KNOWLEDGE MANAGEMENT

Presented by: Chris Hodder | 11/06/2020

cih Solutions
SERVICE MANAGEMENT INTEGRATORS

HALOITSM

COMPANY OVERVIEW

Founded in 2007 specifically to address the gap between ITSM vendors and clients understanding of requirements, process improvement, ‘the art of the possible’ with automation, and to leverage benefit for clients outside the specific vendors tool.

HALOITSM OVERVIEW

HaloITSM helps 100,000+ people, from 40+ countries a year transform legacy ways of working into modern intuitive workflows. With a goal to empower teams to deliver consistent first-rate service to internal users, HaloITSM leaves behind disjointed apps and tools to move under one centralised, powerful ITSM solution.

OUR CLIENTS

Both CIH Solutions Ltd. and HaloITSM have clients across all sectors providing a wide range of approaches to specific ITSM challenges, including:

- ✓ Managed Service Providers
- ✓ Local Government
- ✓ National Health Service
- ✓ Finance
- ✓ Construction
- ✓ Legal
- ✓ Automotive
- ✓ Retail
- ✓ Technology

CIH Solutions CLIENTS CON'T

HALOITSM CLIENTS CON'T

KNOWLEDGE MANAGEMENT FRAMEWORK

cih Solutions
SERVICE MANAGEMENT INTEGRATORS

HALOITSM

INTRODUCTION

In IT the term Knowledge Management means different things to different people. KM is often interchangeable with other terms such as: intellectual capital, information management, data management and document management. In reality, KM embraces all of these.

So, what is our definition of KM in relation to an ITSM organisation?

First, not about scale. A KM system can operate just as effectively in a small organisation as a large enterprise.

Second, the key feature of a KM within ITSM is the understanding that different information has different values depending on circumstances.

Assigning *value* to information is vital and has priority over the capture of all available material.

EXAMPLE ONE

European pharmaceutical company.

Scale - repository contained research papers, trial results and project documents covering decades of research amounting to many millions of pages and database entries.

Structure - The success was derived from the strength of the underlying thesaurus enabling users to discover (or perhaps re-discover) knowledge.

EXAMPLE TWO

SAP Managed Service Provider

Small Team – With no top down sponsorship or funding the technical teams had created their own KM central repository.

Structure - All content was created, published and maintained under very strict guidelines by a few key members of staff.

End User Focus – All content was designed with the end user in mind to be accessed by many.

PRINCIPLES

The principles of KM are simple:

Identification

Collation

Storage

Retrieval

Note:

This is not just about documents and data. When the experience of personnel is added into the mix we get Knowledge and this needs to be captured and stored for future use.

KM MODEL FOR ITSM

A typical organisation creates ‘knowledge’ through:

- Individuals, both staff and sub-contractors; would create multiple documents.
- Store them in isolated repositories or held on local drives,
- Resulting in poor retrieval and inaccurate information.

The solution is a simple one:

- A concept of assigning value to information to be introduced.
- Control introduced by a strong KM framework with a central repository to address a specific local need based on this value.

DEFINING BUSINESS VALUE

Assigning value to information is vital.

Categorise *High Business Value* information: The category of business information that covers all the vital and irreplaceable business records, documents, information and data.

The ITSM organisation is critical to this and should lead by example as material that has been compromised by loss, breach of security, inaccuracy or the inability to locate and retrieve will initiate ITSM activities.

It is the failure to identify, capture, publish and retrieve this category of knowledge that can have a significant impact on the management of risk and cost control.

Whilst all information is valuable, depending on circumstances, some information suddenly becomes more valuable.

KNOWLEDGE MANAGEMENT FRAMEWORK

Our first step is to build a KM Framework.

This framework must define the KM life cycle to:

- Create
- Capture
- Review
- Release
- Amend
- Publish
- Retire

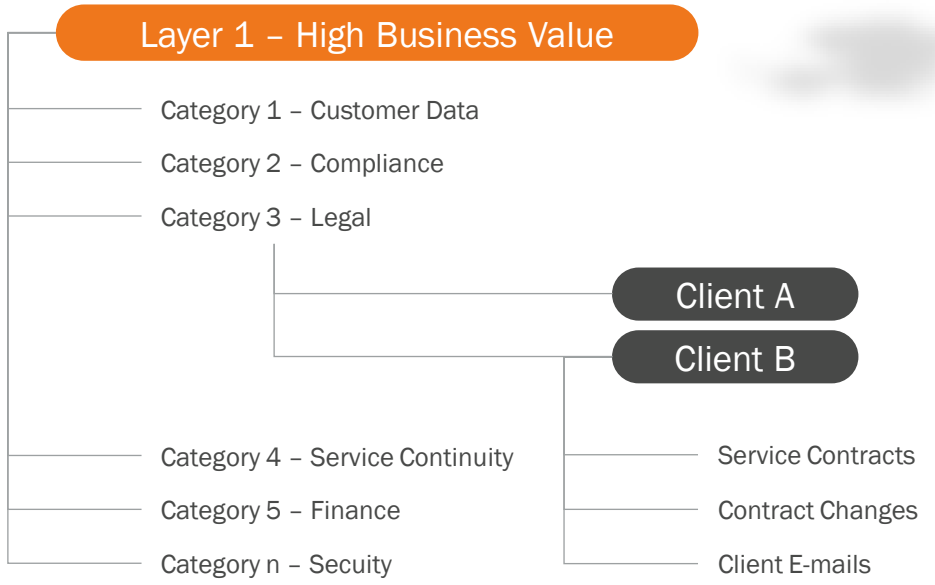
In addition, the KM Framework must define a system of classification for the ITSM information.

High value information Layer 1 information.

All the remainder of the ITSM information and data is collected into Layer 2.

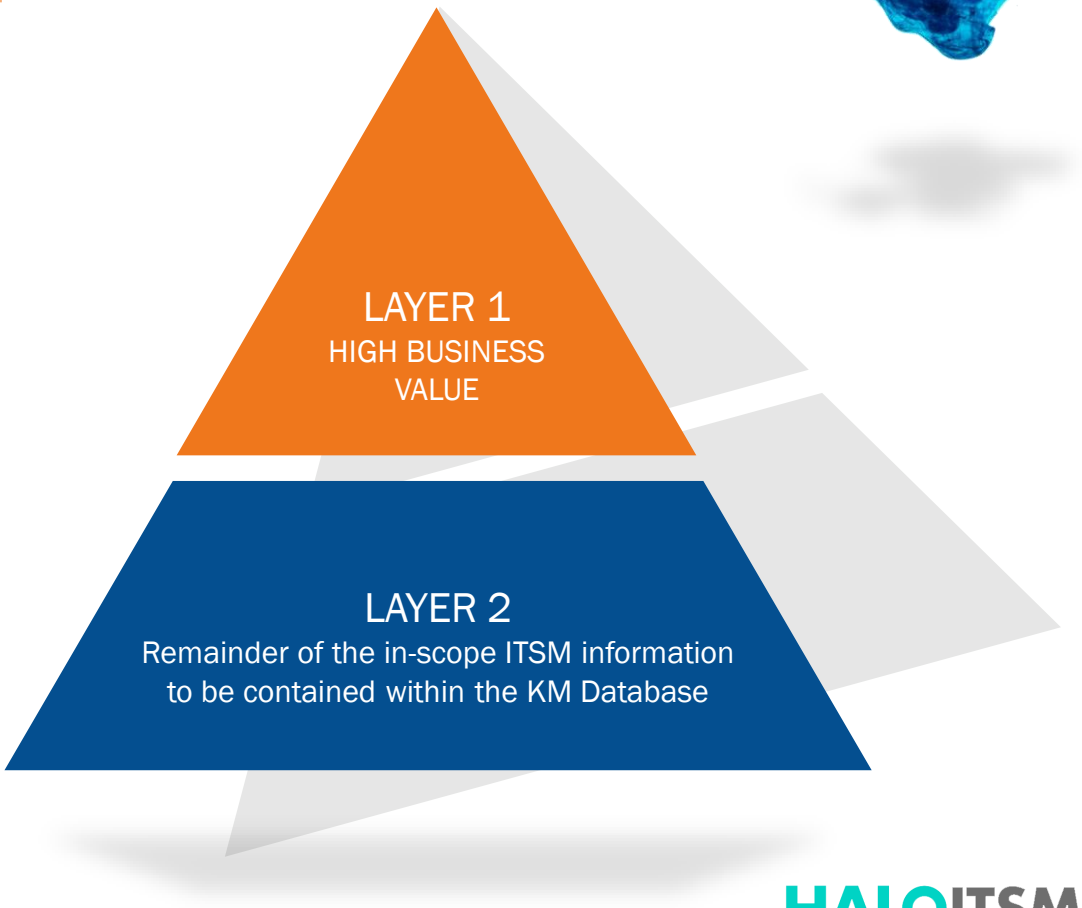
LAYER 1: HIERARCHY

- Start with a simple structure of KM system for Layer 1, based on a hierarchy of Categories and Sub-categories using a controlled vocabulary to tag documents and data sets.
- Once Layer 1 has been identified all the information and data can be divided into Categories. These categories will be assembled under various functional headings.
- Once all the Categories have been identified then the material should be further divided into Sub- categories. Three drill-downs are sufficient to hold all the information in Layer 1.



LAYER 2: CLASSIFICATION

- We recommend a Hierarchical structure for Layer 1 and a Linear approach to Layer 2 classification.
- Layer 2 - we suggest a thesaurus with a more linear structure that will allow more of a free form of search and retrieval
- Not everything needs to be tagged in Layer 2, broader searches and cross searches can be adopted to allow a more ‘search and discovery’ approach.
- The population of Layer 2 will cover all manner of archived project material, design documentation, presentations, non-critical business records etc.

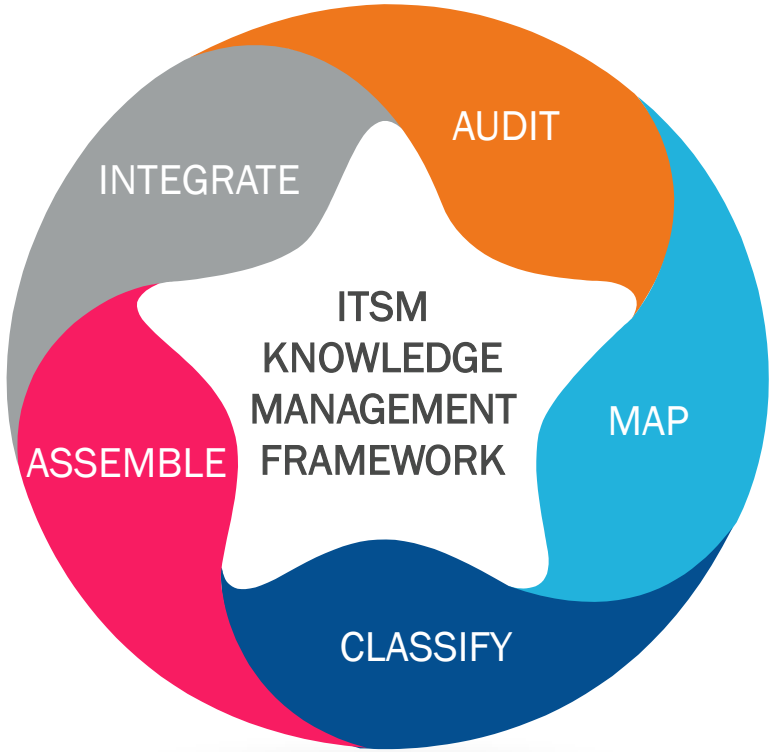


FIVE STAGES OF THE KM FRAMEWORK

There are five stages within the KM Framework.

By following this five-stage sequence all the information considered as *High Business Value* can be identified and either uploaded into the KM Database or retained in local repositories (known as source databases). This is the Integrate stage that is covered in detail later.

Each stage should be followed for Layer 1 and then repeated for Layer 2.



FIVE STAGES OF THE KM FRAMEWORK

ONE

Audit –categories within **Layer 1** have been identified. All the material to be included in each category needs to be identified. This will cover different media formats such as PDF, database tables, e-mails, webinars and HTML etc.

TWO

Map – the location of the material is identified. This is mapped and will be needed when the KM database is designed and built to identify what material should be transferred to the KMDB and what material should remain in local repositories.

FIVE STAGES OF THE KM FRAMEWORK

THREE

Classify – once all the information has been identified for the categories of **Layer 1**, the documents and data can be classified according to the controlled vocabulary system and the hierarchy structure.

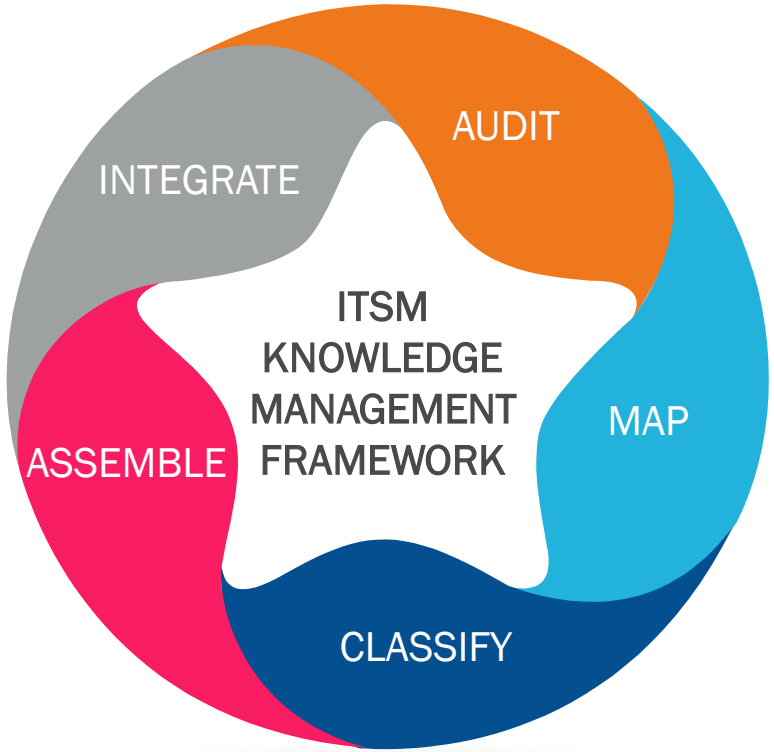
FOUR

Assemble – once classified and physically located, the content for each category should be assembled as a schedule of descriptive metadata tables complete with information titles, document numbers, versions, data sets and physical location.

FIVE STAGES OF THE KM FRAMEWORK

FIVE

Integrate – once all the information has been assembled the metadata tables can be used to manage the population of the KMDB – either directly with content or connected to other repositories to extract the content. These are known as source databases.



EXAMPLE HOT SPOTS

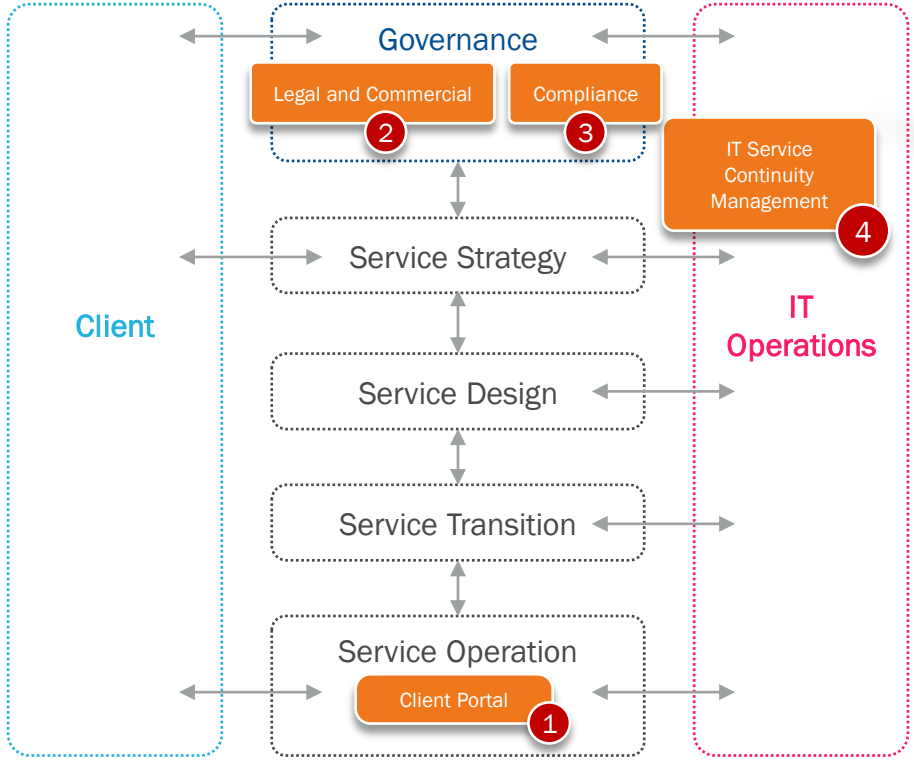
Two examples

The figure is based on a simplified ITSM organisation that could be either a MSP dedicated to external clients, or an ITSM organisation providing IT services to an internal client. The IT Operations can be either internal or external hosting with or without applications support. For the purpose of this paper it is assumed that the IT Operations is in-house and provides hosting, communications and applications support - within an overall governance framework.

EXAMPLE HOT SPOTS

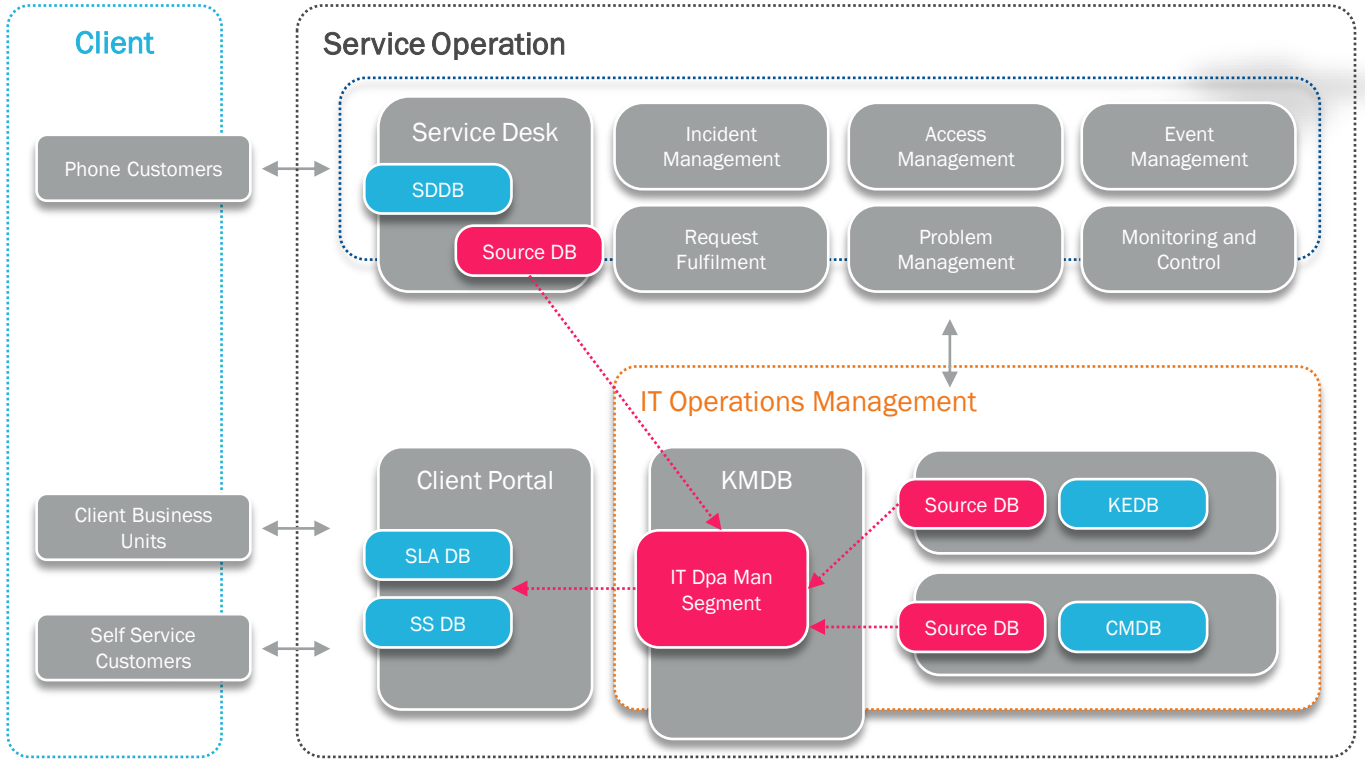
There are four example ‘hot ‘spots’ shown in Figure 4.

- **Client Portal** – Risk to reputation due to poor quality of customer information **Legal and Commercial** – Cost of litigation due to incomplete contract audit trail. **Compliance** – Cost of compliance due to audit failure and forced re-work **Service Continuity** – Risk to IT service continuity due to inadequate preparation.
- All of the above examples relate to the absence, inaccuracy or timely retrieval of information.



HOTSPOT ONE: CLIENT PORTAL

- Service Management team responsible for managing the information available to customers via a Client Portal.
- Some material will be supplied by other teams e.g. Marketing such as prospectus and a product offerings.
- Most material will be service and technical support information covering topics as service availability status, technical self-help and how-to-do-it video clips application forms. The client portal also has a secure area for the client customer groups to access data on performance against SLAs.



cih Solutions
SERVICE MANAGEMENT INTEGRATORS

HALOITSM

HOTSPOT ONE: CLIENT PORTAL

The ‘Risk’ we are trying to mitigate here is out-of-date, missing and inaccurate information being posted to the client portal.

Information is identified and collected and then manually or semi-automatically uploaded onto the Client Portal database using scripts. The risk here is that:

- Not all information is collected at the right time (like monthly SLA data updates).
- Incorrect information is selected for the right location.
- Correct information is uploaded to the wrong location.
- Not all information is collected.

HOTSPOT ONE: CLIENT PORTAL

All the client information that was previously managed manually has now been compiled into metadata tables from the Audit – Map – Classify – Assemble stages.

We can now move to the Integrate stage. The metadata tables will hold the locations of all the information and data needed to be accessed by the client portal and the KMDB will use distributed queries to collect all the information and data from these locations.

For example,

The Known Error database (KEDB) could supply diagnostic help and work-arounds for self-service customers for the most common errors.

The KEDB will also collect Event and Incident Management data in support of the SLA reporting that is provided to the client business units via the portal.

The Configuration Management database (CMDB) will also be another source database for the supply of data to the client on service configuration.

HOTSPOT TWO:
COST OF COMPLIANCE

Here is an example of the importance of a KM sub-set of material that can be assembled on the basis of a specific demand.

During a compliance audit, ISO27001 for example, there will be a specific document sets that will need to be made available to the auditors for the certification process.

Without a rigorous KM approach there is the risk of auditors finding a shortfall in the control objectives and controls.

This will result in low auditor marking and possible non-compliance.

There is now a real cost involved with the remedial work needed for a re-run of the audit.

HOTSPOT TWO: COST OF COMPLIANCE

The material can range from Information Security Policies to Physical and Environmental Security.

There is a wide range of different types of information and data and the Audit and Map stages of the KM Framework will require a lot of research and agreement from the KM Stakeholders on what should be included in this KMDB Compliance segment.

One particular example is software asset management (ISO 27001 - Clause A8: Asset Management).

Auditors will check the number and validity of software contracts held and check that the licences cover all the users who actually use the software.

This could be addressed by setting up a source DB within a SAM tool and extracting all the data needed for the audit (as a controlled set) and then sending it to the KMDB.

HOTSPOT THREE: COST OF LITIGATION

This is an example of how the KMDB can be used to store high business value information. Our proposed Layer 1 Hierarchy KMDB can contain a Legal DB segment.

This will be used to store all contractual SLA information relating to an individual client/service. As with Hotspot One, the metadata tables will hold the locations of all the data

Again, distributed queries are used to collect all the information and data from these source DB locations.

The information will include all versions of contracts, contract amendments, SLAs including email trails between the client and the ITSM Operation.

This latter point of email capture is increasingly used to highlight any communication that might indicate an implied contract variation by either party. We would suggest the inclusion of a Message Record Management (MRM) system as part of the KM solution.

HOTSPOT FOUR:
RISK TO SERVICE CONTINUITY

In this final scenario we want to look at how the KMDB can be used to support Service Continuity.

With a much broader scope than just KM we're not intending to cover the whole subject of Business Continuity Management (BCM). Again, there are multiple terms involved here – like Disaster Recovery, Business Recovery and Service Recovery.

In the case of ITSM and KM, we focus on describing how KM can be used in support of Service Recovery within the broader BCM that covers the end-to-end business.

The dilemma facing an ITSM organisation is no one can really identify all the situations likely to occur and therefore will be unable to have Knowledge covering all potential outcomes.

Certainly, the evacuation of a data centre due to fire and flood is an obvious scenario. Clearly you can't prepare for every instance, but it is possible to target some common 'knowns'.

HOTSPOT FOUR:
RISK TO SERVICE CONTINUITY

So, as a possible starting point. In our Layer 1 (High Business Value) under the Service Continuity category, the sub-categories should be constructed to reflect various 'threat scenarios' – one per sub-category for example:

- Cyber threat
- Data theft
- Denial of service
- Major software outages.

Each 'threat scenario' can then be structured along the scope and guidelines of ISO223014.

This will create a consistent framework for compiling all the recovery procedures, communication escalations and fall back plans for each scenario.

KEY TAKEWAYS

- The KM system described here should be considered an ‘entry level’ system, but with the capability of extension as time and budget permit.
- This KM system is also predicated on content being held within existing repositories, as well as a central KMDB, but extracted on demand.
- The KM system can operate on a variety of scales; it is introducing information with value in the right circumstances which is key.

Emphasis must always be on developing a KM Framework as the starting point.

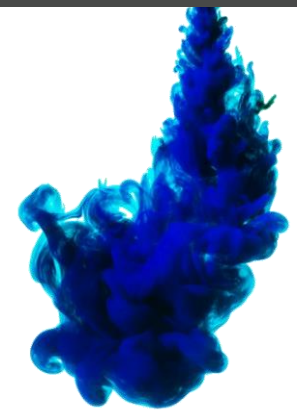
The success of implementing a KM system will always reside with the management and staff of an ITSM organisation and not the technology.

THANK YOU

Founder of CIHS in 2007 Chris has 23 years experience exclusively in the ITSM sector, working with clients across the global on Process engineering best practice, Knowledge Management, CMDB design and toolset implementation.

Chris Hodder
CEO

THANK YOU



Halo Service Solutions has gone from strength to strength since it's inception in 1994; opening offices in the USA and Australia, expanding its global reach to over 100,000+ users and bringing award winning software to over 40 countries.

Paul Hamilton
Managing Director

cih Solutions
SERVICE MANAGEMENT INTEGRATORS

HALOITSM