Just do anything!

What do you mean…Are there standards?

Whether we like them or not, there are standards, laws and frameworks in which we are bound to operate, especially where there are legal and financial aspects concerned. It is important we have some idea of what these are to manage the risk to organisations.

"Knowledge, like air, is vital to life. Like air, no one should be denied it."
Alan Moore

Don't get scared of the direction we're going…there are actually some benefits (!) that come along with knowing this stuff:

•**Safety and reliability** – Standards help ensure safety, reliability and environmental care resulting in the perception standardised products and services as more dependable, raising user confidence, increasing sales and the take-up of new technologies.

•**Support of government policies and legislation** – Standards and laws protect users and business interests while supporting government policies.

•**Maintain order** - Laws make certain that disputed or doubtful claims can be resolved in a peaceful manner at the appropriate level.

- **Interoperability** – The ability to work together from countries down to the device level relies on complying with standards.
- **Business benefits** – Standards and laws provide a solid foundation upon which to develop new technologies and to enhance existing practices while providing protection and clear guidelines including safety requirements.
- **Choice** - Standards provide the **foundation for new features** and options enhancing our daily lives.

There are specific standards, laws and frameworks we need to be aware within the ITAM community. The following is a list of the more dominate standards affecting ITAM.

As always: "Please check on the local conditions to ensure all relevant standards, laws and frameworks are being considered in your situation".

ISO 19770 – ITAM Standards and Interaction

The ISO 19770 standard provides the concept of ITAM standardization, specifically Software Asset Management (SAM). It provides organizations of all sizes with information and assistance for risk and costs minimisation. This allows a competitive advantage to be gained through:

- Management of the risk of interrupted IT service delivery, breach of legal agreements and audit.
- Reducing overall software costs through the implementation of various processes.
- Better information availability leading to improved decision-making based on accurate data

ISO 19770 is split into five parts:

1) **ISO/IEC 19770-1:2012** Processes and tiered assessment of conformance which is a process framework to enable an organization to prove that it is performing IT Asset Management to a standard sufficient to satisfy corporate governance requirements and ensure effective support for IT service management overall.

2)**ISO/IEC 19770-2:2009**- Software identification tag - provides an ITAM data standard for unique identification of software (SWID) tags. These tags are created:

a)By a software creator or publisher as part software,

b)By organisations for software that doesn't have a tag, and

c)By 3rd party tools when software is discovered without a tag.

3)**ISO/IEC DIS 19770-3** – Currently in Draft, Software entitlement schema will provide a technical definition of an XML schema to encapsulate the details of software entitlements, including usage rights, limitations and metrics. The idea is to provide uniform, measurable data for both license compliance and license optimization processes of the SAM practice.

4) **ISO/IEC CD 19770-4** – This standard provides details resource utilization measurement information (RUM) structures. This standard will make use of ISO/IEC 19770-2:2009 and ISO/IEC 19770-3 protocols allowing greater ITAM process automation.

5) **ISO/IEC 19770-5:2015** - Contains an overview and vocabulary:

a) An overview of the ISO/IEC 19770 family of standards,

b) An introduction to IT asset management (ITAM) and software asset management (SAM),

c) A brief description of the foundation principles and approaches on which SAM is based, and

d) Consistent terms and definitions for use throughout the ISO/IEC 19770 family of standards.

(The years suffix shows revisions to the standards)

ISO 20000 - IT Service Management and IT Governance

ISO/IEC 20000 is the first international standard for IT service management and was updated in 2012. Originally, it was developed to reflect best practice guidance contained within the ITIL framework, and supports other IT service management frameworks and approaches including Microsoft Operations Framework and components of ISACA's COBIT framework.

The parts within the standard are:

1) ISO/IEC 20000-1:2011 - Service management system requirements.

2) ISO/IEC 20000-2:2012 - Guidance on the application of service management systems.

3) ISO/IEC 20000-3:2012 - Guidance on scope definition and applicability of ISO/IEC 20000-1

4) ISO/IEC TR 20000-4:2010 - Process reference model

5) ISO/IEC TR 20000-5:2013 - Implementation plan for ISO/IEC 20000-1

6) ISO/IEC CD 20000-6 – (*Under Development*) Requirements for bodies providing audit and certification of service management systems

7) ISO/IEC WD 20000-8 - (*Under Development)* Guidance on the application of service management systems for smaller organizations

8) ISO/IEC TR 20000-9:2015 - Guidance on the application of ISO/IEC 20000-1 to cloud services

9) ISO/IEC PRF TR 20000-10 - (*Under Development*) Concepts and terminology for ISO/IEC 20000-1. Currently being developed.

10) ISO/IEC PRF TR 20000-11 - (*Under Development*) Will provide guidance on the relationship between ISO/IEC 20000-1 and ITIL.

11) ISO/IEC PDTR 20000-12 - (*Under Development*) Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: CMMI-SVC

IAITAM IBPL

The IAITAM Best Practice Library provides the what, why and how of ITAM. It addresses a number of standards such as ISO 19770 and the ISO 20000, and regulations such as Sarbanes-Oxley and HIPAA. IAITAM's mission is to be the principal resource for comprehensive IT Asset Management best practices worldwide They provide ITAM specific certification training through accredited agencies such as Burswood Information Solutions.

There are twelve volumes in the IBPL addressing twelve Key Process Areas (KPA's):

- Acquisition Management
- Asset Identification
- Communication and Education
- Compliance Management
- Disposal Management
- Documentation Management
- Financial Management
- Legislation Management
- Policy Management
- Program Management
- Project Management
- Vendor Management

ISO 55000 – General Asset Management

- **ISO 55000:2014** - This document provides an overview of asset management, its principles and terminology, and the expected benefits from adopting asset management. This allows the principles of asset management to be applied to all types of assets and by all types and sizes of organizations.
- **ISO 55001:2014** - Specifies requirements for an asset management system within the context of the organization.
- **ISO 55002:2014** - Provides guidance for the application of an asset management system, in accordance with the requirements of ISO 55001.

Microsoft SAM Optimization Model

The Microsoft SAM Optimization Model provides guidance for implementation of a SAM program aligned with the ISO 19770-1 standard. It provides a tactical framework to evaluate your SAM policies without having to interpret and adapt ISO 19770-1.

Microsoft SOM uses tipping points to establish an organisation SAM maturity, and plot a path for ongoing improvement. Organisational maturity is measured and ranked in one of four levels (Basic, Standardized, Rationalized and Dynamic) across 10 competencies. The SAM Optimisation Model Key Competencies are aligned and mapped to the key categories and requirements from the ISO 19770-1. There are templates, guides, checklists and documents to assist, with a focus on Microsoft and Microsoft license state reporting.

ISO 27000 Information Security Management

The ISO 27000 family of standards helps organizations keep information assets secure and is a specification for an information security management system (ISMS). The series is deliberately broad in scope, covering more than just privacy, confidentiality and IT or technical security issues. It is applicable to organizations of all shapes and sizes.

Organisations which meet the standard may gain an official certification issued by an independent and accredited certification body on successful completion of a formal audit process.

Benefits to be realised from the standard include:

- Identification of risks allowing controls to be put in place to manage or reduce them
- Provides flexibility to adapt controls to all or selected business areas
- Assist with gaining stakeholder and customer trust that their data is protected
- Demonstrates compliance and assists with gaining status as preferred supplier
- Meet more tender expectations by demonstrating compliance

DoD 5220.22-M Data Erasure

DoD 5220.22-M is a software based data sanitisation method used in various file shredder and data destruction programs to overwrite existing information on a hard drive or other storage device.

Erasing a hard drive using the DoD 5220.22-M data sanitisation method will prevent all software based file recovery methods from lifting information from the drive and should also prevent most if not all hardware based recovery methods.

It is usually implemented in the following way:

- **Pass 1:** Writes a zero and verifies the write
- **Pass 2:** Writes a one and verifies the write
- **Pass 3:** Writes a random character and verifies the write

You might also come across various iterations of DoD 5220.22-M including DoD 5220.22-M (E), DoD 5220.22-M (ECE), or others. Each will probably use a character and its compliment (as in 1 and 0) and varying frequencies of verifications.

Basel Convention – Hazardous Waste Disposal

We need to be aware of this in the IT Project and Asset Management space as we deal with disposal of the assets at various time. Gone are the days of throwing items into a dumpster or burying items in the ground. Many assets have dangerous waste products including mercury, PCBS, cadmium and other toxins. How dispose of these items is of concern for our own safety and the environment.

The **Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and Their Disposal**, usually known as the **Basel Convention. It is** an international treaty that was

designed to reduce the movements of hazardous waste between nations, and specifically to prevent transfer of hazardous waste from developed to less developed countries (LDCs).

There are also stringent requirements for notice, consent and tracking for movement of wastes across national boundaries. The Convention places a general prohibition on the exportation or importation of wastes between Parties and non-Parties. The exception to this rule is where the waste is subject to another treaty that does not take away from the Basel Convention. The United States has signed the convention but is to ratify it however they have a number of such agreements for allowing the shipping of hazardous wastes to Basel Party countries.

In Australia, the Product Stewardship Act 2011 introduced new legislation and provided a framework for developing legislatively backed product stewardship for Australia. Product Stewardship Australia (PSA) is a not-for-profit organisation established by the television industry to lead the way in developing recycling programs for e-waste in Australia, particularly televisions. PSA works closely with both state and federal governments along with other industry associations in advancing stewardship.

New Zealand signed the Basel Convention in 1989 and ratified it in 1994. The Government initiated a Waste Minimization Act in 2008 to deal with waste streams and ultimately the impact on the environment of wastes. An eDay for collection began in 2006 but stopped in 2012.

R2:2013 – Responsible Recycling

This standard provides additional emphasis on disposing of goods properly and provides the governance structure to ensure tractability. This is a standard that can be used in part of the decision for disposal by IT Project and Asset Managers.

The standard was originally developed in 2008 through a joint process convened by the U.S. Environmental Protection Agency and involving electronics recyclers and refurbishers, manufacturers, retailers, non-profit organizations and other stakeholders.

The overall goal of R2:2013 is to help IT asset disposition (ITAD) companies optimize their systems and practices and, by certifying to its requirements, assure their upstream clients that they are fully addressing potential risks to brand and potential legal and financial liabilities.

The R2:2013 Standard is the latest version of R2, the electronics recycling industry's leading certification. Each provision of the R2 Standard is designed to help ensure the quality, transparency, and environmental and social responsibility, of R2 Certified electronics recycling facilities.

The R2 Standard consists of 13 provisions. The most significant change to the R2 program is the requirement for all R2 facilities to have an approved environmental, health and safety management system (EHSMS). Currently approved management systems include a combination of ISO 14001 and OHSAS 18001 or the Recycling Industry Operating Standard (RIOS™) system. The EHSMS requirement improves the integrity and accountability of the entire R2 certification.

Further information can be obtained here.

Berne Convention – International Copyright Treaty

The Berne Convention for the Protection of Literary and Artistic Works, usually known as the Berne Convention, is an international agreement governing copyright, which was first accepted in Berne, Switzerland, in 1886.

The Berne Convention formally mandated several aspects of modern copyright law; it introduced the concept that a copyright exists the moment a work is "fixed", rather than requiring registration. It also enforces a requirement that countries recognize copyrights held by the citizens of all other signatory countries.

Broadly speaking, each convention member country gives the same rights to the nationals of other convention countries as it gives to its own nationals under its own law. The laws of members of the conventions or treaties must conform with the minimum rights specified in the conventions or treaties.

The USA has the basis of its copyright law instituted as Copyright Act of 1976 under Title 17 (United States Code) with criminal law breaches up to $250,000 per infringement. The **Digital Millennium Copyright Act (DMCA)** 1998 criminalises production and dissemination of technology, devices, or services intended to circumvent measures (commonly known as digital rights management or DRM) that control access to copyrighted works. It also criminalises the act of circumventing an access control, whether or not there is actual infringement of copyright itself.

Australia has the Copyright Act 1968 and the Copyright Amendment Act 2006 with Copyright Amendment (Online Infringement) Bill 2015 introduced for ratification plus other amendments to keep the laws current. Penalties of $60,000 for an individual or $300,000 for a company are in place.

New Zealand Copyright Act 1994 automatically extends copy right to relevant material.
The Copyright (New Technologies) Amendment Act 2008 contains amendments to the Copyright Act which were put in place to update New Zealand's copyright law to reflect advances in digital technology. Click here to view the amending act.
The Copyright (Infringing File Sharing) Amendment Act 2011 contains amendments to the Copyright Act which were put in place in order to address the issue of infringing file sharing. Criminal liability can attract fines of up to $150,000 and imprisonment for up to 5 years.

Sarbanes-Oxley

The Sarbanes-Oxley Act 2002 (abbreviated as SOX), also known as the Public Company Accounting Reform and Investor Protection Act 2002, is a United States federal law enacted after several major corporate and accounting scandals. More detail on SOX and be found on Wikipedia or through the USA SEC.

This Act triggered reviews in Australia and New Zealand strengthening local corporate compliance. In Australia details of accounting standards can be found here. In New Zealand the regulations include the NZ IFRS with details here.

An overview of the SOX Act is:

1. **Public Company Accounting Oversight Board** (PCAOB) - Details which provide independent oversight of public accounting firms providing audit services, auditor registration, audit processes and procedures, conduct and quality control and enforcement of SOX mandates.
2. **Auditor Independence -** Establishes standards for external auditor independence, to limit conflicts of interest and other auditor requirements

3. **Corporate Responsibility Mandates** - Which mandates senior executives take individual responsibility for the accuracy and requirements for financial transactions
4. **Analyst Conflicts of Interest** - Defines the codes of conduct for securities analysts and requires disclosure of knowable conflicts of interest.
5. **Commission Resources and Authority** - Defines the SEC's completeness of corporate financial reports, behavior requirements and con-compliance penalties
6. **Enhanced Financial Disclosures** - Describes enhanced reporting authority to censure or bar securities professionals from practice and defines conditions under which a person can be barred from practicing as a broker, advisor, or dealer.
7. **Studies and Reports** - Requires the Comptroller General and the SEC to perform various studies and report their findings.
8. **Corporate and Criminal Fraud Accountability** - Describes specific criminal penalties for manipulation, destruction or alteration of financial records or other interference with investigations, while providing certain protections for whistle-blowers.
9. **White Collar Crime Penalty Enhancement** - Recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense associated with white-collar crimes and conspiracies.
10. **Corporate Tax Returns** - States that the Chief Executive Officer should sign the company tax return.
11. **Corporate Fraud Accountability** - Identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It includes sentencing guidelines and strengthens their penalties

COBIT

Control **Ob**jectives for **I**nformation and Related **T**echnology (COBIT) is a framework created by ISACA for information technology (IT) management and IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. The framework supports governance of IT by defining and aligning business goals with IT goals and IT processes.

ITAM can make use of objectives and details in COBIT where the organisation utilises COBIT Principles. Security is well defined and should be considered.

The COBIT 5 framework is built on five basic principles, and includes extensive guidance on enablers for governance and management of enterprise IT.

The COBIT 5 product family includes the following products:

1. COBIT 5 (the framework)
2. COBIT 5 enabler guides, in which governance and management enablers are discussed in detail. These include:
    a. *COBIT 5: Enabling Processes*
    b. COBIT 5: Enabling Information (in development)
    c. Other enabler guides (check *www.isaca.org/cobit*)
3. COBIT 5 professional guides, which include:
    a. *COBIT 5 Implementation*
    b. COBIT 5 for Information Security (in development)
    c. COBIT 5 for Assurance (in development)

d. COBIT 5 for Risk (in development)
e. Other professional guides (check *www.isaca.org/cobit*)

UNSPSC® United Nations Standard Products and Services Code®

This is a standard for efficient, accurate classification of products and services. The standard is useful as it provides a standard categorization naming and identification convention (hierarchically) which could be used in most systems.

Officially – "UNSPSC is a flexible classification system for achieving company-wide visibility of spend analysis, as well as enabling procurement to deliver on cost-effectiveness demands and allowing full exploitation of electronic commerce capabilities".

Encompassing a five level hierarchical classification codeset and over 17,000 items, UNSPSC enables analysis by drilling down through the grouping levels.

HIPAA Health Insurance Portability and Accountability Act

An ITAM Manager needs to be aware of HIPAA (especially in the USA) as part of the lifecycle and especially during disposal actions.

This is a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.

The standards provide patients with access to their medical records and control over how their personal health information is used and disclosed. They represent a uniform, federal floor of privacy protections for consumers across the country. State laws providing additional protections to consumers are not affected by this new rule. HIPAA took effect on April 14, 2003.

In Australia the Privacy Act 1988 (Privacy Act) regulates the handling of personal information about individuals. This includes the collection, use, storage and disclosure of personal information, and access to and correction of that information

In New Zealand the Privacy Act 1993 covers much of what is integral to HIPAA. The Privacy Commissioner site gives very good guidelines, assessment and information.

DAM - Digital Asset Management

Digital assets are becoming very relevant in todays world due to the proliferation of digital assets and media. This will become an extension of ITAM (if it isn't already) as part of the documentation and management requirements of the role and worth mentioning here.

A digital asset in essence is anything that exists in a binary format and comes with the right to use. Files that do not possess the right to use are not considered assets. Digital assets are classified as images, multimedia and textual content files.

The legal terms "digital asset" refers, but is not exclusive to, files, including but not exclusive to, electronic mails, digital documents, audible content, motion picture, and relevant digital files that are currently in circulation or are to, or will be.

These files can be stored on digital appliances, including, but not exclusive to, personal computers, laptops, portable media players, tablets, storage devices, telecommunication devices, and any and all apparatuses which are in existence or are to, or will be once technology progresses to accommodate for the conception of new modalities which would be able to carry digital assets; notwithstanding the proprietorship of the physical device onto which the digital asset is located.

DAM refers to the protocols for downloading, renaming, backing up, rating, grouping, archiving, optimizing, maintaining, thinning, management, organization, distributing and exporting files.

There are 2 basic metadata schemas used to describe the data:

- Dublin Core - The **Dublin Core Schema** (ISO 15836:2009) is a small set of vocabulary terms (55) that can be used to describe web resources (video, images, web pages, etc.), as well as physical resources such as books or CDs, and objects like artworks abstracts.
- PB Core - The **PBCore** standard is built on the foundation of the Dublin Core (ISO 15836), an international standard for resource discovery, and has been reviewed, though not endorsed, by the Dublin Core Metadata Initiative Usage Board. PBCore extends Dublin Core by adding a number of elements specific to audio visual (AV) assets. These AV assets can be physical analogue media items, or digital media objects.

In conclusion, there are a variety of standards, laws and frameworks we need to be aware in the IT and the ITAM space. We can't ignore and likewise, we aren't restricted by them. There is enough flexibility to be able to operate without infringement while maintaining good corporate and business governance. Being aware and maintaining that knowledge is essential as part of our role as IT professionals and IT Asset Managers.