The Organisation As A System

The Old Geek

Structured Coherent Design

14. Document Management – Security

14. Document Management – Security

The slide deck set:

- 1. Introduction – document management, why do it

The Operating Environment

- 2. Document Life Cycle– Documents have lives of their own…
- 3. The Building Blocks – Its all about the architecture
- 4. Documents Are Packages – Document files have form, function and purpose beyond just the content
- 5. Legal Considerations – You are all international lawyers now
- 6. Infrastructure – You need to find a home, one that is safe…..
- 7. Meta Data. "Data" about data.
- 8. Naming Convention – Privacy by design starts here

The Architecture

- 9. Document Design. If there is a requirement to tap into documents for data analysis purpose.. They must be designed.
- 10. Corporate Dictionary –Not as many words as you think
- 11. Location – Location, if you do not know where something should be, it may as well not be there!
- 12. Writing with style, People do what people do, therefore, with the lightest touch, let them do that, but order their work.
- 13. The Tool Architecture – No one tool can cover it all and cookies? They don't count.
- 14. Security Considerations you can't ignore the "S" word.

- 15. Key Players People do what people do.
- 16. Closing Summary - Wrap up..

14. Document Management – Security

Revision

Viewers who have not done so may find is useful to review the following slide decks in the series

- 2. Document Life Cycle– Documents have lives of their own…
- 4. Document Are Packages – Nowadays document files are composites.
- 11. Location – Location, if you do not know where something should be, it may as well not be there!
- 13. The Tool Architecture – No one tool can cover it all and cookies? They don't count.

14. Document Management – Security

Introduction

Document Management has security implications. This deck, supported by the others in the series, set out the need for a document management security policy, but does so within the context of an ISO 27001 compliant Information Security Management System (ISMS) or something similar

14. Document Management – Security

Caveats

This slide deck does not attempt to address the full scope of the security risk and associated policy and governance issues and instead focusses on some guidance on matters to do with document security specifically.

This deck has its basis in the Microsoft Windows series of operating systems. What is described and referred to in this deck will have their equivalents with the other majors.

14. Document Management – Security

The Security Risk

The security risk is multi dimensional and multi impact, the impact being felt and seen in the rise in computer related crime. So much so that, as an indicator, insurance costs are rising with the assessment of risk making insurance untenable for many as the LinkedIn post available here indicates

The security risk is multi dimensional and multi impact, the impact being felt and seen in the rise in computer related crime. So much so that, as an indicator, insurance costs are rising with the assessment of risk making insurance untenable for many as the LinkedIn post available here indicates

Arguably, above all, failure to secure your information is a commercial risk, an existential one at that.

14. Document Management – Security

The ISMS

Document Management policy is subordinate to security policy. Where there is any conflict of interest, Security Policy will take precedence.

End of!

Supporting this series of decks and templates is an ISO 27001:2013 template library available on request. The front page of which can be viewed here

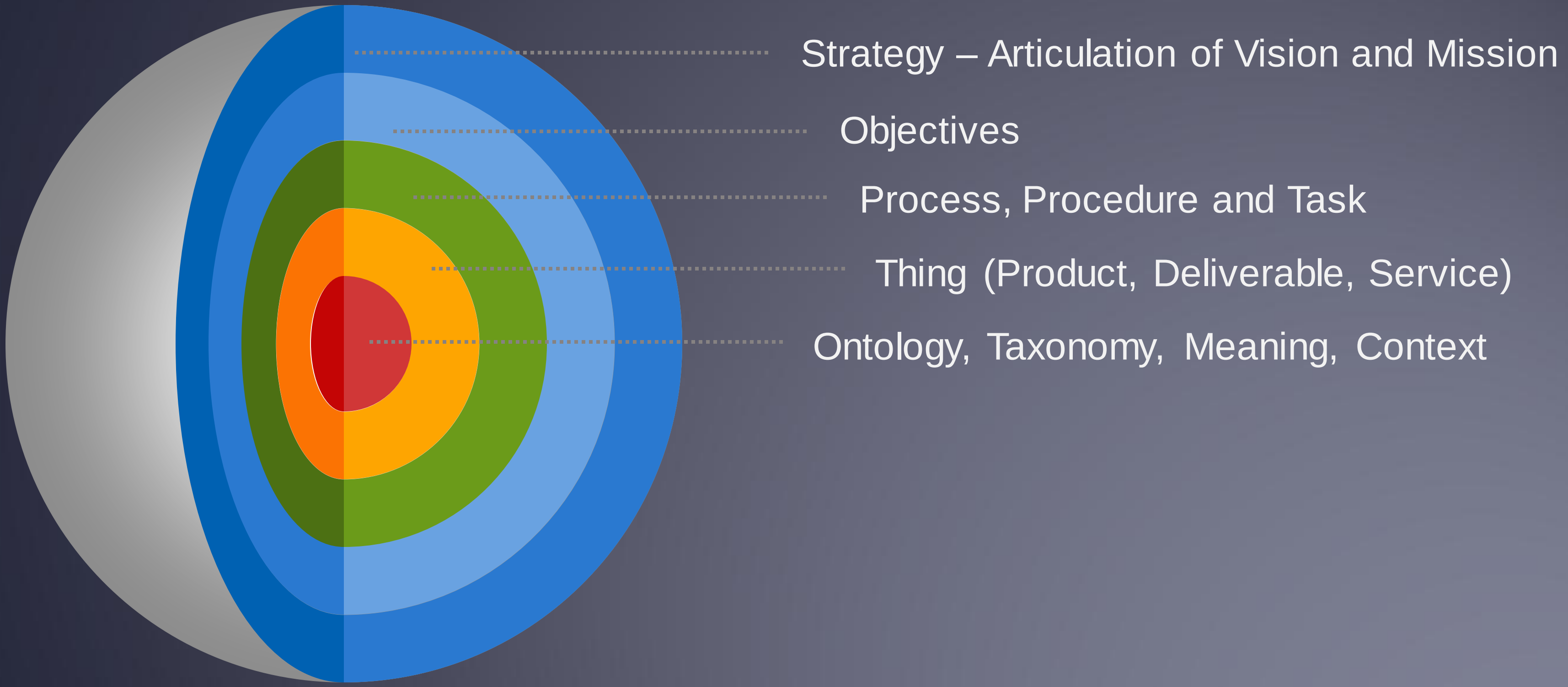
Writing an ISMS is an evolutionary process, one that should be subject to regular review and revision.

14. Document Management – Security

Policy and Governance

1. Document Management - Introduction

Your Documents Are Part Of A Layered Information Management Architecture



Strategy – Articulation of Vision and Mission

Objectives

Process, Procedure and Task

Thing (Product, Deliverable, Service)

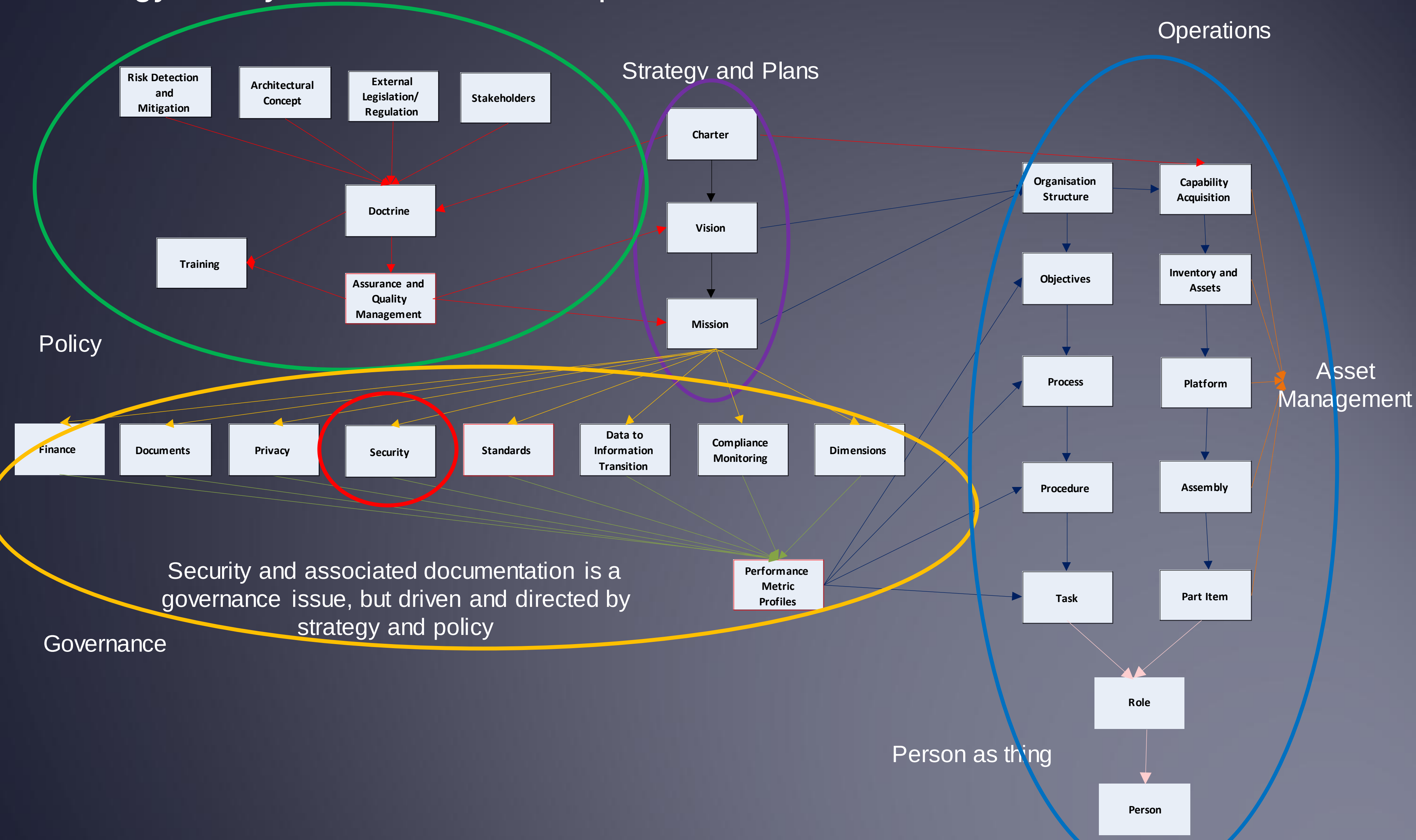
Ontology, Taxonomy, Meaning, Context

A set of conceptual architectural schematics is available here

The Old Geek

14. Document Management – Security

Strategy, Policy, Governance and Operations



Security and associated documentation is a governance issue, but driven and directed by strategy and policy

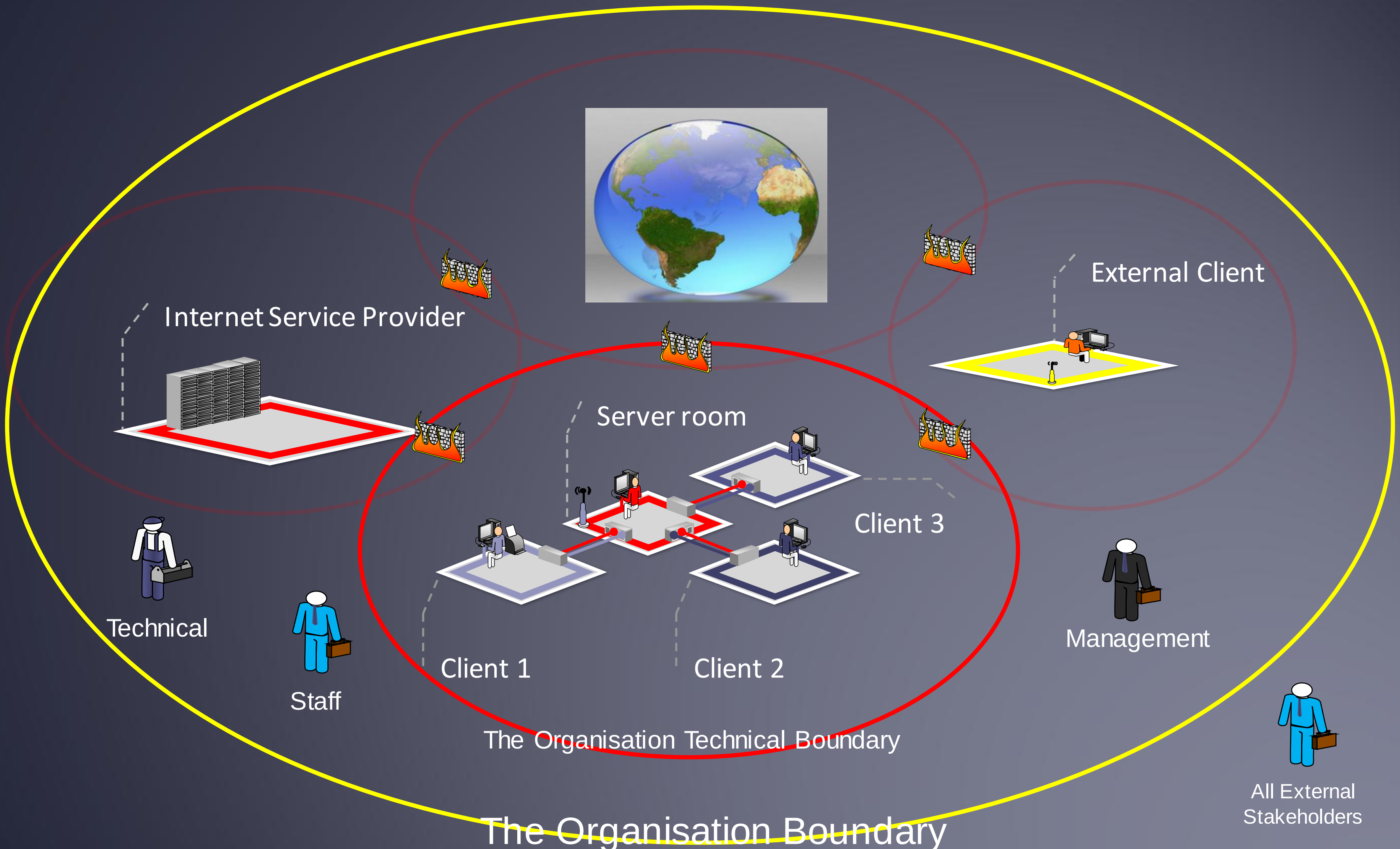
High Level Document Classification By Type

14. Document Management – Security

Security And The Organisation Boundary

14. Document Management – Security

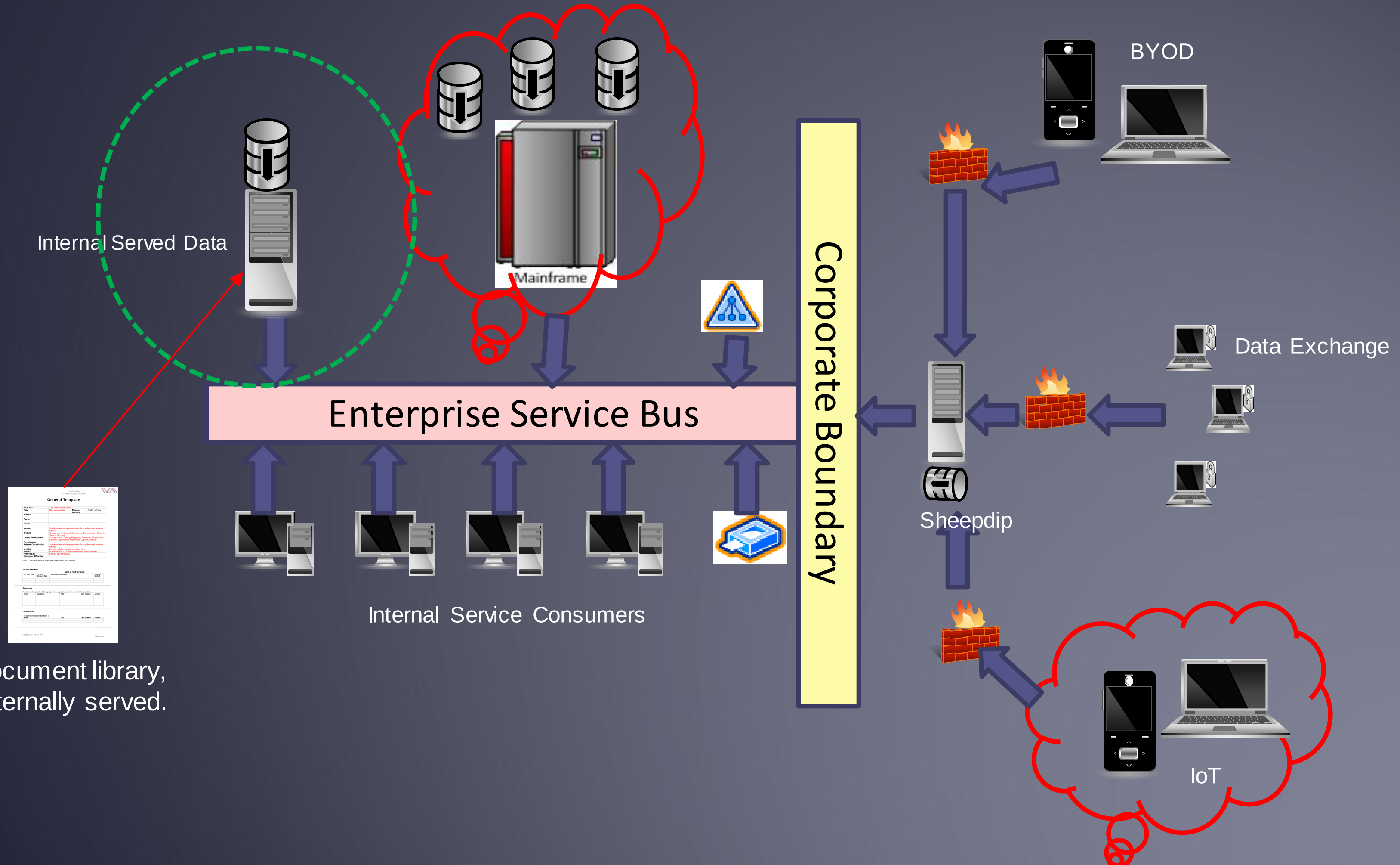
The Organisation Boundary


Internet Service Provider
External Client
Server room
Client 3
Client 1
Client 2
Technical
Staff
Management
The Organisation Technical Boundary
All External Stakeholders
The Organisation Boundary

Nothing should cross your organisation boundary without the knowledge and approval of the organisation or its knowledge of such transfers

14. Document Management – Security

Internal Boundaries



Nothing crosses your organisation boundary in or out, without approval

14. Document Management – Security

Security And The Organisation Boundary

14. Document Management – Security

Security Marking of Documents

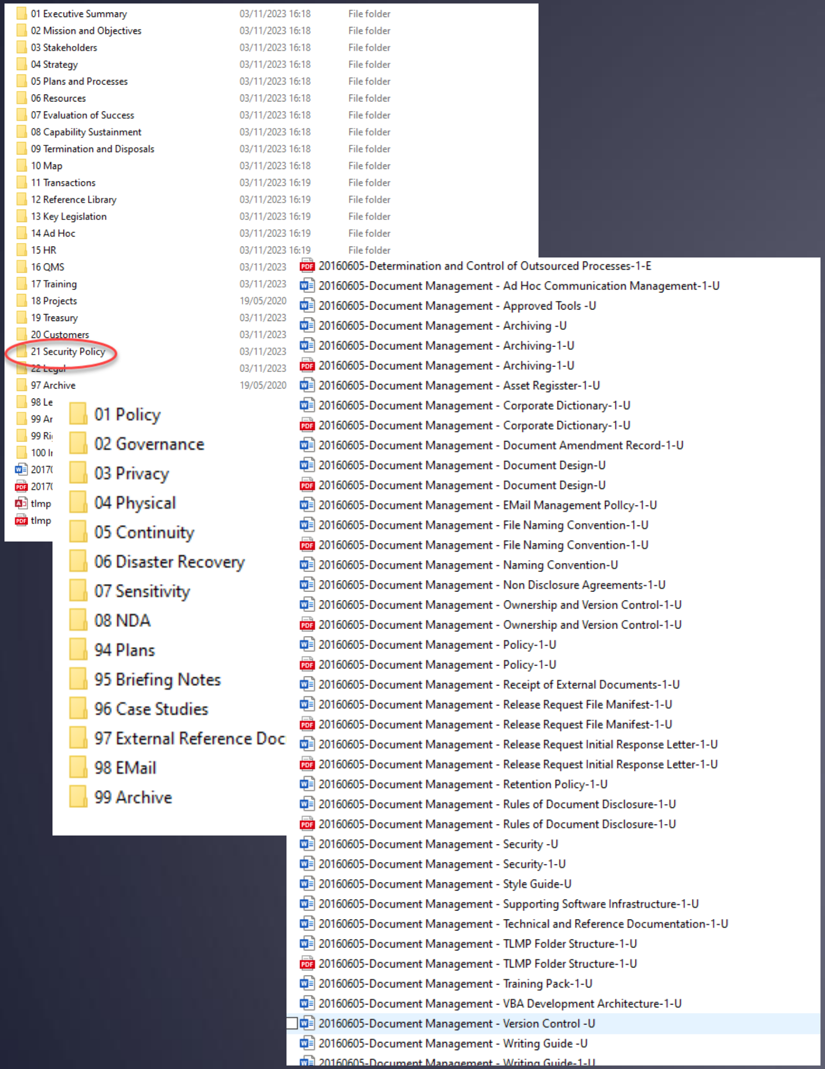
The next three slides outline the nature of a document design that seeks to specify a means to profile a document properly in an operating environment in which legal compliance and security requirements are mutually dependent and supportive.

What is presented here is not THE way to do anything, just “a” way driven by the application of several key best practice methodologies and tools. The result of applying those methods and standards being a library of templates, the catalogue of which can be viewed here

A copy of a base, or general template on which to design others, can be found here.

14. Document Management – Security

Security and Privacy Policy Documentation



01 Executive Summary	03/11/2023 16:18	File folder
02 Mission and Objectives	03/11/2023 16:18	File folder
03 Stakeholders	03/11/2023 16:18	File folder
04 Strategy	03/11/2023 16:18	File folder
05 Plans and Processes	03/11/2023 16:18	File folder
06 Resources	03/11/2023 16:18	File folder
07 Evaluation of Success	03/11/2023 16:18	File folder
08 Capability Sustainment	03/11/2023 16:18	File folder
09 Termination and Disposals	03/11/2023 16:18	File folder
10 Map	03/11/2023 16:18	File folder
11 Transactions	03/11/2023 16:19	File folder
12 Reference Library	03/11/2023 16:19	File folder
13 Key Legislation	03/11/2023 16:19	File folder
14 Ad Hoc	03/11/2023 16:19	File folder
15 HR	03/11/2023 16:19	File folder
16 QMS	03/11/2023	
17 Training	03/11/2023	
18 Projects	19/05/2020	
19 Treasury	03/11/2023	
20 Customers	03/11/2023	
21 Security Policy	03/11/2023	
22 Legal	03/11/2023	
97 Archive	19/05/2020	
98 Le		
99 Ar		
99 Ri		
100 I		
2017		
2017		
tlmp		
tlmp		

01 Policy
02 Governance
03 Privacy
04 Physical
05 Continuity
06 Disaster Recovery
07 Sensitivity
08 NDA
94 Plans
95 Briefing Notes
96 Case Studies
97 External Reference Doc
98 EMail
99 Archive

20160605-Determination and Control of Outsourced Processes-1-E
20160605-Document Management - Ad Hoc Communication Management-1-U
20160605-Document Management - Approved Tools -U
20160605-Document Management - Archiving -U
20160605-Document Management - Archiving-1-U
20160605-Document Management - Archiving-1-U
20160605-Document Management - Asset Regsister-1-U
20160605-Document Management - Corporate Dictionary-1-U
20160605-Document Management - Corporate Dictionary-1-U
20160605-Document Management - Document Amendment Record-1-U
20160605-Document Management - Document Design-U
20160605-Document Management - Document Design-U
20160605-Document Management - EMail Management Pollcy-1-U
20160605-Document Management - File Naming Convention-1-U
20160605-Document Management - File Naming Convention-1-U
20160605-Document Management - Naming Convention-U
20160605-Document Management - Non Disclosure Agreements-1-U
20160605-Document Management - Ownership and Version Control-1-U
20160605-Document Management - Ownership and Version Control-1-U
20160605-Document Management - Policy-1-U
20160605-Document Management - Policy-1-U
20160605-Document Management - Receipt of External Documents-1-U
20160605-Document Management - Release Request File Manifest-1-U
20160605-Document Management - Release Request File Manifest-1-U
20160605-Document Management - Release Request Initial Response Letter-1-U
20160605-Document Management - Release Request Initial Response Letter-1-U
20160605-Document Management - Retention Policy-1-U
20160605-Document Management - Rules of Document Disclosure-1-U
20160605-Document Management - Rules of Document Disclosure-1-U
20160605-Document Management - Security -U
20160605-Document Management - Security-1-U
20160605-Document Management - Style Guide-U
20160605-Document Management - Supporting Software Infrastructure-1-U
20160605-Document Management - Technical and Reference Documentation-1-U
20160605-Document Management - TLMP Folder Structure-1-U
20160605-Document Management - TLMP Folder Structure-1-U
20160605-Document Management - Training Pack-1-U
20160605-Document Management - VBA Development Architecture-1-U
20160605-Document Management - Version Control -U
20160605-Document Management - Writing Guide -U
20160605-Document Management - Writing Guide-1-U

Security policy and governance are stored as reference documents in the central library, in this case posited on the ida of "though life management planning".

The security policy folder structure is illustrated to the left.

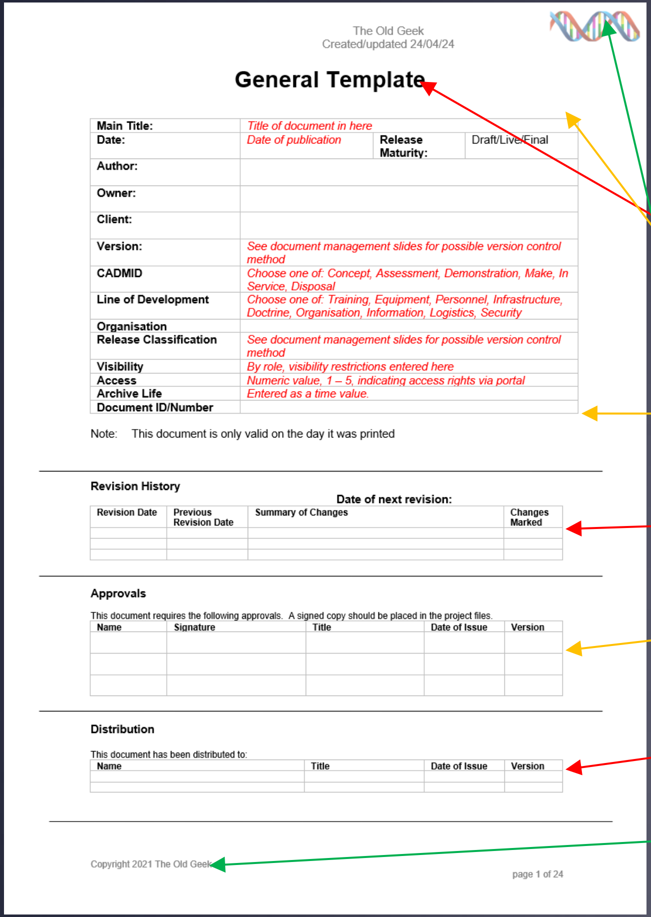
An illustrative he security policy folder document manifest is provided here. Some 97 files of various kinds in all

The Old Geek

14. Document Management – Security

Security Marking of Documents

For the purposes of this exercise, the written content is proceded by the following with the aim of establishing the means to treat a document as a database record and provide the means to add a rich set of sensitivity markings. The part of the template for “profile record keeping” section is presented in this slide.



The Old Geek
Created/updated 24/04/24

General Template

Main Title:	*Title of document in here*		
Date:	*Date of publication*	**Release Maturity:**	Draft/Live/Final
Author:			
Owner:			
Client:			
Version:	*See document management slides for possible version control method*		
CADMID	*Choose one of: Concept, Assessment, Demonstration, Make, In Service, Disposal*		
Line of Development	*Choose one of: Training, Equipment, Personnel, Infrastructure, Doctrine, Organisation, Information, Logistics, Security*		
Organisation			
Release Classification	*See document management slides for possible version control method*		
Visibility	*By role, visibility restrictions entered here*		
Access	*Numeric value, 1 – 5, indicating access rights via portal*		
Archive Life	*Entered as a time value.*		
Document ID/Number			

Note: This document is only valid on the day it was printed

Revision History

Date of next revision:

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked

Approvals

This document requires the following approvals. A signed copy should be placed in the project files.

Name	Signature	Title	Date of Issue	Version

Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version

page 1 of 24

Main Document Title

Document profile containing version, visibility and ownership markings

Document revision history providing an indication of version change and reasons for same

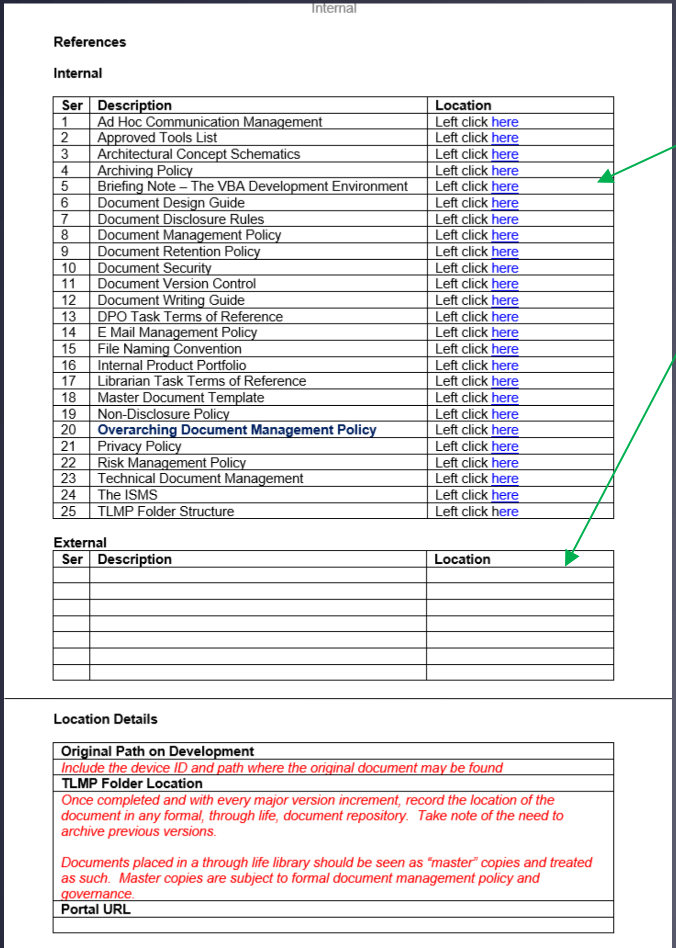
Approvals – Amendment sign off history

Distribution List – By role, who has received a copy of the document

Copyright and logo markings (on each page)

14. Document Management – Security

Security Marking of Documents



Internal

References

Internal

Ser	Description	Location
1	Ad Hoc Communication Management	Left click here
2	Approved Tools List	Left click here
3	Architectural Concept Schematics	Left click here
4	Archiving Policy	Left click here
5	Briefing Note – The VBA Development Environment	Left click here
6	Document Design Guide	Left click here
7	Document Disclosure Rules	Left click here
8	Document Management Policy	Left click here
9	Document Retention Policy	Left click here
10	Document Security	Left click here
11	Document Version Control	Left click here
12	Document Writing Guide	Left click here
13	DPO Task Terms of Reference	Left click here
14	E Mail Management Policy	Left click here
15	File Naming Convention	Left click here
16	Internal Product Portfolio	Left click here
17	Librarian Task Terms of Reference	Left click here
18	Master Document Template	Left click here
19	Non-Disclosure Policy	Left click here
20	**Overarching Document Management Policy**	Left click here
21	Privacy Policy	Left click here
22	Risk Management Policy	Left click here
23	Technical Document Management	Left click here
24	The ISMS	Left click here
25	TLMP Folder Structure	Left click here

External

Ser	Description	Location

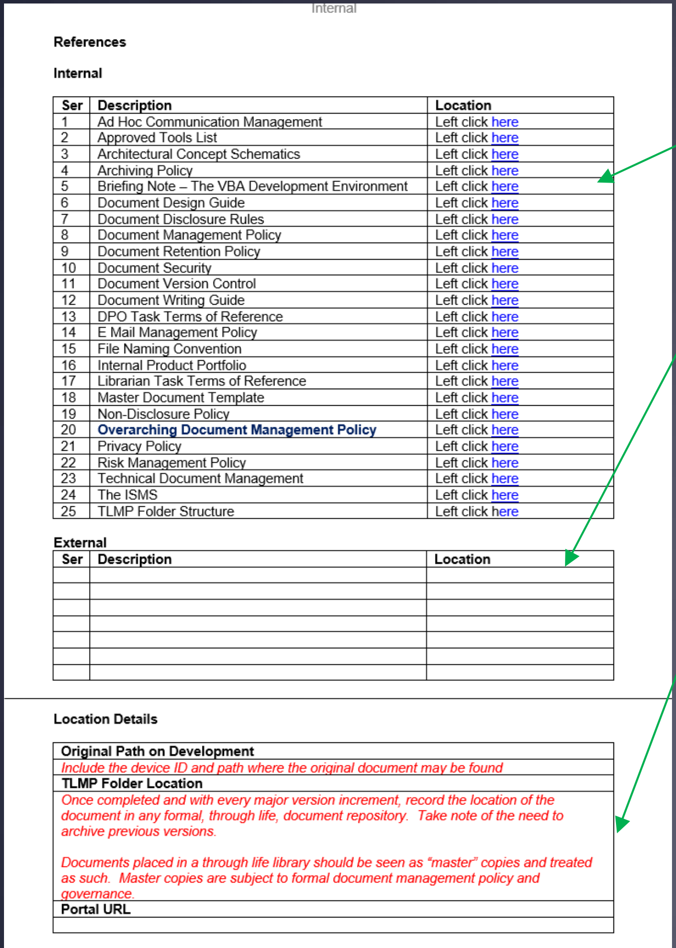
Location Details

Original Path on Development
Include the device ID and path where the original document may be found
TLMP Folder Location
Once completed and with every major version increment, record the location of the document in any formal, through life, document repository. Take note of the need to archive previous versions. *Documents placed in a through life library should be seen as "master" copies and treated as such. Master copies are subject to formal document management policy and governance.*
Portal URL

Page two, internal and external references, linked to those references by hyperlink

14. Document Management – Security

Security Marking of Documents



Internal

References

Internal

Ser	Description	Location
1	Ad Hoc Communication Management	Left click here
2	Approved Tools List	Left click here
3	Architectural Concept Schematics	Left click here
4	Archiving Policy	Left click here
5	Briefing Note – The VBA Development Environment	Left click here
6	Document Design Guide	Left click here
7	Document Disclosure Rules	Left click here
8	Document Management Policy	Left click here
9	Document Retention Policy	Left click here
10	Document Security	Left click here
11	Document Version Control	Left click here
12	Document Writing Guide	Left click here
13	DPO Task Terms of Reference	Left click here
14	E Mail Management Policy	Left click here
15	File Naming Convention	Left click here
16	Internal Product Portfolio	Left click here
17	Librarian Task Terms of Reference	Left click here
18	Master Document Template	Left click here
19	Non-Disclosure Policy	Left click here
20	**Overarching Document Management Policy**	Left click here
21	Privacy Policy	Left click here
22	Risk Management Policy	Left click here
23	Technical Document Management	Left click here
24	The ISMS	Left click here
25	TLMP Folder Structure	Left click here

External

Ser	Description	Location

Location Details

Original Path on Development
Include the device ID and path where the original document may be found
TLMP Folder Location
Once completed and with every major version increment, record the location of the document in any formal, through life, document repository. Take note of the need to archive previous versions. *Documents placed in a through life library should be seen as "master" copies and treated as such. Master copies are subject to formal document management policy and governance.*
Portal URL

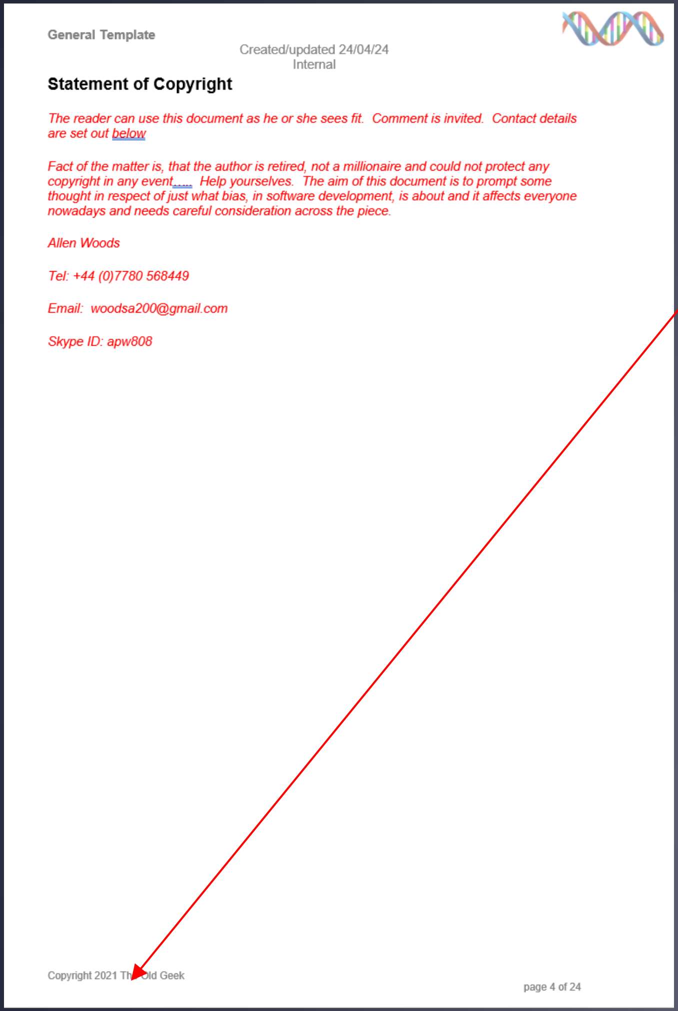
Page two, internal and external references, linked to those references by hyperlink

File Storage Location

The Old Geek

14. Document Management – Security

Security Marking of Documents



General Template

Created/updated 24/04/24
Internal

Statement of Copyright

The reader can use this document as he or she sees fit. Comment is invited. Contact details are set out below

Fact of the matter is, that the author is retired, not a millionaire and could not protect any copyright in any event….. Help yourselves. The aim of this document is to prompt some thought in respect of just what bias, in software development, is about and it affects everyone nowadays and needs careful consideration across the piece.

Allen Woods

Tel: +44 (0)7780 568449

Email: woodsa200@gmail.com

Skype ID: apw808

Copyright 2021 The Old Geek

page 4 of 24

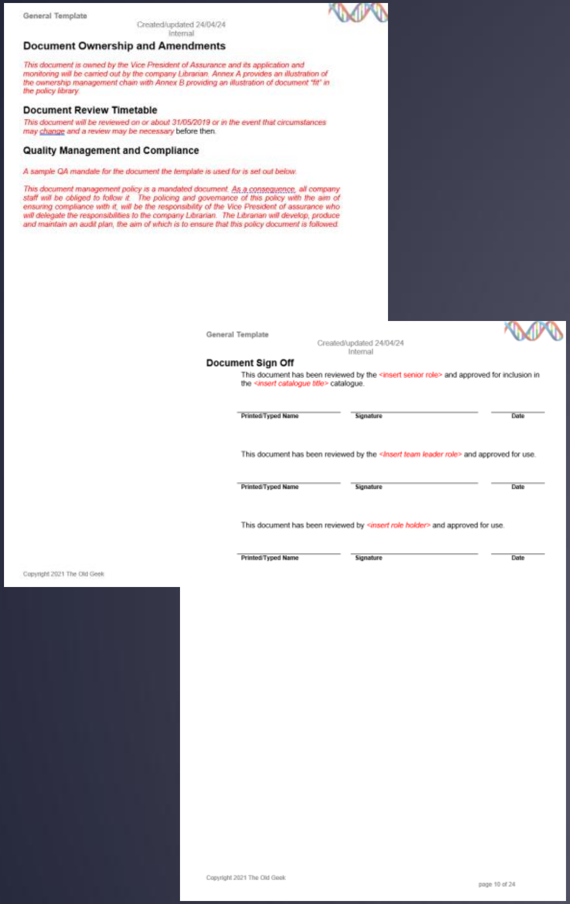
Page 3. An explicit statement of copyright to establish ownership.

With the statement of copyright reinforced by markings on ech page

Note, pages 1, 2, and 3 would not normally be distributed to outside agencies

14. Document Management – Security

Security Marking of Documents



General Template

Created/updated 24/04/24
Internal

Document Ownership and Amendments

This document is owned by the Vice President of Assurance and its application and monitoring will be carried out by the company Librarian. Annex A provides an illustration of the ownership management chain with Annex B providing an illustration of document "fit" in the policy library.

Document Review Timetable

This document will be reviewed on or about 31/05/2019 or in the event that circumstances may change and a review may be necessary before then.

Quality Management and Compliance

A sample QA mandate for the document the template is used for is set out below.

This document management policy is a mandated document. As a consequence, all company staff will be obliged to follow it. The policing and governance of this policy with the aim of ensuring compliance with it, will be the responsibility of the Vice President of assurance who will delegate the responsibilities to the company Librarian. The Librarian will develop, produce and maintain an audit plan, the aim of which is to ensure that this policy document is followed.

General Template

Created/updated 24/04/24
Internal

Document Sign Off

This document has been reviewed by the *<insert senior role>* and approved for inclusion in the *<insert catalogue title>* catalogue.

Printed/Typed Name Signature Date

This document has been reviewed by the *<Insert team leader role>* and approved for use.

Printed/Typed Name Signature Date

This document has been reviewed by *<insert role holder>* and approved for use.

Printed/Typed Name Signature Date

page 10 of 24

The last two pages of each document explicitly stating quality assurance measures taken followed by final sign off

14. Document Management – Security

Security Marking of Documents

The design presented here is not "MUST DO" for everything, it is a judgement call when such rigor needs to be applied.

It needs to be understood that the reasons for going to this length are to establish ownership, protect content and, in the event that an external auditor comes to call, the organisation can demonstrate that there was and is, an assurance regime in place.

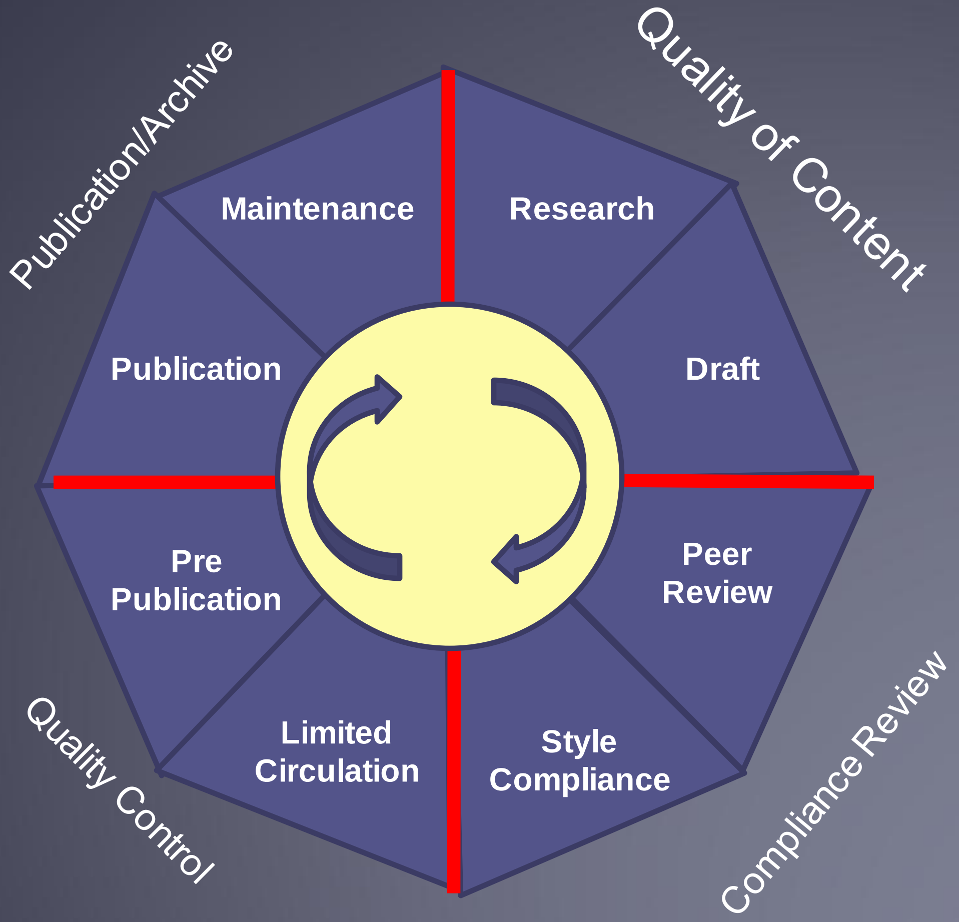
Your call, your risk…

14. Document Management – Security

Security And The Document Life Cycle As Focus

14. Document Management – Security

Document Life Cycle – Security Key Stages



Corporate Asset

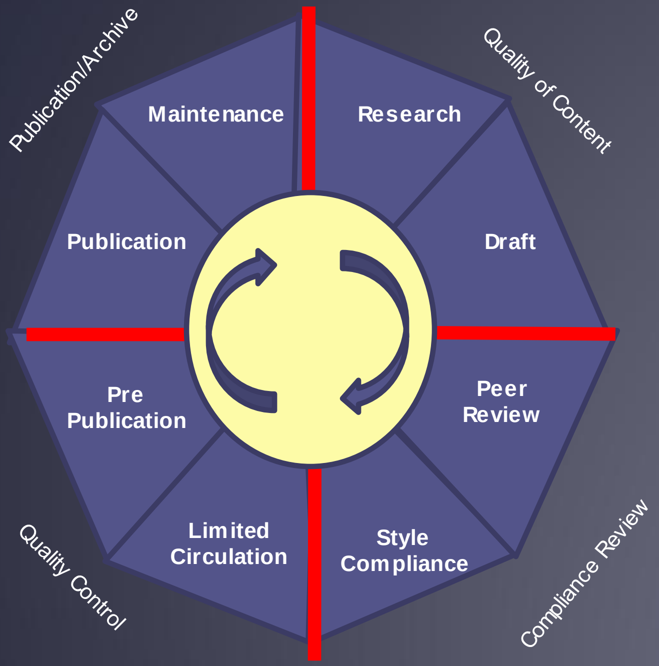
Documents have lives. They are created, they are used, they are disposed of.

The unequivocal establishment of ownership is key.

The Old Geek

14. Document Management – Security

Pre Publication

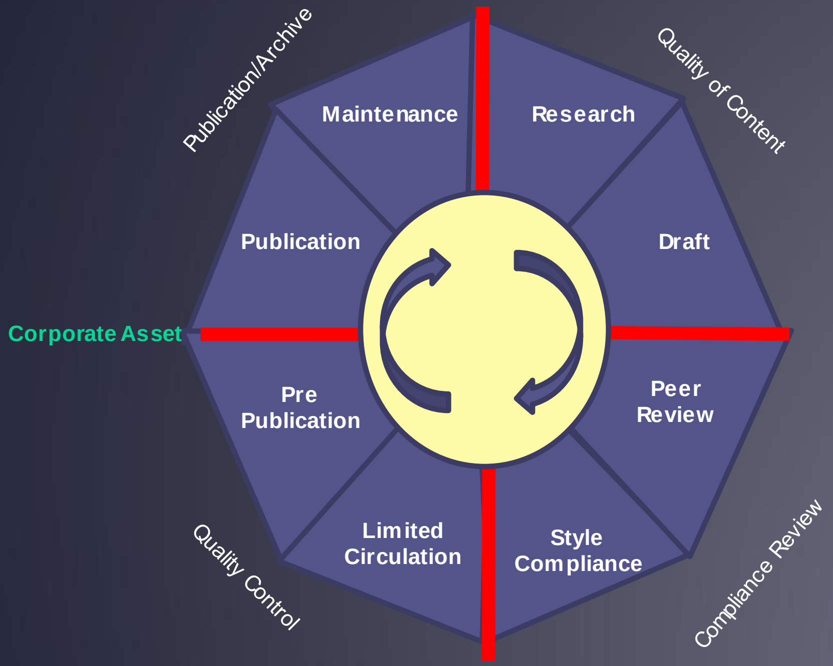


At pre-publication documents should be fully formatted, with the document profile properly completed. Style guide followed and quality of content checked.

All signed off ready for submission into the organisation library

14. Document Management – Security

Establishment of Ownership



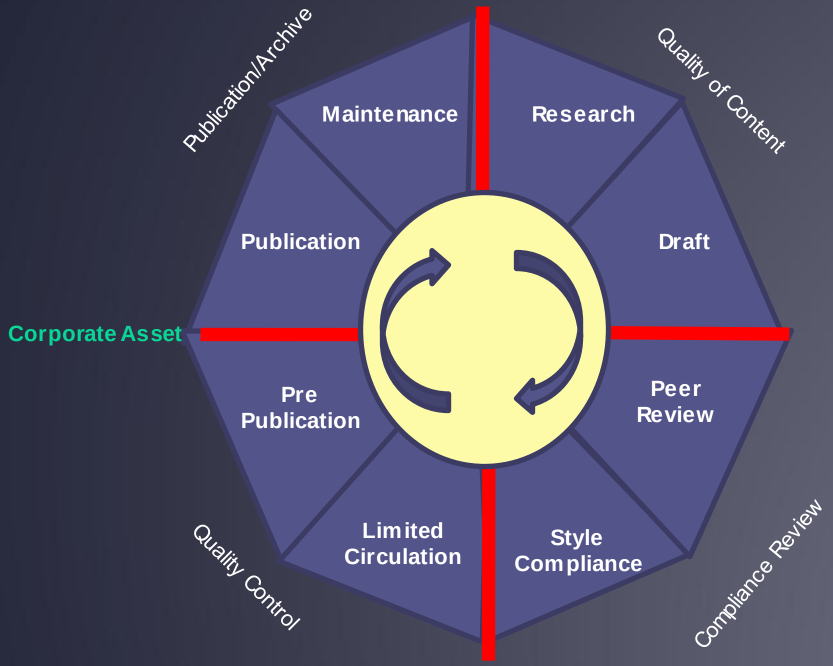
Once accepted into the library, a document becomes a corporate asset. Version increment is applied and the document stored in the correct place in the library.

At this point, for official business purposes, copies for internal and external use should only be drawn from the library.

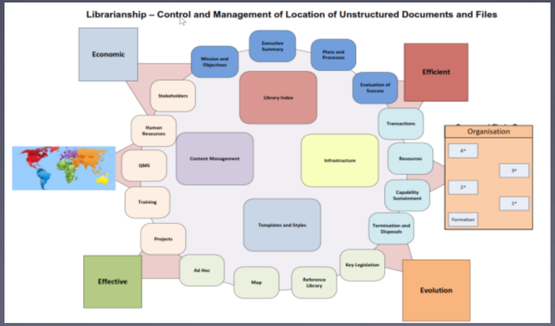
It is an internal decision as to whether or not "work in progress" documents should be retained and for how long.

14. Document Management – Security

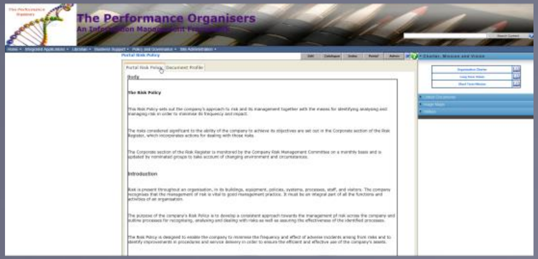
Publication



In publication, document copies for internal and external distribution should only be supplied from the library and drawn though the relevant portal.


Librarianship – Control and Management of Location of Unstructured Documents and Files

At the portal gateway, requests for documents to be logged by job role or stakeholder title (as opposed to the individual). Access and visibility controls applied here



The Risk Policy

This Risk Policy sets out the company's approach to risk and its management together with the means for identifying analysing and managing risk in order to minimise its frequency and impact.

The risks considered significant to the ability of the company to achieve its objectives are set out in the Corporate section of the Risk Register, which incorporates actions for dealing with those risks.

The Corporate section of the Risk Register is monitored by the Company Risk Management Committee on a monthly basis and is updated by nominated groups to take account of changing environment and circumstances.

Introduction

Risk is present throughout an organisation, in its buildings, equipment, policies, systems, processes, staff, and visitors. The company recognises that the management of risk is vital to good management practice. It must be an integral part of all the functions and activities of an organisation.

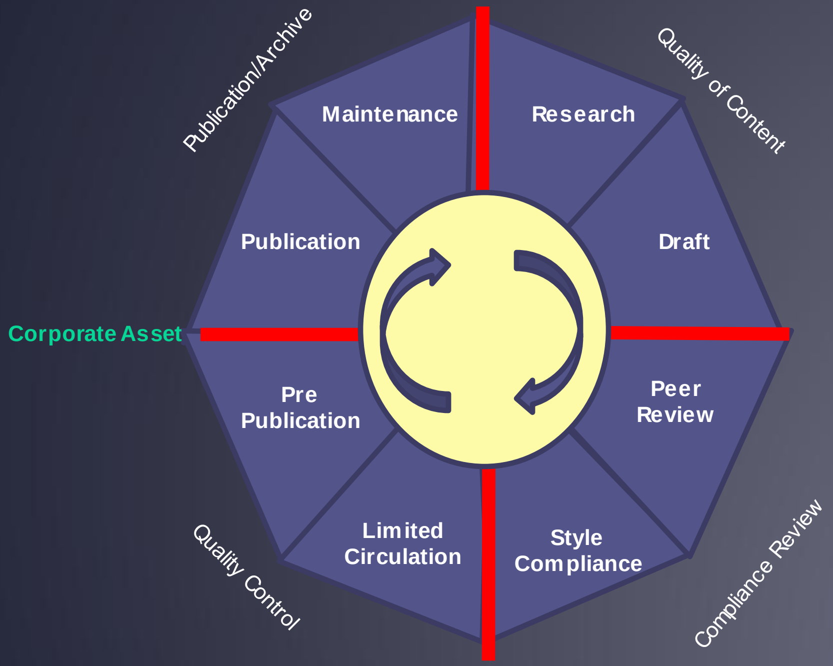
The purpose of the company's Risk Policy is to develop a consistent approach towards the management of risk across the company and outline processes for recognising, analysing and dealing with risks as well as assuring the effectiveness of the identified processes.

The Risk Policy is designed to enable the company to minimise the frequency and effect of adverse incidents arising from risks and to identify improvements in procedures and service delivery in order to ensure the efficient and effective use of the company's assets.

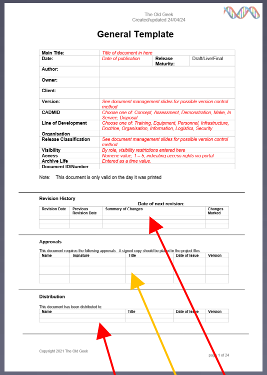
Documents may be presented on subject matter expert intranet or external site pages, but referenced back to the TLMP library. All document download requests to be logged by job role or stakeholder title

14. Document Management – Security

Maintenance



Authorised changes to document content recorded on the indicated listings below



The Old Geek
Created/updated 24/04/24

General Template

Main Title:	*Title of document in here*		
Date:	*Date of publication*	**Release Maturity:**	Draft/Live/Final
Author:			
Owner:			
Client:			
Version:	*See document management slides for possible version control method*		
CADMID	*Choose one of: Concept, Assessment, Demonstration, Make, In Service, Disposal*		
Line of Development	*Choose one of: Training, Equipment, Personnel, Infrastructure, Doctrine, Organisation, Information, Logistics, Security*		
Organisation			
Release Classification	*See document management slides for possible version control method*		
Visibility	*By role, visibility restrictions entered here*		
Access	*Numeric value, 1 – 5, indicating access rights via portal*		
Archive Life	*Entered as a time value.*		
Document ID/Number			

Note: This document is only valid on the day it was printed

Revision History

Date of next revision:

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked

Approvals

This document requires the following approvals. A signed copy should be placed in the project files.

Name	Signature	Title	Date of Issue	Version

Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version

Copyright 2021 The Old Geek

page 1 of 24

Document revision history providing an indication of version change and reasons for same

Approvals – Amendment sign off history

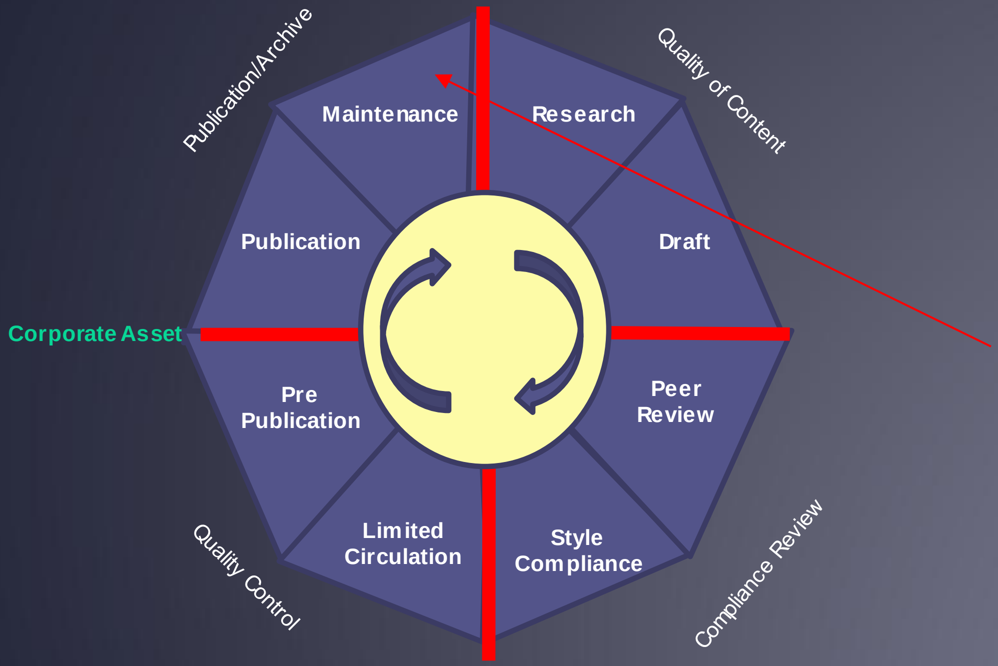
Distribution List – By role, who has received a copy of the document

More than 10 modifications and reviews should trigger a quality assurance review with the aim being to decide if a new version needs to be written.

Triggering a new version will eventually bring about a version increment on release of the new version into the library. On new release, all existing releases to be archived.

14. Document Management – Security

Archive and Disposal



Archiving and disposal is driven, in no small measure, by the need to comply with legislative requirements.

At the time of writing a “hot topic” in information management generally was the EU GDPR and similar legislation elsewhere in the world.

However, the GDPR is not the only regulation that counts and it will be the case that a balance must be struck, based on the concept of “legitimate interest”. With archiving policy and governance being derived from that operating principle.

14. Document Management – Security

The Security Risks (an overview)

14. Document Management – Security

Considerations

What follows is a series of slides that set out, in overview some issues to be consider in respect of document security.

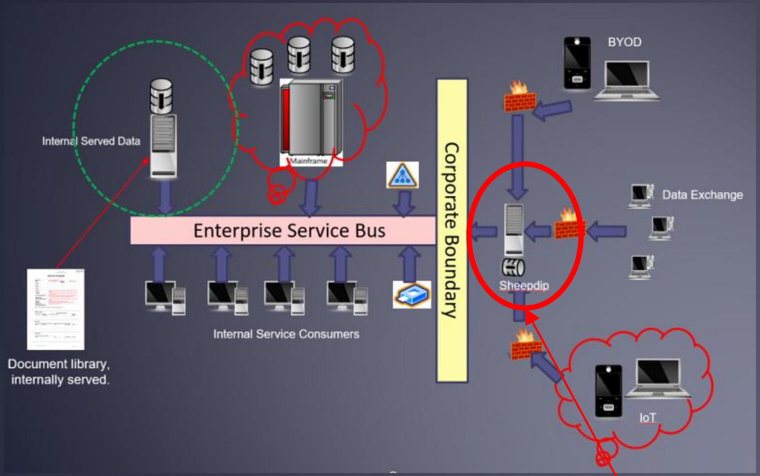
It is not possible to be specific, given the generalist nature of IT use nowadays which suggests that what is presented here will not be complete and nor would recommendations to address issues raised would be appropriate for everyone.

In short, you must plan your own security approach, but within the context of an overall security plan of the kind that the ISO 27000 family of standards would bring about.

Note too, that given incidents like "sunburst" and other "hacks", not to mention the rise of computer related crime generally and its estimated financial hit, just in the UK, failure to address security issues is an existential commercial risk.

14. Document Management – Security

Document Receipt



Documents are packages, an early slide deck in this series illustrates the idea that document files are in fact composite files that contain a number of file based components. It is possible to “unzip” or decompress files to expose the constituent parts

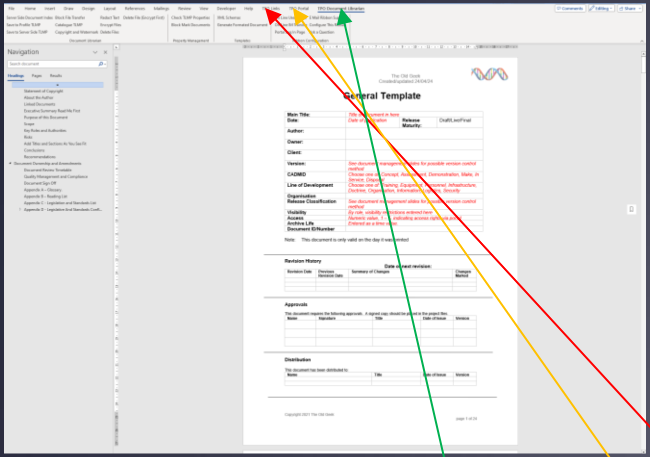
Needless to say it is possible to insert items into the packages which become a constituent part of the file structures if those considering it know how to execute an insertion.

One of the more extreme forms of insertion being the “sunburst” hack a few years ago. For that particular exercise, part of the package was for the malignant element of the incursion, to remain dormant for a few days before its ful effect was deployed.

“Sheep dipping”, holding files coming into an organisation on a sanitised machine for detailed checking of files should be an active consideration

14. Document Management – Security

MS Office Inserts



The Old Geek
Created/updated 24/04/24

General Template

Main Title:	*Title of document in here*		
Date:	*Date of publication*	**Release Maturity:**	Draft/Live/Final
Author:			
Owner:			
Client:			
Version:	*See document management slides for possible version control method*		
CADMID	*Choose one of Concept, Assessment, Demonstration, Make, In Service, Disposal*		
Line of Development	*Choose one of Training, Equipment, Personnel, Infrastructure, Doctrine, Organisation, Information, Logistics, Security*		
Organisation			
Release Classification	*See document management slides for possible version control method*		
Visibility	*By role, visibility restrictions entered here*		
Access	*Numeric value, 1 – [illegible], indicating access rights via portal*		
Archive Life	*Entered as a time value.*		
Document ID/Number			

Note: This document is only valid on the day it was printed

Revision History

Date of next revision:

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked

Approvals

This document requires the following approvals. A signed copy should be placed in the project files.

Name	Signature	Title	Date of Issue	Version

Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version

Copyright 2021 The Old Geek

page 1 of 24

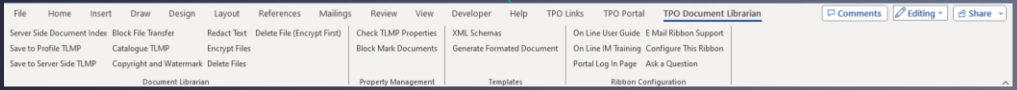
To facilitate controlled document management and access a number of “add ins” were built with the aim of implementing co-ordinated security management from “desk top to server”.

The add-ins were deployed locally. Three core components:

An external hyperlink librarian

A series of controlled portal gateways

Enhanced document management capabilities



Which were themselves supported by other special to task portfolio tools, the aim of which was to enhance document management security capabilities

14. Document Management – Security

Bring Your Own Device (BYOD)

Bring Your Own Device is a common practice nowadays, but..

By definition a BYOD device is not a corporate asset.

BYOD devices can be easily connected into a corporate network by a variety of methods both directly (via USB, say) or indirectly.

There is no control over the nature of the device and as a result, each BYOD device may introduce security integration issues from operating system on up over which there is no corporate control

There is no “ownership” of such devices and as a result, in the event of a compromise of security of any kind, device owners can refuse an audit.

Go figure..

14. Document Management – Security

USB Ports and Devices

Following on from BYOD, a fortress is only as secure as its gateways. A USB port is a gateway. Learn how to disable them as part of a security review.

A video available here explains how to disable USB ports at the operating system level through the Windows registry.

A second method of disabling USB ports is through the device "basic input output services" may be applied.

ANY DEVICE, ANY DEVICE AT ALL, that may be connected via a USB port should be a corporate asset, properly managed as company asset and reviewed on the basis of a network integration plan or process.

Given that USB memory sticks are for sale now that can store 2Tb of data and many organisations do not hold that volume, then placing an entire corporate information architecture on such a device is a significant risk.

14. Document Management – Security

Release – General Policy

Nothing should cross your organisation boundary without the knowledge and approval of the organisation or its knowledge of such transfers

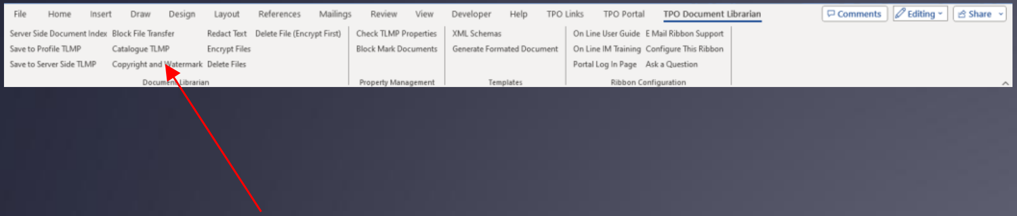
A "Document Disclosure" policy should be developed for the release of sensitive documents

Given the complexity of some kinds of disclosure requests (A GDPR DSA for example), it is also prudent to develop a suitable "initial response letter" and for each such complex request maintain a release file manifest.

A review of external regulation should be executed in order to determine a legally sound definition of "legitimate interest".

14. Document Management – Security

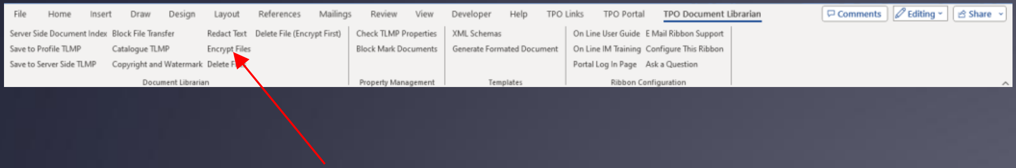
Release - Watermarking



All copies of released sensitive documentation should be watermarked, where possible as a “certified true copy” using whatever term to describe the integrity of the copy that the organisation has supplied.

14. Document Management – Security

Release - Encryption

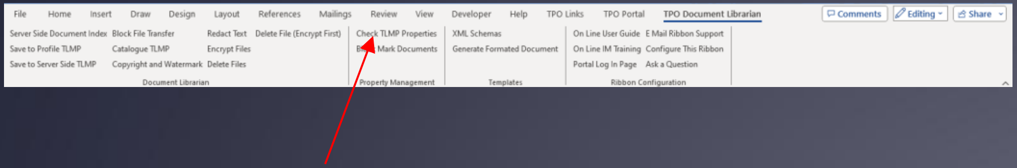


Where agreed and appropriate, sensitive documents despatched to external recipients should be encrypted.

The MS Office add-ins illustrated above supported several encryption methods.

14. Document Management – Security

Release – Password Protection and a Sealed “Wrapper”

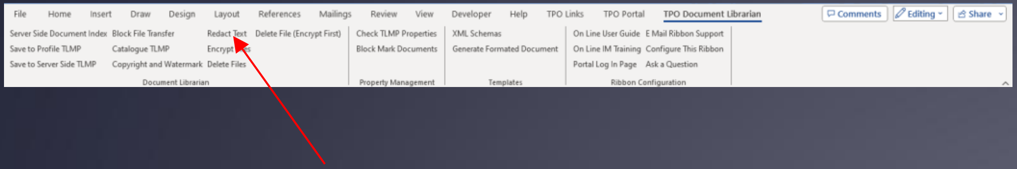


Where agreed and appropriate, sensitive documents despatched to external recipients should be password protected.

Release documents should also be converted and wrapped in a form different to the original document, for example from “WORD” to “PDF”, the aim being to ensure, in the best way possible, the integrity of the content

14. Document Management – Security

Personal Data Protection



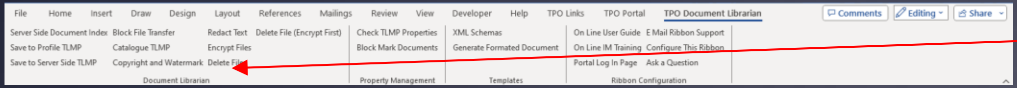
Where document content contains sensitive material, such as the personal details of third parties, the boy of the text should be redacted.

In this case of the add in, redaction was executed by opening the original file, taking a copy and then searching the copy for sensitive text w and replacing it with the word “redacted” followed by a date time group of the redaction exercise.

The redacted copy being sent for despatch in due course

14. Document Management – Security

Deletion



Enhanced File Deletion

It is the case that the form of “deletion” in a windows operating environment is typically a two stage process:

Place a file in a “trash can”

At some point, empty the trash can

However, as described here, when the “trash can” is emptied the storage space a a file occupies is only marked as “free” or “blank” space and until the space is overwritten, document content can still be read (through a “hex” editor), or recovered. So..

The deletion capability indicated in the office add-ins supported the following, optional deletion techniques:

1. Password protect, then encrypt as a whole file then delete.

Or

2. Open a document file encrypt the content, close the file, password protect and then encrypt at fie level.

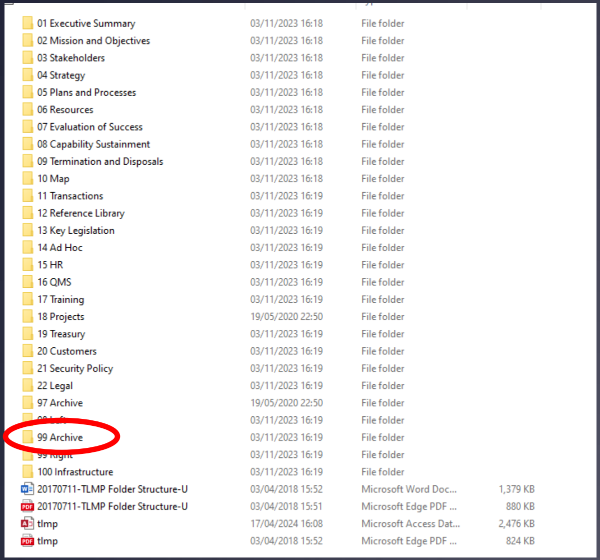
Or..

3. Open a document file at the absolute disk level and encrypt, byte by byte. This last option taking quite some time to execute given document file storage requirements nowadays.

With each file, once dealt with, marked for deletion at operating system level.

14. Document Management – Security

Archiving



01 Executive Summary	03/11/2023 16:18	File folder	
02 Mission and Objectives	03/11/2023 16:18	File folder	
03 Stakeholders	03/11/2023 16:18	File folder	
04 Strategy	03/11/2023 16:18	File folder	
05 Plans and Processes	03/11/2023 16:18	File folder	
06 Resources	03/11/2023 16:18	File folder	
07 Evaluation of Success	03/11/2023 16:18	File folder	
08 Capability Sustainment	03/11/2023 16:18	File folder	
09 Termination and Disposals	03/11/2023 16:18	File folder	
10 Map	03/11/2023 16:18	File folder	
11 Transactions	03/11/2023 16:19	File folder	
12 Reference Library	03/11/2023 16:19	File folder	
13 Key Legislation	03/11/2023 16:19	File folder	
14 Ad Hoc	03/11/2023 16:19	File folder	
15 HR	03/11/2023 16:19	File folder	
16 QMS	03/11/2023 16:19	File folder	
17 Training	03/11/2023 16:19	File folder	
18 Projects	19/05/2020 22:50	File folder	
19 Treasury	03/11/2023 16:19	File folder	
20 Customers	03/11/2023 16:19	File folder	
21 Security Policy	03/11/2023 16:19	File folder	
22 Legal	03/11/2023 16:19	File folder	
97 Archive	19/05/2020 22:50	File folder	
98 Left	03/11/2023 16:19	File folder	
99 Archive	03/11/2023 16:19	File folder	
99 Right	03/11/2023 16:19	File folder	
100 Infrastructure	03/11/2023 16:19	File folder	
20170711-TLMP Folder Structure-U	03/04/2018 15:52	Microsoft Word Doc...	1,379 KB
20170711-TLMP Folder Structure-U	03/04/2018 15:51	Microsoft Edge PDF ...	880 KB
tlmp	17/04/2024 16:08	Microsoft Access Dat...	2,476 KB
tlmp	03/04/2018 15:52	Microsoft Edge PDF ...	824 KB

An archive folder should be located within the corporate document library, or Elsewhere as defined by corporate governance rules.

The archive folder falls under the direct control of the organisation librarian. Documents placed in archive should only be released on request and the request logged when documents are issued

For consistency of location management, the sub folder structure of the archive folder should mirror the overarching library folder structure

Archived documents should be secured by password with the original content “wrapped” in a machine readable format different to the original form.

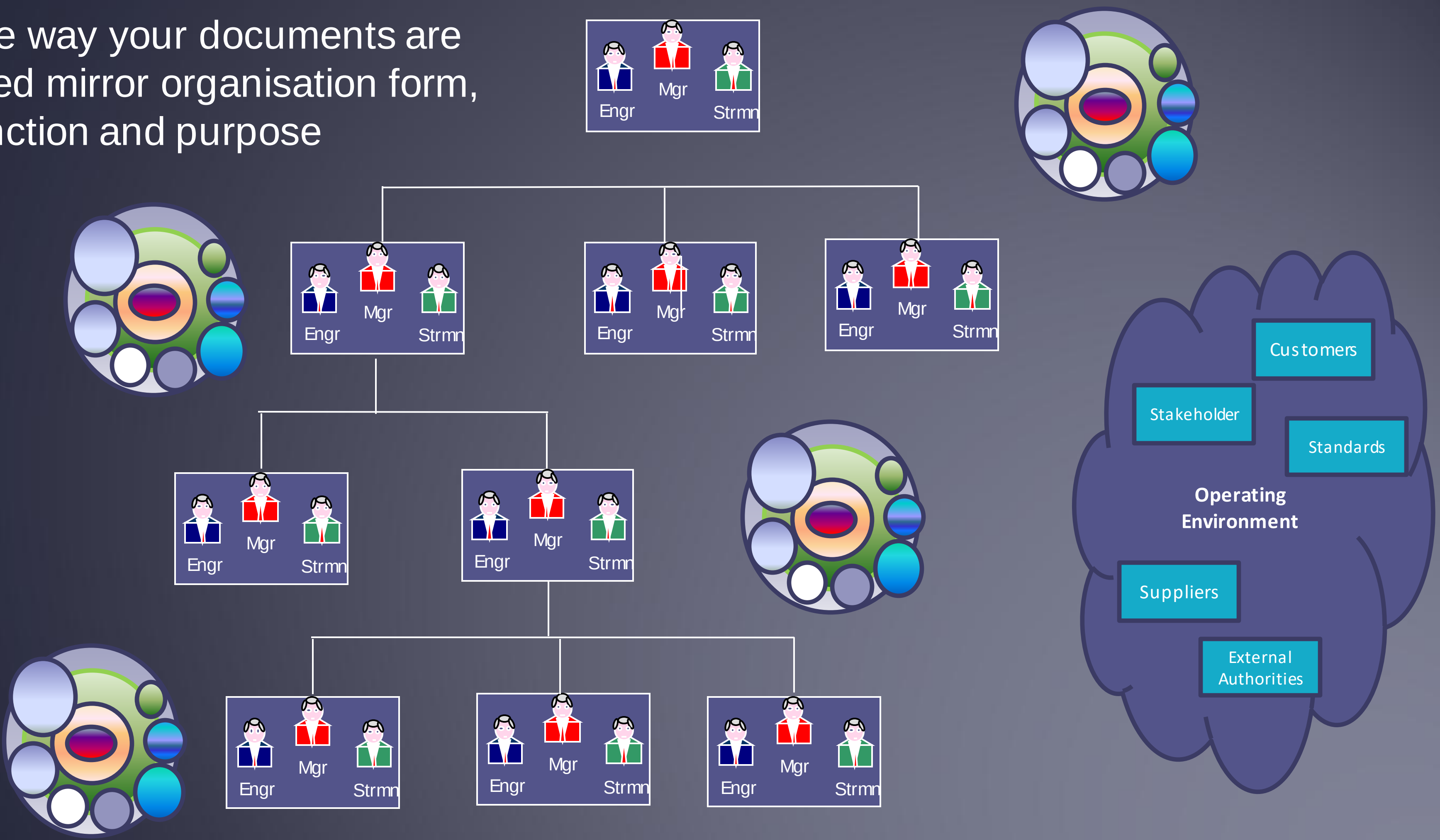
Archived documents should be held for the minimum period required consistent with any regulatory requirements (which could be for quite some time.

An appropriate archiving policy and governance regime will need to be developed. A sample can be read here

14. Document Management – Security

Cleanse Locally On File Deletion and Archive

The way your documents are used mirror organisation form, function and purpose



Customers

Stakeholder

Standards

Operating Environment

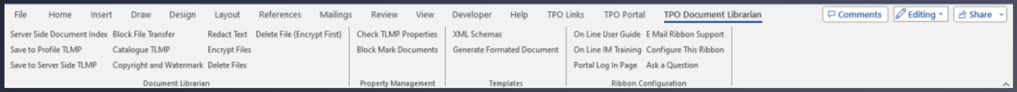
Suppliers

External Authorities

There will be more than one document store

14. Document Management – Security

Cleanse Locally On File Deletion and Archive



There will therefore be a need to regularly cleanse local stores wherever they may be on organisation or system owned assets.

Two corporate events require corporate cleansing of data stores where they exist:

Archiving – with the aim being to delete redundant document files

Deletion from the main library – with the aim of ensuring integrity of content

As a consequence, the MS office add ins and a supporting document spider were deployed to every desk top device on internal networks when the opportunity and need arose

14. Document Management – Security

The Insider Risk

Do not underestimate the scale and scope of the insider risk.

Plan carefully, the end of employment departure of key staff, particularly those with a high level of access to corporate information stores of any kind.

Lock visitor technology in a secure area on entry to your organisation, return it to them on departure

The insider risk is diverse, most recently the ability of some generative AI capabilities, that have the means to write computer code have had the effect of democratising sophisticated hacking techniques

For just one example of the impact of the insider risk, review the UK Supreme Court judgement available here. Noting there will be others…..

14. Document Management – Security

Software Asset Management

Software Asst Management (SAM) is a many splendored phrase, it sounds like it refer to running an asset register for your software inventory, which indeed is what it is about in part. After all organisations and individuals do buy software, install it, register it and then go on to use it.

However, what rarely happens is that those doing the using rarely read the Terms and Conditions (T&C). That failure to read them is a mistake.

T&C are a contract, they impose conditions, set by the owner of the rights to the software, on the end users. The basic aim, to protect vendor/owner intellectual property rights and grant end users limited use rights. Limited by virtue of the fact that as much responsibility and liability as possible associated with safe use is shifted client side. T&C change frequently, often if there are legislative changes being applied.

Note too that T&C are written under the jurisdiction of the vendor and compliance with that law rather than yours.

Finally, as a licensed asset, that you or your organisation may use, bear in mind the IP owner will choose to exercise their right to audit your platform of IT device, as they see fit, to make sure that you and your organisation are not contravening licence conditions.

Microsoft Licence Audit Information can be viewed here. The Oracle equivalent here. Those for Apple here. The others too will have similar SAM licensing terms. Make sure someone in your organisation understand your major vendor SAM rules. It is an expensive mistake not to.

14. Document Management – Security

Finally folks…

The next deck? The key players

14. Document Management – Security

That’s all folks…..

The original deck and others, are available on request, free, using any of these means to get in touch:

Tel: +44 07780 568449

Email: woodsa200@gmail.com

Skype: apw808

Authors Linked In Profile here