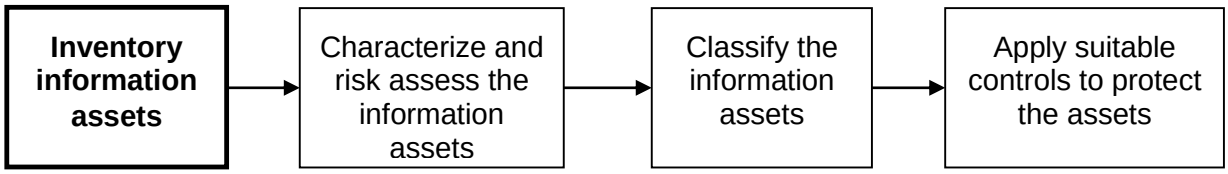
Information asset inventory/register

Version 3 16th October 2007

Introduction

One of the first jobs to do when implementing an ISO/IEC 27000-series Information Security Management System (ISMS) is to create an inventory/register of the information assets requiring protection. The information assets will subsequently be risk assessed, classified and secured.



If the ISMS is to be comprehensive, it is important that the asset inventory/register is reasonably complete. This document gives you a structure to work from, a starting point to get you thinking about all the information assets you have. You will need to adapt it to suit your specific circumstances, setting up an inventory list, asset register or database of your information assets. Be absolutely certain to cover all the organization's most valuable information assets (the 'crown jewels') but don't worry too much about the minor or insignificant information assets - they should be covered by the general baseline security controls anyway.

Pure information assets

Digital data

Personal, financial, legal, research and development, strategic and commercial, email, voicemail, databases, personal and shared drives, backup tapes/CDs/DVDs and digital archives, encryption keys

Tangible information assets

Personal, financial, legal, research and development, strategic and commercial, mail/post, FAXes, microfiche and other backup/archival materials, keys to safes/offices and other media storage containers, Journals, magazines, books

Intangible information assets

Knowledge, business relationships, trade secrets, licenses, patents, trademarks, accumulated experience and general know-how, corporate image/brand/commercial reputation/customer confidence, competitive advantage, ethics, productivity

Application software

In-house/custom-written systems, client software (including shared or single-user 'End User Computing' desktop applications), 'commercial off-the-shelf' (COTS), ERP, MIS, databases, software utilities/tools, eBusiness applications, middleware

Operating system software

For servers, desktops, mainframes, network devices, handhelds and embedded systems (including BIOS and firmware)

Physical IT assets

IT support infrastructure

IT buildings, data centers, server/computer rooms, LAN/wiring closets, offices, desks/drawers/filing cabinets, media storage rooms and safes, personnel identification and authentication/access control devices (turnstiles, card-access systems *etc*.) and other security devices (CCTV *etc*.)

IT environmental controls

Fire alarms/suppression/fire fighting equipment, uninterruptible power supplies (UPSs), power and network feeds, power conditioners/filters/transient suppressors, air conditioners/chillers/alarms, water alarms

IT hardware

Computing and storage devices *e.g*. desktops, workstations, laptops, handhelds, servers, mainframes, modems and line terminators, communications devices (network nodes), printers/copiers/FAX machines and multifunction devices

IT service assets

User authentication services and user administration processes, hyperlinks, firewalls, proxy servers, network services, wireless services, anti-spam/virus/spyware, intrusion detection/prevention, teleworking, security, FTP, email/IM *etc*., Web services, software maintenance and support contracts

Human information assets

Employees

Staff and managers, particularly those in key knowledge management roles such as senior/executive managers, software architects/developers/testers, systems managers, security administrators, operators, legal and regulatory compliance people, power users, local IT / IT security administrators and "go-to" people in general

Non-employees

Temporary workers, external consultants/specialist advisors, specialist contractors (*e.g*. those who understand maintenance of the physical IT environment), suppliers and business partners ...

Implementation hints

Many information assets would have been inventoried for "Y2k". Do you still have the records? You might be very lucky and find someone has maintained the Y2k database of all your systems, applications *etc*. (some hope!). Alternatively your Business Continuity and Disaster Contingency function (if it exists) should already have details of the most important information and IT assets supporting business-critical processes. Maybe IT or Finance or Procurement have IT systems inventories for their own purposes?

Copyright