3.0 Manage ITSM Data, Information and Knowledge		
Number	**Process Activity**	**Description**
3.3	Establish/Refine Authority, Control & Responsibility Required for Management	The Enterprise ITSM KM Process Manager will establish protocol for the authority, controls and responsibility required to properly manage the data, information and ITSM knowledge governed by the ITSM KM process. This includes ownership responsibilities for ITSM Knowledge Artifacts and procedural controls for ensuring timely maintenance.
3.4	Define/Refine Rights Regarding Retention, Transmission and Access	The Enterprise ITSM KM Process Manager will define rights and policies regarding the retention, transmission and access of ITSM data, information and knowledge managed by the ITSM KM Process to ensure compliance with USMC policies and legal requirements. These rights will include any rules for supporting security and sensitivity obligations.
3.5	Identify/Review Requirements for Organization and Technology Environment	The Enterprise ITSM KM Process Manager and the Enterprise ITSM KM Solution Architect will identify and review any changing organizational and technology requirements for how the ITSM data, information and knowledge requirements need to be managed. These requirements could include additional tools or automation to streamline manual procedures or refinement of current architecture based on any previously agreed upon procedures, controls and rights definitions.
3.6	Validate Maintenance Management Plan	After the different requirements, procedures and policies are completed for managing ITSM data, information and knowledge artifacts, the collective set of materials are assembled and validated by the Enterprise ITSM KM Process Manager for completeness. These maintenance plan materials are readied for review and sign-off by the Enterprise ITSM KM Process Owner.
3.7	Input User Evaluations Regarding Process and Procedures	The Enterprise ITSM KM Process Manager will facilitate soliciting formal periodic feedback from users via satisfaction surveys and other means to provide input to the Enterprise ITSM KM Process Manager for efficiency and effectiveness of how the ITSM KM process and artifacts are being managed. This input is factored into the validation of the maintenance plan for improvement opportunities and additional requirements.
3.8	Approve Maintenance Management Plan?	The Enterprise ITSM KM Process Owner reviews the maintenance plan for approval and evaluates the documented procedures and materials for completeness and how the ITSM KM process will be managed for ongoing operational control. If the maintenance management plan is not approved, the Enterprise ITSM KM Process Owner notes the rationale for not approving along with the notes needed to address open issues or updates. This is then passed back to the Enterprise ITSM KM Process Manager to refine the procedures accordingly. Yes: Go to 3.9 Create/Refine Technology Architecture (for architecture) No: Go to "Initial Start or Periodic Review" (for rework)
3.9	Create/Refine Technology Architecture	The Enterprise ITSM KM Solution Architect creates or refines any changes required to the technology architecture for supporting the operational procedures to manage the process and will provide any feedback to the Enterprise ITSM KM Process Manager of any new changes or feedback.

3.0 Manage ITSM Data, Information and Knowledge		
Number	**Process Activity**	**Description**
3.10	Implement and Publish Mechanisms to Capture, Store & Retrieve Information	After the approval is received from the Enterprise ITSM KM Process Owner, the Enterprise ITSM KM Process Manager publishes the procedures within the maintenance plan and implements the mechanisms to operationally support the capture and retrieval of ITSM data, information and knowledge stored.
3.11	Archive/Manage Information Storage and Movement	The Enterprise ITSM KM Process Manager will ensure that the appropriate information movement between storage, archiving and purging are executed and follow the defined procedures and protocol.
3.13	Perform Governance/Reporting/Operational Procedures for CSI	The Enterprise ITSM KM Process Owner will perform required governance, review reports and operational activities required to enable ongoing continual service improvement. This ensures ongoing evaluation and improvement is occurring as part of the broader management of the ITSM data, information and knowledge. The evaluation should include regular review of report relevancy, measurements of ITSM KM usage and identification of any obsolete components.
3.14	ITSM Knowledge Management Updates Needed?	As an ongoing activity, the Enterprise ITSM KM Process Owner will periodically review the reports to identify continuous improvement opportunities. Yes: Go to "Initial Start or Periodic Review (for updates). No: Go to 4.0 Use SKMS (for implementation of solution).

4.4 Use ITSM Service Knowledge Management System

The purpose of the ITSM Use Service Knowledge Management System sub-process is to provide the capabilities required by stakeholders and users to store, manage, update and present ITSM data, information and knowledge. In this sub-process, a holistic solution for the SKMS is designed and implemented based upon the functional requirements needed to deliver the desired capabilities. Beyond tools, the holistic solution also includes the policies, processes and standards leveraged in the design, implementation and use of the SKMS. This includes ongoing enhancements and extensions to the capabilities and knowledge offered within the SKMS. As Knowledge Stakeholders/Users use the SKMS, the solution is monitored and feedback is requested to obtain an understanding of usage patterns as well as the degree to which the SKMS is delivering the required capabilities. Based on this feedback, subsequent updates may be made to the overarching ITSM KM Strategy defined in sub-process 1.0 Create/Update ITSM KM Strategy and to the SKMS solution itself.

Why ITSM Service Knowledge Management System (4.0)?

Provides controlled access to ITSM data, information and knowledge that is appropriate for each audience

The following Figure 4-5 depicts process roles for the USMC, followed by a description of these roles (Table 11).

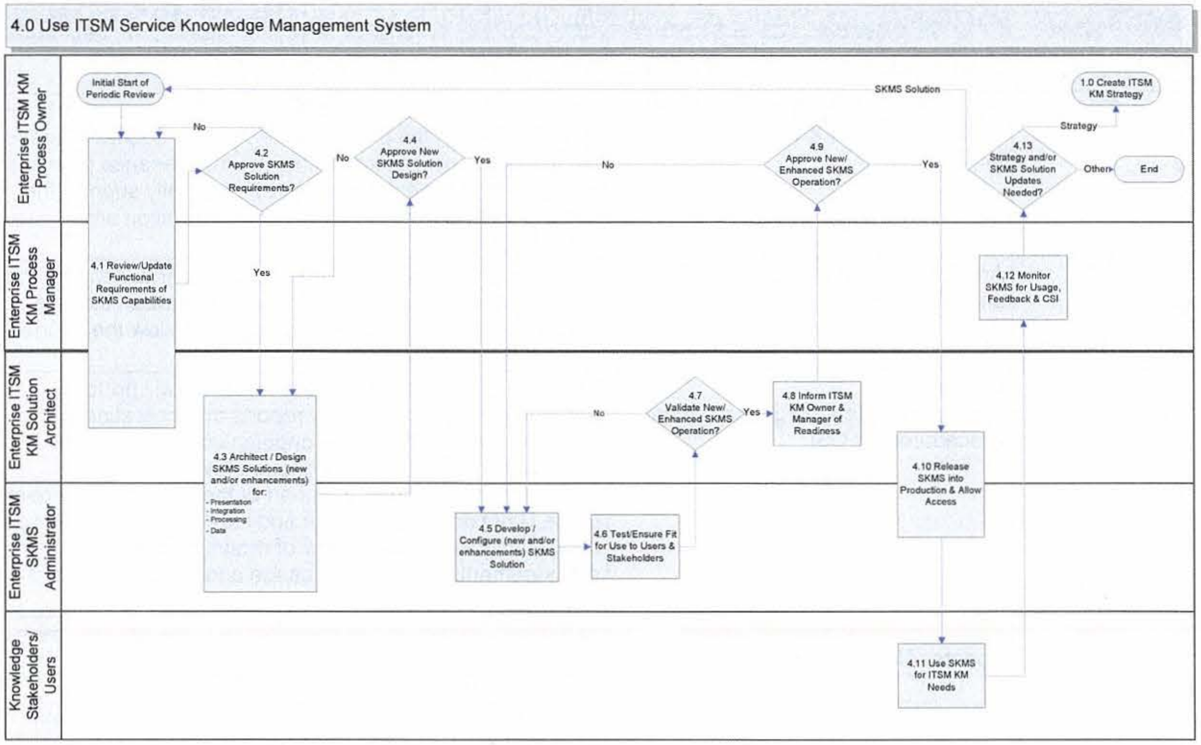
4.0 Use ITSM Service Knowledge Management System
Enterprise ITSM KM Process Owner
Enterprise ITSM KM Process Manager
Enterprise ITSM KM Solution Architect
Enterprise ITSM SKMS Administrator
Knowledge Stakeholders/ Users
Initial Start of Periodic Review
4.1 Review/Update Functional Requirements of SKMS Capabilities
No
4.2 Approve SKMS Solution Requirements?
Yes
No
4.4 Approve New SKMS Solution Design?
Yes
No
4.3 Architect / Design SKMS Solutions (new and/or enhancements) for:
- Presentation
- Integration
- Processing
- Data
4.5 Develop / Configure (new and/or enhancements) SKMS Solution
4.6 Test/Ensure Fit for Use to Users & Stakeholders
No
4.7 Validate New/ Enhanced SKMS Operation?
Yes
4.8 Inform ITSM KM Owner & Manager of Readiness
4.9 Approve New/ Enhanced SKMS Operation?
Yes
4.10 Release SKMS into Production & Allow Access
4.11 Use SKMS for ITSM KM Needs
4.12 Monitor SKMS for Usage, Feedback & CSI
SKMS Solution
1.0 Create ITSM KM Strategy
Strategy
4.13 Strategy and/or SKMS Solution Updates Needed?
Other
End

Figure 4-5. Use ITSM Service Knowledge Management System

Table 11 describes the activities in the Perform Data, Information and Knowledge Management sub-process.

Table 11. Use ITSM Service Knowledge Management System

4.0 Use ITSM Service Knowledge Management System		
Number	**Process Activity**	**Description**
4.1	Review/Update Functional Requirements of SKMS Capabilities	The Enterprise ITSM KM Process Owner, Enterprise ITSM KM Process Manager and Enterprise ITSM KM Solution Architect will collaboratively review the functional requirements needed for an initial design of a SKMS solution or enhancements to the existing SKMS solutions.
4.2	Approve SKSM Solution Requirements?	The Enterprise ITSM KM Process Owner will review and evaluate the requirements and provide approval to move forward with the design of a technical solution for the SKMS requirements. Yes: Go to 4.3 Architect/Design SKMS Solutions (new and/or enhancements) for: Presentation, Integration, Processing and Data (for design) No: Go to 4.1 Review/Update Functional Requirements of SKMS Capabilities (for rework.)

4.0 Use ITSM Service Knowledge Management System		
Number	**Process Activity**	**Description**
4.3	Architect/Design SKMS Solutions (new and/or enhancements) for - Presentation - Integration - Processing - Data	Based on the review of functional requirements, the Enterprise ITSM KM Solution Architect will collaborate with the Enterprise SKMS Administrator to design a comprehensive SKMS solution to provide the needed capabilities at each of the architectural layers (i.e., presentation, integration, processing and data). They will identify what existing components of the SKMS solution may be leveraged as well as any new components required. As part of this analysis, they will scan the market to determine what components may be acquired from vendors. If additional products or services outside of USMC are required, the Acquisition process will be initiated by the Enterprise ITSM KM Process Owner.
4.4	Approve New SKMS Solution Design?	The Enterprise ITSM KM Process Owner will evaluate the new or refined SKMS solution design and approve for implementation. Yes: Go to 4.5 Develop/Configure (new and/or enhancements) SKMS Solution (for implementation.) No: Go to 4.3 Architect/Design SKMS Solutions (new or enhancements) for: Presentation, Integration, Processing and Data (for rework.)
4.5	Develop/Configure (new and/or enhancements) SKMS Solution	The Enterprise SKMS Administrator develops and/or configures the SKMS solution in a non-production environment.
4.6	Test/Ensure Fit for Use to Users & Stakeholders	To ensure the solution meets the requirements, the Enterprise ITSM SKMS Administrator, as well as an independent test team, will test new/enhanced capabilities of the SKMS solution. Testing should address knowledge-sharing and access methods and include end user/stakeholder participation. Testing should also include technical requirements (e.g., performance, security, etc.) to validate delivery of the desired capabilities. Testing details and results will be captured and documented. Other stakeholders such as the Enterprise ITSM KM Process Manager and end users may also be engaged in testing.
4.7	Validate New/Enhanced SKMS Operation?	The Enterprise ITSM KM Solution Architect will review the test results to determine whether or not the new functionality is operating as intended. Yes: Go to 4.8 Inform Enterprise ITSM KM Process Owner & Enterprise ITSM KM Process Manager of Readiness No: Go to 4.5 Develop/Configure (new and/or enhancements) SKMS Solution (for rework)
4.8	Inform Enterprise ITSM KM Process Owner & Enterprise ITSM KM Process Manager of Readiness	Upon completion of the testing in the prior steps, the Enterprise ITSM KM Solution Architect informs both the Enterprise ITSM KM Process Owner and Enterprise ITSM KM Process Manager of the test results.
4.9	Approve New/Enhanced SKMS Operation?	The Enterprise ITSM KM Process Owner will review the test results and approve or disapprove for release into production. Yes: Go to 4.10 Release SKMS into Production & Allow Access No: Go to 4.5 Develop/Configure (new and/or enhancements) SKMS Solution (for rework)

4.0 Use ITSM Service Knowledge Management System		
Number	**Process Activity**	**Description**
4.10	Release SKMS into Production & Allow Access	The Enterprise ITSM KM Solution Architect and Enterprise SKMS Administrator release the solution into the production environment and allow access to the appropriate individuals (in accordance with the Change Management and other relevant processes).
4.11	Use SKMS for ITSM KM Needs	End users and stakeholders with the appropriate rights will use the SKMS to meet their ITSM data, information and knowledge needs and provide feedback.
4.12	Monitor SKMS for Usage, Feedback & CSI	The Enterprise ITSM KM Process Manager will monitor the SKMS and corresponding usage reports on an ongoing basis to determine whether or not the solutions are meeting the stakeholder needs. The Enterprise ITSM KM Process Manager will also review and solicit feedback from end users and key stakeholders on a regular basis.
4.13	Strategy and/or SKMS Solution Updates Needed?	The Enterprise ITSM KM Process Owner will use results of the user feedback and monitoring to drive the next iteration of updates to the ITSM KM Strategy refresh and additional enhancements to the SKMS solution as part of the ongoing continual service improvement cycle. If no updates to the strategy or SKMS solution are identified, the process will end. Strategy: Go to 1.0 Create ITSM KM Strategy SKMS Solution: Go to "Initial Start or Periodic Review" for updates Other: End

Appendix A — ACRONYMS

The official list of E-ITSM acronyms can be found on the Enterprise Information Technology Service Management site (https://eis.usmc.mil/sites/irm/ITSM/default.aspx). The link to the document is referenced below:

https://eis.usmc.mil/sites/irm/ITSM/Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Firm%2FITSM%2FDocuments%2FE%2DITSM%20Acronym%20List&FolderCTID=0x0120001918760B7D35A5478C0474985E3ACBCD&View={9CD820B3-EF85-4D2C-BD0C-A255AEE9E40D}

Appendix B — GLOSSARY

Term	Definition
Asset Management	Asset Management is the process responsible for tracking and reporting the financial value and ownership of assets throughout their life cycle.
Back-out Plan	A Back-out Plan is developed in the Release planning phase. This plan provides a recovery plan to return to the original configuration or process if the release fails to achieve the planned outcome.
Backup	Backup is copying data to protect against loss of integrity or availability of the original data.
Capture	The activity ensures reliable and accurate ITSM Knowledge Artifact(s) needed are identified, input and accessible for sharing.
Change Schedule	A Change Schedule is a document that lists all approved changes and their planned implementation dates.
Configuration Control	Configuration Control is a sub-process of Configuration Management. Configuration Control is a set of processes and approval stages required to change a CI attribute. Configuration Control encompasses the oversight to ensure that a CI is changed through the Change Management process.
Configuration Identification	A sub-process of Configuration Management, Configuration Identification is the selection, identification and labeling of the configuration structures and CIs including their respective technical owner and the relationships between them. CIs become the manageable unit that is planned for release into a configuration controlled environment. The CIs consist of hardware, software, services and documentation.
Configuration Item	A Configuration Item (CI) is any component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System (CMS) and is maintained throughout its life cycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT services, hardware, software, buildings, people and formal documentation such as process documentation and SLAs.
CI Type	CI Type is a category used to Classify CIs. The CI Type identifies the required attributes and relationships for a configuration record. Common CI Types include: server, document, user, etc.
Configuration Management Database	A Configuration Management Database (CMDB) is a database used to store configuration records throughout their life cycle. The Configuration Management System (CMS) maintains one or more CMDBs and each CMDB stores attributes of CIs and relationships with other CIs.
Configuration Management Plan	Document defining how configuration management will be implemented (including policies and procedures) for a particular acquisition or program. (Source: MIL HDBK-61A)
Configuration Management System	A Configuration Management System (CMS) is a set of tools and databases used to manage an IT service provider's configuration data. The CMS also includes information about incidents, problems, known errors, changes and releases and may contain data about employees, suppliers, locations, units, customers and users. The CMS includes tools for collecting, storing, managing, updating and presenting data about all CIs and their relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management processes.
Data	A collection of facts. An n example of data is the date and time at which an incident was logged.
Definitive Media Library (DML)	A DML is single logical storage area that can be in one or more locations in which the definitive and approved versions of all software CIs are securely stored. The DML may also contain associated CIs such as licenses and documentation. All software in the DML is under the control of Change and Release Management and is recorded in the Configuration Management System.
Deployment	Deployment is the activity responsible for movement of new or changed hardware, software, documentation, process, etc. to the live environment. Deployment is part of the Release and Deployment Management Process.

Term	Definition
Deployment Readiness Test	A Deployment Readiness Test is conducted to ensure that the deployment processes, procedures and systems can deploy, install, commission and decommission the release package and resultant new or changed service in the production/deployment environment.
Deployment Verification Test	A Deployment Verification Test is conducted to ensure the service capability has been correctly deployed for each target deployment group or environment.
Early Life Support	Early Life Support (ELS) involves Technical Management or IT Operations providing support for a new or changed IT service for a period of time after it is released. During ELS, the IT service provider may review the KPIs, service levels and monitoring thresholds and provide additional resources for incident management and problem management (when implemented).
EM System	The EM System (EMS) is composed of tools which monitor CIs and provide event notifications. It is a combination of software and hardware which provides a means of delivering a message to a set of recipients. The EMS often requires real-time interaction, escalation and scheduling.
Environment	Environment is a subset of the IT infrastructure used for a particular purpose (e.g., live environment, test environment or build environment). It is possible for multiple environments to share a CI (e.g., test and live environments may use different partitions on a single mainframe computer). In the term physical environment, environment can be defined as the accommodation, air conditioning, power system, etc. Environment can be used as a generic term defined as the external conditions that influence or affect something.
Error	An Error is a design flaw or malfunction that causes a failure of one or more CI or IT services. A mistake made by a person or a faulty process that affects a CI or IT service is also an error.
Escalation	Escalation is an activity that obtains additional resources when needed to meet service-level targets or customer expectations.
Event	An Event is a piece of data that provides information about one or more system resources. Most events are benign. Some events show a change of state which has significance for the management of a CI or IT service. The term 'event' is also used to define an alert or notification created by any IT service, CI, or monitoring tool. Events typically require IT operations personnel to take actions and often lead to incidents being logged.
Event Correlation	Event correlation involves associating multiple related events. Often, multiple events are generated as a result of the same infrastructure fault. Events need correlation to prevent duplication of effort in resolving the original fault.
Exit and Entry Criteria (Pass/Fail)	These are criteria (defined well in advance and accepted by the stakeholders) defined at authorized points in the Release and Deployment Process to set expectations of acceptable/unacceptable results.
Fault	Fault is the deviation from *normal* operation of a CI or a series of CIs. A fault is a design flaw or malfunction that causes a failure of one or more CIs or IT services. Fault is also referred to as an error.
Governance	Governance is the process of ensuring policies and strategy are actually implemented and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring and reporting and taking actions to resolve any issues identified.
Information	Data + Context. In terms of data, it can be defined as a collection of facts from which conclusions may be drawn
Innovation	The process of translating an idea or invention into a good or service that creates value for customers
Key Performance Indicator	A Key Performance Indicator (KPI) is a metric used to help manage a process, IT service, or activity. Many metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the process, IT service, or activity. KPIs are selected to ensure that efficiency, effectiveness and cost-effectiveness are all managed.
Knowledge	Information + Rules. Information combined with experience, context, interpretation and reflection.

Term	Definition
ITSM Knowledge Artifact	ITSM knowledge is stored in units known as ITSM Knowledge Artifacts. Each artifact captures a key facet of knowledge and using the appropriate attributes, documents the relevant information for aiding in decisions or actions. They can include any piece of documentation, work-arounds, notes, emails, directories, articles, white papers, case studies, etc. which exists within an ITSM.
Knowledge Management — Enterprise	Enterprise Knowledge Management is the process which is responsible for the management of enterprise data, information and knowledge across the full life cycle. The Enterprise KM process includes the integration of people and processes, enabled by technology, to facilitate the exchange of operationally relevant information and expertise to increase organizational performance. Reference: • MCO 5400.52 (DON DCIO USMC Roles and Responsibilities) • Forthcoming revision to MCWP 3040.2 (Information Management)
Knowledge Management — ITSM	ITSM Knowledge Management is the process which is responsible for the management of IT Service Management data, information and knowledge across the full life cycle. The ITSM KM process includes the integration of people and processes, enabled by technology, to facilitate the exchange of operationally relevant information and expertise to increase ITSM performance.
Known Error	A Known Error is a problem that has a documented root cause and a work-around. Known errors are created and managed throughout their life cycle by Problem Management. Known errors may also be identified by SIE or suppliers.
Monitoring	Monitoring is the process of repeated observation of a CI, IT service, or process to detect events and to ensure that the current status is known.
Notification	Notification is a communication that provides information.
Pilot	A Pilot is a limited deployment of an IT service, a release, or a process to the live environment. A pilot is used to reduce risk and to gain user feedback and acceptance.
Process	A Process is a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process may include any of the roles, responsibilities, tools and management controls required to reliably deliver the outputs. A process may define policies, standards, guidelines, activities and work instructions, if needed.
Quality Assurance	Quality Assurance (QA) is the process responsible for ensuring the quality of a product and also ensuring it will provide its intended value.
Role	A Role refers to a set of connected behaviors or actions that are performed by a person, team, or group in a specific context.
Severity	Severity refers to the level or degree of intensity.
Service Design Package	A Service Design Package (SDP) is composed of document(s) defining all aspects of an IT service and its requirements through each stage of its life cycle. An SDP is produced for each new IT service, major change, or IT service retirement.
Service Improvement Plan	A Service Improvement Plan (SIP) is a formal plan to implement improvements to a process or IT service.
Service Knowledge Management System	A Service Knowledge Management System (SKMS) is a set of tools and databases used to manage ITSM knowledge and information. The SKMS includes the Configuration Management System (CMS) as well as other tools and databases. The SKMS stores, manages, updates and presents all information that an IT service provider needs to manage the full life cycle of IT services.
Service Level Agreement	A Service-Level Agreement (SLA) is an agreement between an IT service provider and a customer. The SLA describes the IT service; documents service-level targets and specify the responsibilities of the IT service provider and the customer. A single SLA may cover multiple IT services or multiple customers.
Service Validation and Testing	Service Validation and Testing is the process responsible for validation and testing of a new or changed IT service. Service Validation and Testing ensures an IT service matches the design specification and will meet the needs of the business. Service Validation and Testing during release conducts testing in the pre-production System Integration Environment (SIE) and during deployment in the pilot production environment.

Term	Definition
Single Point of Contact	A Single Point of Contact (SPOC) is an agreement used to assign a single, consistent way to communicate within an organization or unit. For example, the Service Desk will be the SPOC for a service provider.
Snapshot	A Snapshot is the baseline as captured by a discovery tool. A snapshot can also be called a benchmark.
Test	A Test is an activity that verifies that a CI, IT service, or process meets its specification or agreed requirements.
Test Environment	A Test Environment is a controlled environment used to test CIs, builds, IT services and processes.
Throttling	Some events do not need to be acted on until they have occurred a number of times within a given time period. This is called Throttling. Once a repeated event has reached its limit for repetition, forward that event to be acted upon.
User Acceptance Testing	User Acceptance Testing is a testing activity conducted by the user intended to verify a CI, IT service, or process meets a specification. It is also used to validate whether agreed requirements have been met.
Wisdom	Knowledge + Experience. The ability to make correct judgments and decisions by making the best use of available knowledge
Work-around	Work-arounds for problems are documented in known error records and are intended to reduce or eliminate the impact of an incident or problem for which a full resolution is not yet available. Work-arounds for incidents that do not have associated problem records are documented in the incident record.
Work Instruction	The Work Instruction is a document containing detailed instructions that specify exactly what steps are followed to carry out an activity. A work instruction contains much more detail than a procedure and is only created if very detailed instructions are needed.