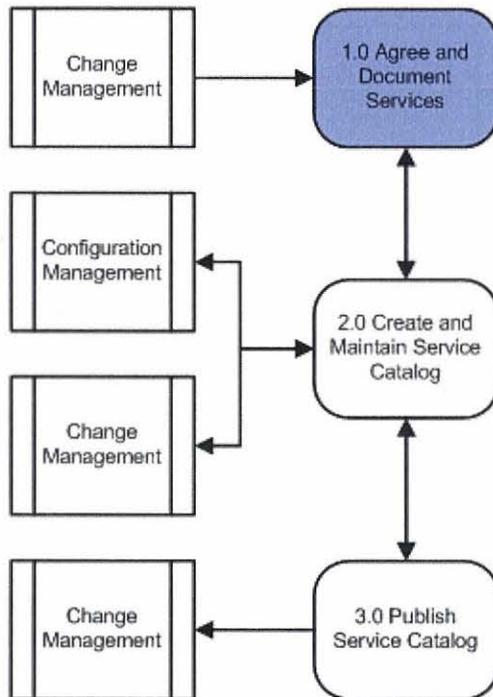


## 4.0 SUB-PROCESSES

### 4.1 Agree and Document Services



Candidate services are identified based upon those specified by the Service Owners and provisioned by the IT provider(s) to the user community. All changes to the Service Catalog, including additions and deletions, are processed through ChM.

The scope of the USMC IT Service Catalog and identification of those services included within the catalog are defined and ultimately authorized by C4 in partnership with MCSC. Through participation in the Enterprise ChM process, the Service Catalog manager and owner will be aware and participate in change analysis and implementation responsibilities for the Service Catalog.

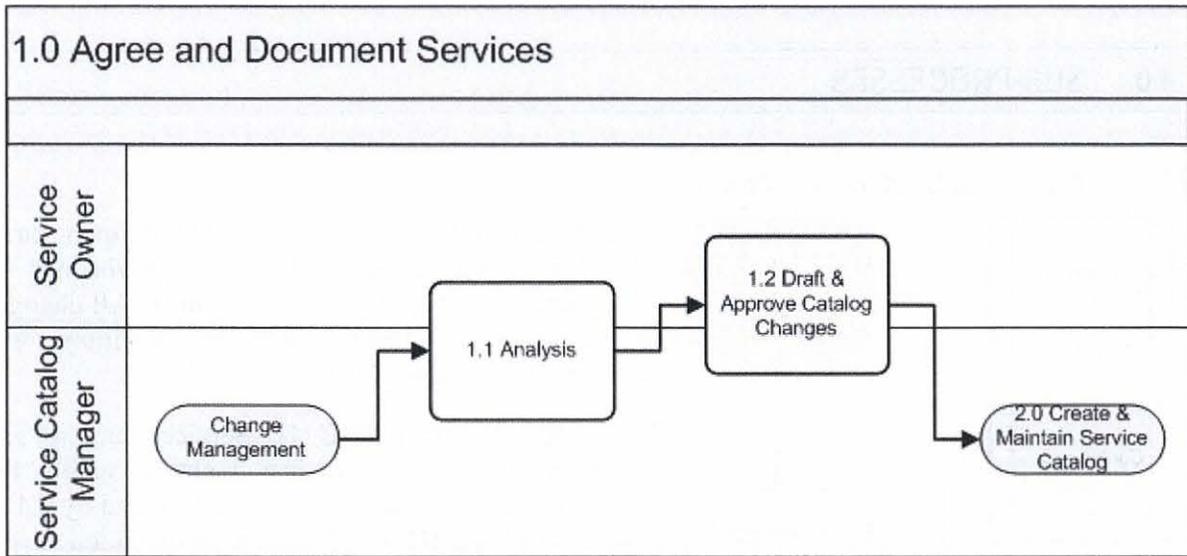


Figure 4. SCM Agree and Document Services Sub-Process

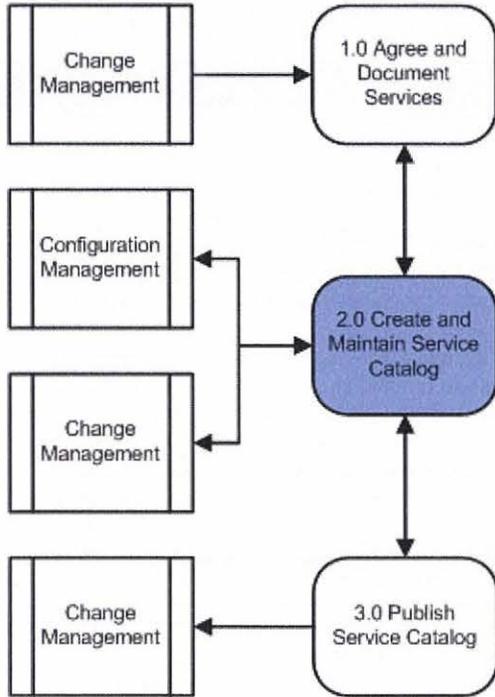
Table 5 describes the sub-process steps for 1.0, Agree and Document Services.

Table 5. SCM Agree and Document Services Sub-Process Descriptions

1.0 Agree and Document Services		
Number	Process Activity	Description
1.1	Analysis	Approved change requests that result in the addition, modification, or deletion of services in the Service Catalog are analyzed by the Service Catalog Manager and appropriate Service Owner to examine impact on the Service Catalog.  The Service Catalog Manager works closely with the appropriate USMC IT Service Owner(s) to consider change requests. A duplication check is conducted as part of this analysis to avoid the duplication of services in the Service Catalog.
1.2	Draft and Approve Catalog Changes	Upon ChM's approval, changes to the Service Catalog are drafted. The details of the change are contained in the RFC and as such the RFC is the guidance for the scope of the changes.  The Service Catalog Manager is accountable for the change and will involve appropriate Service Manager(s), Change Management, and Configuration Management in drafting the Catalog entry, and will also involve the Service Owner and other stakeholders in approval of the change.



## 4.2 Create and Maintain Service Catalog



The Service Catalog comprises two separate views of Service information: the Business Service Catalog and the Technical Service Catalog.

The Business Service Catalog contains details of all IT services delivered to the customer, together with relationships to the business units and the business processes that rely on the IT services, forming the customer view of the Service Catalog.

The Technical Service Catalog contains details of all the IT services delivered to the customer, together with relationships to the supporting services, shared services, components and CIs necessary to support the provision of the service to the business. This catalog underpins the Business Service Catalog and does not form part of the customer view of IT services.

Information about agreed Business Services, as published in the Business Service Catalog, should also be stored in the Configuration Management System (CMS).

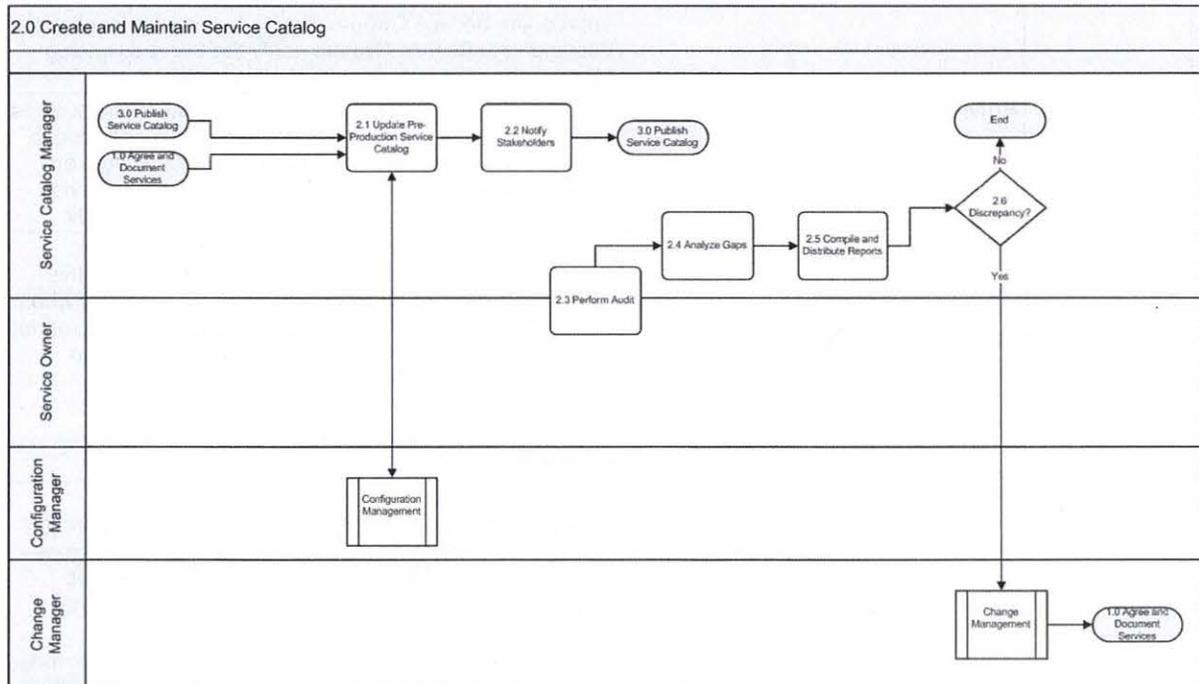


Figure 5. SCM Create and Maintain Service Catalog Sub-Process



Table 6 describes the sub-process steps for 2.0, Create and Maintain Service Catalog.

**Table 6. SCM Create and Maintain Service Catalog Sub-Process Descriptions**

2.0 Create and Maintain Service Catalog		
Number	Process Activity	Description
2.1	Update Pre-Production Service Catalog	The approved Catalog changes are entered with the following objective: when updates are complete, the pre-production Service Catalog will be consistent with the specified changes. The USMC pre-production Service Catalog is updated in conjunction with the change implementation. The Service Catalog Manager executes such changes.
2.2	Notify Stakeholders	Stakeholders are identified as part of the RFC analysis. Stakeholders are notified in conjunction with the change implementation. Depending on the complexity of the change, a communications plan can be developed and employed. USMC Service Catalog stakeholders are identified as members of two primary groups: service stakeholders and catalog stakeholders. Service stakeholders are people who have a responsible, accountable, consulted, informed, or participant role with a particular service. Catalog stakeholders are people who have a responsible, accountable, consulted, informed, or participant role with the SCM process and/or the Service Catalog.
2.3	Perform Audit	Regularly scheduled and ad hoc audits are performed to identify any discrepancies between the Service Catalog content as entered, and the contents of the CMS. Audits are performed by the USMC Service Catalog Manager and the appropriate Service Owners. Discrepancies are identified and documented. Service Owners notify the Service Catalog Manager of audit outcomes for further action.
2.4	Analyze Gaps	Analysis of Service Catalog gaps uncovered by the audit is performed by the Service Catalog Manager in partnership with the appropriate Service Owner(s). Stakeholders are subsequently notified of potential changes to the Service Catalog that are recommended as a result of the audit.
2.5	Compile and Distribute Reports	Reports contain the audit scope, schedule, approach, outcomes, and any recommended remediation activities. Each report will identify who performed the audit and who compiled the report. Reports are delivered to the appropriate stakeholders, to include the SCM Process Owner and appropriate Service Owners. Reports are compiled as a result of any ad hoc or planned/scheduled audits and subsequent analysis performed.
2.6	Discrepancy?	Service Catalog discrepancies are defined as (a) unauthorized changes to Service Catalog contents and (b) differences between Service Catalog contents and the as-deployed environment and/or the CMS. Discrepancies identified as a result of analysis are documented in the report. If no discrepancies are identified, the audit cycle is repeated in the future in accordance with the audit schedule. If there are discrepancies identified, the discrepancy is analyzed to determine the need for an RFC, in consultation with Change Management.





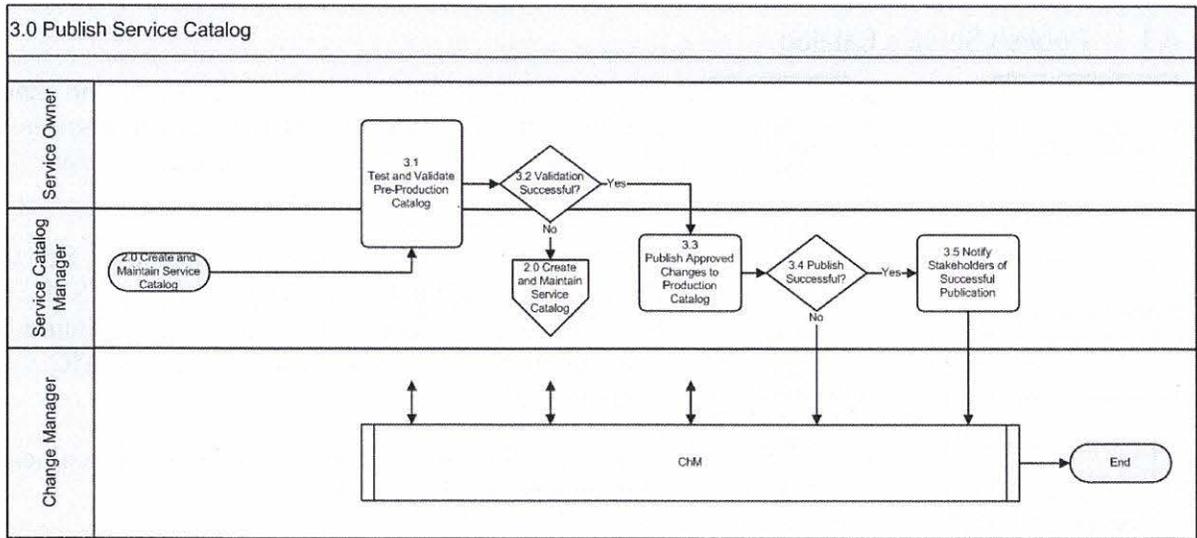


Figure 6. SCM Publish Service Catalog Sub-Process

Table 7 describes the sub-process steps for 3.0, Publish Service Catalog.

Table 7. SCM Publish Service Catalog Sub-Process Descriptions

3.0 Publish Service Catalog		
Number	Process Activity	Description
3.1	Test and Validate Pre-Production Catalog	The Service Catalog Manager and the Service Owner test and validate the approved changes to the pre-production Service Catalog content before the changes are published to the end user-visible (production) version of the Service Catalog.
3.2	Validation Successful?	If the Service Catalog Manager and the Service Owner successfully validate the changes to the pre-production Catalog content, proceed to the next step. If the validation is not successful, the Service Catalog Manager and the Service Owner make any further updates that are necessary to the pre-production Service Catalog.
3.3	Publish Approved Changes to Production Catalog	The Service Catalog Manager ensures that the necessary configuration steps have been taken so that the approved changes are published to the production (end user-visible) version of the Service Catalog during the specified change window.
3.4	Publish Successful?	If the publish is successful, proceed to the next step.
3.5	Notify Stakeholders of Successful Publication	Upon successful completion of the end-user visible Service Catalog publishing operation, the Service Catalog Manager ensures that stakeholders are informed that the end user-visible Service Catalog has been updated as an output from the Change Management Process.



## Appendix A – ACRONYMS

The 2010-12-23 E-ITSM\_TO 13 Acronyms\_List document is the official list of E-ITSM acronyms and can be found through the link referenced below:

<https://ehqmc.usmc.mil/org/c4/projects/CP/eitsm/Shared%20Documents/Forms/AllItems.aspx>



## 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 lifecycle.
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.
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 lifecycle 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 lifecycle. 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.
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.
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.



Term	Definition
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 comprised 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 <i>normal</i> 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.
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.
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 lifecycle 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.



Term	Definition
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 lifecycle. 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 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 lifecycle 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 specifies 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 Systems Integration Environment (SIE) and during deployment in the pilot production environment.
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.
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.



## Appendix C – POLICIES

1. References to industry governing policies and laws can be found through the link referenced below:  
[https://ehqmc.usmc.mil/org/c4/projects/CP/eitsm/Shared%20Documents/E-ITSM\\_TO\\_13\\_Government\\_Policies.doc](https://ehqmc.usmc.mil/org/c4/projects/CP/eitsm/Shared%20Documents/E-ITSM_TO_13_Government_Policies.doc)
2. Information Resources Management (IRM) Standards and Guidelines Program:  
[http://community.marines.mil/news/publications/Pages/IRM5271\\_01C.aspx](http://community.marines.mil/news/publications/Pages/IRM5271_01C.aspx)
3. Marine Corps Order 5271.1B Subj: INFORMATION RESOURCES MANAGEMENT (IRM) STANDARDS AND GUIDELINES PROGRAM dated 1 Dec 2011
4. The DISA Defense Enterprise Service Management Framework (DESMF) brief and document can be found through the links referenced below:
  - Brief:  
[http://www.disa.mil/News/Conferences-and-Events/DISA-Mission-Partner-Conference-2012/~media/Files/DISA/News/Conference/2012/DISA\\_Enterprise\\_Service\\_Management\\_Framework.pdf](http://www.disa.mil/News/Conferences-and-Events/DISA-Mission-Partner-Conference-2012/~media/Files/DISA/News/Conference/2012/DISA_Enterprise_Service_Management_Framework.pdf)
  - DISA Enterprise Service Management Framework Document:  
[https://acc.dau.mil/adl/en-S/534625/file/65830/%23115329%20DESMF\\_edition%201.0.pdf](https://acc.dau.mil/adl/en-S/534625/file/65830/%23115329%20DESMF_edition%201.0.pdf)
5. Marine Corps Information Technology Portfolio Management: MARADMIN 253/11 Link:  
<http://www.marines.mil/News/Messages/MessagesDisplay/tabid/13286/Article/111305/marine-corps-information-technology-portfolio-management.aspx>
6. Marine Corps Order 5230.21 Subj: INFORMATION TECHNOLOGY PORTFOLIO MANAGEMENT dated 3 Oct 2012
7. SECNAV Instruction 5230.15 Subj: INFORMATION MANAGEMENT/INFORAMTION TECHNOLOGY POLICY FOR FIELDING OF COMMERCIAL OFF THE SHELF SOFTWARE dated 10 Apr 2009



## Appendix D – BUSINESS SERVICE CATALOG

The following is a list of the service attributes (service offering detail) associated with services identified for inclusion in the initial version of the Business Service Catalog by the USMC. Thus, information should address the following primary, end user concerns:

- What is the service?
- How do I request the service?
- When can I expect support for this service?
- What level of performance can I expect for the delivered service?

Service Attribute	Intended Use (working definition)
<b>Service Name</b>	Specifies the name of the service.
<b>NIPRNet/SIPRNet Service</b>	Identifies the Service as NIPRNet, SIPRNet, or both.
<b>Service Customers/Users</b>	Describes the intended user community for the Service.
<b>Service Prerequisites</b>	Describes what must be in place before using the Service, such as the existence of a particular type of account.
<b>Request the Service</b>	Describes how to formally request the Service.
<b>Service Terms of Use</b>	Describes the set of conditions within which the Service is authorized to be used (analogous to an End User License Agreement).
<b>Service Short Description</b>	Explains in non-technical terms what the purpose of the Service is.
<b>Service Long Description</b>	Provides a detailed description of the Service.
<b>Service Support</b>	Provides Service Desk contact information and other support information related to the Service.
<b>Service Hours</b>	Describes the period of time during which the Service is available for use and optionally can provide information about recurring periods during which the Service is not normally available (e.g., maintenance windows).
<b>Program(s) of Record</b>	Specifies the Program(s) of Record for the Service.
<b>Technical Service Components</b>	Lists components (Configuration Items) that provide support for the Service.
<b>Technical Prerequisites</b>	Describes technical requirements associated with the use of the service, such as a particular desktop configuration.
<b>Service Lifecycle State</b>	Identifies where the Service is in the Service Lifecycle (Pending [date], Active, or Retired).



Service Attribute	Intended Use (working definition)
<b>Service Owner</b>	Specifies who the Service Owner is and how to contact them.
<b>Service Manager</b>	Specifies who the Service Manager is and how to contact them.
<b>Service Escalation Points of Contact</b>	Specifies site- or function-specific points of contact for the Service (Subject Matter Experts [SMEs]) that can assist with operational issues associated with the Service.
<b>Service Reporting</b>	Describes metrics or data points associated with measurement, reporting, and trend analysis activities for the Service.
<b>Service Level Objectives</b>	Describes operational service level goals or objectives for the Service.
<b>Service Cost</b>	Provides information about costs associated with delivering the Service, for use by decision makers involved with IT governance activities.
<b>Service Continuity Level</b>	Describes parameters associated with backup and recovery and Continuity of Operations for the Service.
<b>Change Model</b>	Describes the Change Model that applies to the Service.
<b>DITIL Mapping</b>	Describes where the Service fits in the DITIL service taxonomy.

