**Information Security Management System**

# Information asset checklist

Control 5.9 in ISO/IEC 27002:2022 recommends that “An inventory of information and other associated assets, including owners, should be developed and maintained … to identify the organization’s information and other associated assets in order to preserve their information security and assign appropriate ownership.” Thesupporting advice mentions just a few examples of information assets, hence **it is not entirely clear from the standard *which* ‘information and other associated assets’ an organization’s Information Security Management System is intended to protect.**

This checklist illustrates a selection of typical information assets. It is incomplete, a prompt set you thinking about the information assets relevant to *your* organisation. Please adapt it to suit your specific circumstances and needs.

## Pure information (content) assets

### Digital data

⎕ The data *content* of digital storage media

⎕ Personal, financial, legal, research and development, strategic and commercial data

⎕ Emails, voicemails and other inter-personal messages

⎕ Databases

⎕ Digital data backups

⎕ Cryptographic keys, hash codes, algorithms

⎕ Data in transit

### Tangible information assets

⎕ Personal, financial, legal, research and development, strategic and commercial documents

⎕ Contracts and agreements (particularly the final, signed/executed versions)

⎕ Policies, procedures, guidelines, checklists

⎕ Data storage *media*

### Intangible information assets

⎕ Brands

⎕ Workers’ knowledge, skills, capabilities

⎕ Trade secrets

⎕ Intellectual property

⎕ Business relationships

### Application software

⎕ Commercial off-the-shelf packages

⎕ Cloud and mobile apps

⎕ Client-server software

⎕ Custom-written or customised applications

⎕ ERP, MIS, CRM, ISMS

⎕ Middleware, shareware, freeware, abandonware

### Operating system software

⎕ Operating systems

⎕ BIOS, firmware, boot loaders

## Physical IT assets

### IT support infrastructure

⎕ IT buildings, data centres, server/computer rooms, LAN/wiring closets

⎕ Offices

⎕ Media storage rooms, libraries, archives

⎕ Personnel identification and authentication/access control devices and tokens

### IT environmental controls

⎕ Fire alarms/suppression/fire-fighting equipment

⎕ Uninterruptible power supplies (UPSs)

⎕ Air conditioners/water chillers

### IT hardware

⎕ Computing and storage devices

⎕ Network and communications devices

## Information service assets

⎕ User authentication services

⎕ User administration processes and services

⎕ Network services (wired and wireless)

⎕ Help Desk/s

## Human information assets

### Employees

⎕ Staff and managers (particularly those in key knowledge management roles)

⎕ Senior/executive managers

⎕ Specialists/professionals

### Non-employees

⎕ External consultants/specialist advisors and contractors

⎕ Temporary workers, interns, secondees