays in overloaded networks or systems
- ☐ Covert backdoors or loopholes
- ☐ Crypto-ransomware
- ☐ Exploitable architectural or design flaws
- ☐ Inability to access and use/administer systems, data, facilities, people *etc*.
- ☐ Incompetence and negligence
- ☐ Ineffective controls
- ☐ Inept or incompetent information security management and governance failures
- ☐ Information overload

- ☐ Loss or theft of security tokens and passwords
- ☐ Misconfiguration, misidentification and misuse of information
- ☐ Personal issues affecting cognitive capabilities, recall, performance and judgment
- ☐ Rogues
- ☐ Security control failures
- ☐ Social engineering, social factors, social media and social interactions
- ☐ Overload, stress, burnout
- ☐ Toxic cultures, dysfunctional relationships
- ☐ Untrustworthy partners
- ☐ War, terrorism and extremism

Other information risks

- ☐ Breaches of contracts, agreements and understandings, broken promises
- ☐ Carelessness, negligence, thoughtlessness
- ☐ Changes in the risk landscape, technologies, business *etc*.
- ☐ Inadequate risk management *e.g*. excessive risk-aversion, unowned risks
- ☐ Insider threats
- ☐ Knowledge gaps
- ☐ Limited creativity, lack of innovation
- ☐ Noncompliance and nonconformity
- ☐ Paranoia, irrational fears and anxieties
- ☐ Perfectionism and procrastination
- ☐ Supply chain issues, breaches, incidents, disruptions …
- ☐ Underinvestment
- ☐ Unforeseen/unexpected events and challenging situations
- ☐ Unreasonable resistance to change
- ☐ Unworkable rules, requirements or expectations
- ☐ Vagueness and uncertainty in general

Copyright