



Sample: Audit Plan

Version 1.0

 **

This work is licensed under a [Creative Commons Attribution 4.0 International License.](https://creativecommons.org/licenses/by/4.0/)

[www.fiitsm.eu](http://www.fiitsm.eu)

Table of Contents

1. Introduction & Context 1

2. General information 1

3. Audit activities 3

4. Audit criteria 6

5. Document control 12

1. Introduction & Context

This document specifies the audit plan for a service management audit to be conducted on behalf of ACME in June 2016. The audit plan has been created under consideration of the Guidelines for management systems auditing according to EN ISO 19011:2011. Audit activities will follow this approach.

The main goal of this audit consists of a baseline assessment of the current basic/core service management system (SMS) at the ACME head office in Taos in the context of delivering IT services to customers with no specific further limitations in scope.

This audit plan shall cover all relevant information for the audit, reflecting in particular planned on-site audit activities and requirements, allowing both the audit team and the auditee to prepare for the audit.

NOTE: This audit plan may be subject to changes after its release / distribution.

1. General information

|  |  |
| --- | --- |
| **Audit objectives** | Baseline assessment of the current basic/core service management system (SMS).  Identification of nonconformities and opportunities for improvement with respect to effectiveness, efficiency and overall organizational maturity, plus definition of follow-up actions. |
| **Audit scope** | SMS of ACME at site Taos to deliver IT services to customers.  **Audit criteria relate to the following topic areas:**  Topic area 1: General requirements for a service management system   * Focus on:   + Top Management Commitment & Responsibility   + Documentation   + Scoping, Planning, Implementing, Monitoring/Reviewing and Continually Improving Service Management * Requirements based on FitSM-1 (Edition 2015 – Version 2.0), Clause 5   Topic area 2: Process-specific requirements   * Focus on:   + Service Portfolio Management (SPM)   + Service Level Management (SLM)   + Service Reporting Management (SRM)   + Service Availability & Continuity Management (SCAM)   + Capacity Management (CAPM)   + Information Security Management (ISM)   + Customer Relationship Management (CRM)   + Supplier Relationship Management (SUPPM)   + Incident & Service Request Management (ISRM)   + Problem Management (PM)   + Configuration Management (CONFM)   + Change Management (CHM)   + Release & Deployment Management (RDM)   + Continual Service Improvement Management (CSI) * Requirements based on FitSM-1 (Edition 2015 – Version 2.0), Clause 6 |
| **Audit client** | ACME  Represented by: Jane Doe |
| **Auditing company** | FITSM Consulting Inc.  Represented by: Jack Smith |
| **Audit team** | Lead auditor: Jack Smith  Co-auditor: Emma Harris |
| **Auditee** | (see audit client) |
| **Language** | Audit plan (this document): English  Interviews: English  Audit report: English |
| **Dates and places** | Date: Monday, 6 June 2016  Time: 9:00-17:45  Audit location: ACME head office, Taos |

1. Audit activities

This schedule may be subject to changes on short notice.

|  |  |
| --- | --- |
| **Date, time** | **Activities** |
| **05/06/2016**  9:00-17:45 | On-site audit activities: opening meeting, collection and verification of evidence (including documentation review, interviews)  **Details:**  **9:00-9:30**  Opening meeting  *Participants:*   * *Jack Smith (Lead auditor)* * *Emma Harris (Co-auditor)* * *Martin Jones (ACME Technical Director; SMS Owner; Process Owner of all ITSM processes)* * *Jane Doe (SMS Manager, Process manager CSI)* * *Carla Stalling (Process Manager SPM, SLM, SRM, CRM)* * *Frederick Avery (Process Manager SUPPM, SCAM, CAPM)* * *Jerome Blank (Process Manager ISM, Chief Security Officer)* * *Paulina Husted (Process Manager ISRM, PM)* * *Michael Maltese (Process Manager CONFM, CHM, RDM)* * *Rita Larriva (Senior staff member at ACME Service Desk)* * *John Smith (Manager Document Control)*   **9:30-10:00**  Top Management Commitment & Responsibility  *Participants:*   * *Jack Smith (Lead auditor)* * *Emma Harris (Co-auditor)* * *Martin Jones (SMS Owner, Process Owner of all ITSM processes* * *Jane Doe (SMS Manager)*   **10:15-11:00**  Documentation  Scoping, Planning, Implementing, Monitoring/Reviewing and Continually Improving Service Management  Continual Service Improvement Management (CSI)  *Participants:*   * *Jack Smith (Lead auditor)* * *Emma Harris (Co-auditor)* * *Martin Jones (SMS Owner, Process Owner of all ITSM processes)* * *Jane Doe (SMS Manager, Process Manager CSI)* * *John Smith (Manager Document Control)*   **11:15-11:45**  Service Portfolio Management (SPM)  *Participants:*   * *Jack Smith (Lead auditor)* * *Emma Harris (Co-auditor)* * *Martin Jones (SMS Owner, Process Owner of all ITSM processes)* * *Jane Doe (SMS Manager)* * *Carla Stalling (Process Manager SPM, SLM, SRM, CRM)*   **11:45-12:30**  Service Level Management (SLM)  Service Reporting Management (SRM)  *Participants:*   * *Jack Smith (Lead auditor)* * *Emma Harris (Co-auditor)* * *Jane Doe (SMS Manager)* * *Carla Stalling (Process Manager SPM, SLM, SRM, CRM)*   **12:30-13:30**  Lunch break  **13:30-14:00**  Service Availability & Continuity Management (SCAM)  Capacity Management (CAPM)  *Participants:*   * *Jack Smith (Lead auditor)* * *Emma Harris (Co-auditor)* * *Jane Doe (SMS Manager)* * *Frederick Avery (Process Manager SUPPM, SCAM, CAPM)*   **14:00-14:30**  Information Security Management (ISM)  *Participants:*   * *Jack Smith (Lead auditor)* * *Emma Harris (Co-auditor)* * *Jane Doe (SMS Manager)* * *Jerome Blank (Process Manager ISM, Chief Security Officer)*   **14:45-15:00**  Customer Relationship Management (CRM)  Supplier Relationship Management (SUPPM)  *Participants:*   * *Jack Smith (Lead auditor)* * *Emma Harris (Co-auditor)* * *Jane Doe (SMS Manager)* * *Carla Stalling (Process Manager SPM, SLM, SRM, CRM)* * *Frederick Avery (Process Manager SUPPM, SCAM, CAPM)*   **15:00-15:45**  Incident & Service Request Management (ISRM)  Problem Management (PM)  *Participants:*   * *Jack Smith (Lead auditor)* * *Emma Harris (Co-auditor)* * *Jane Doe (SMS Manager)* * *Paulina Husted (Process Manager ISRM, PM)* * *Rita Larriva (Senior staff member at ACME Service Desk)*   **16:00-16:45**  Configuration Management (CONFM)  Change Management (CHM)  Release & Deployment Management (RDM)  *Participants:*   * *Jack Smith (Lead auditor)* * *Emma Harris (Co-auditor)* * *Jane Doe (Internal ITSM consultant, ITSM project lead)* * *Michael Maltese (Process Manager CONFM, CHM, RDM)*   **17:15-17:45**  Closing remarks  *Participants:*   * *Jack Smith (Lead auditor)* * *Emma Harris (Co-auditor)* * *Martin Jones (ACME Technical Director; SMS Owner, Process Owner of all ITSM processes)* * *Jane Doe (SMS Manager)* * *Carla Stalling (Process Manager SPM, SLM, SRM, CRM)* * *Frederick Avery (Process Manager SUPPM, SCAM, CAPM)* * *Jerome Blank (Process Manager ISM, Chief Security Officer)* * *Paulina Husted (Process Manager ISRM, PM)* * *Michael Maltese (Process Manager CONFM, CHM, RDM)* * *Rita Larriva (Senior staff member at ACME Service Desk)* * *John Smith (Manager Document Control)* |
|  |  |

1. Audit criteria

All audit criteria are based on the FitSM-1 (Edition 2015) standard for lightweight IT service management and relate to the following topic areas:

* GR: General requirements for a service management system
* PR: Process-specific requirements

|  |  |  |
| --- | --- | --- |
| **Process / category** | **R. #** | **Specification** |
| Top Management Commitment & Responsibility  Top management responsibilities | GR-1.1 | Top management of the organisation(s) involved in the delivery of services shall show evidence that they are committed to planning, implementing, operating, monitoring, reviewing, and improving the service management system (SMS) and services. They shall:   * Assign one individual to be accountable for the overall SMS with sufficient authority to exercise this role * Define and communicate goals * Define a general service management policy * Conduct management reviews at planned intervals |
| Top Management Commitment & Responsibility  Service management policy | GR-1.2 | The service management policy shall include:   * A commitment to fulfil customer service requirements * A commitment to a service-oriented approach * A commitment to a process approach * A commitment to continual improvement * Overall service management goals |
| Documentation  Overall SMS | GR-2.1 | The overall SMS shall be documented to support effective planning. This documentation shall include:   * Service management scope statement (see GR3) * Service management policy (see GR1) * Service management plan and related plans (see GR4) |
| Documentation  Processes | GR-2.2 | Documented definitions of all service management processes (see PR1-PR14) shall be created and maintained. Each of these definitions shall at least cover or reference:   * Description of the goals of the process * Description of the inputs, activities and outputs of the process * Description of process-specific roles and responsibilities * Description of interfaces to other processes * Related process-specific policies as applicable * Related process- and activity-specific procedures as required |
| Documentation  Process outputs | GR-2.3 | The outputs of all service management processes (see PR1-PR14) shall be documented, and the execution of key activities of these processes recorded. |
| Documentation  Document control | GR-2.4 | Documentation shall be controlled, addressing the following activities as applicable:   * Creation and approval * Communication and distribution * Review * Versioning and change tracking |
| Defining the Scope of Service Management  Scope statement | GR-3.1 | The scope of the SMS shall be defined and a scope statement created. |
| Planning Service Management (PLAN)  Service management plan | GR-4.1 | A service management plan shall be created and maintained. |
| Planning Service Management (PLAN)  Service management plan – required contents | GR-4.2 | The service management plan shall at minimum include or reference:   * Goals and timing of implementing the SMS and the related processes * Overall roles and responsibilities * Required training and awareness activities * Required technology (tools) to support the SMS |
| Planning Service Management (PLAN)  Alignment of plans / integrated approach | GR-4.3 | Any plan shall be aligned to other plans and the overall service management plan. |
| Implementing Service Management (DO)  Alignment of plans / integrated approach | GR-5.1 | The service management plan shall be implemented. |
| Monitoring and Reviewing Service Management (CHECK)  Key performance indicators | GR-6.1 | The effectiveness and performance of the SMS and its service management processes shall be measured and evaluated based on suitable key performance indicators in support of defined or agreed targets |
| Monitoring and Reviewing Service Management (CHECK)  Assessments and audits | GR-6.2 | Assessments and audits of the SMS shall be conducted to evaluate the level of maturity and compliance |
| Continually Improving Service Management (ACT)  Identification of nonconformities | GR-7.1 | Nonconformities and deviations from targets shall be identified and corrective actions shall be taken to prevent them from recurring |
| Continually Improving Service Management (ACT)  Planning and implementing improvements | GR-7.2 | Improvements shall be planned and implemented according to the Continual Service Improvement Management process (see PR14). |
| Service Portfolio Management  Maintaining the service portfolio | PR-1.1 | A service portfolio shall be maintained. All services shall be specified as part of the service portfolio. |
| Service Portfolio Management  Planning service design and transition | PR-1.2 | Design and transition of new or changed services shall be planned. |
| Service Portfolio Management  Planning service design and transition – aspects to be considered | PR-1.3 | Plans for the design and transition of new or changed services shall consider timescales, responsibilities, new or changed technology, communication and service acceptance criteria. |
| Service Portfolio Management  Understanding the organizational setup | PR-1.4 | The organisational structure supporting the delivery of services shall be identified, including a potential federation structure as well as contact points for all parties involved. |
| Service Level Management  Maintaining a service catalogue | PR-2.1 | A service catalogue shall be maintained. |
| Service Level Management  SLAs | PR-2.2 | For all services delivered to customers, SLAs shall be in place. |
| Service Level Management  SLA reviews | PR-2.3 | SLAs shall be reviewed at planned intervals. |
| Service Level Management  Evaluating service performance | PR-2.4 | Service performance shall be evaluated against service targets defined in SLAs. |
| Service Level Management  OLAs and UAs | PR-2.5 | For supporting services or service components provided by federation members or groups belonging to the same organisation as the service provider or external suppliers, OLAs and UAs shall be agreed. |
| Service Level Management  OLA and UA reviews | PR-2.6 | OLAs and UAs shall be reviewed at planned intervals. |
| Service Level Management  Evaluating performance of service components | PR-2.7 | Performance of service components shall be evaluated against operational targets defined in OLAs and UAs. |
| Service Reporting  Specification of service reports | PR-3.1 | Service reports shall be specified and agreed with their recipients. |
| Service Reporting  Specification of service reports – required contents | PR-3.2 | The specification of each service report shall include its identity, purpose, audience, frequency, content, format and method of delivery. |
| Service Reporting  Production of service reports | PR-3.3 | Service reports shall be produced. Service reporting shall include performance against agreed targets, information about significant events and detected nonconformities. |
| Service Availability & Continuity Management  Requirements based on SLAs | PR-4.1 | Service availability and continuity requirements shall be identified taking into consideration SLAs. |
| Service Availability & Continuity Management  Plans | PR-4.2 | Service availability and continuity plans shall be created and maintained. |
| Service Availability & Continuity Management  Plans – aspects to consider | PR-4.3 | Service availability and continuity planning shall consider measures to reduce the probability and impact of identified availability and continuity risks. |
| Service Availability & Continuity Management  Monitoring | PR-4.4 | Availability of services and service components shall be monitored. |
| Capacity Management  Requirements based on SLAs | PR-5.1 | Service capacity and performance requirements shall be identified taking into consideration SLAs. |
| Capacity Management  Plans | PR-5.2 | Capacity plans shall be created and maintained. |
| Capacity Management  Plans – aspects to consider | PR-5.3 | Capacity planning shall consider human, technical and financial resources. |
| Capacity Management  Monitoring | PR-5.4 | Performance of services and service components shall be monitored based on monitoring the degree of capacity utilisation and identifying operational warnings and exceptions. |
| Information Security Management  Information security policies | PR-6.1 | Information security policies shall be defined. |
| Information Security Management  Information security controls | PR-6.2 | Physical, technical and organizational information security controls shall be implemented to reduce the probability and impact of identified information security risks. |
| Information Security Management  Reviews of security controls | PR-6.3 | Information security policies and controls shall be reviewed at planned intervals. |
| Information Security Management  Information security events and incidents | PR-6.4 | Information security events and incidents shall be given an appropriate priority and managed accordingly. |
| Information Security Management  Access control | PR-6.5 | Access control, including provisioning of access rights, for information-processing systems and services shall be carried out in a consistent manner. |
| Customer Relationship Management  Customer base | PR-7.1 | Service customers shall be identified. |
| Customer Relationship Management  Customer contact points | PR-7.2 | For each customer, there shall be a designated contact responsible for managing the customer relationship and customer satisfaction. |
| Customer Relationship Management  Communication mechanisms | PR-7.3 | Communication mechanisms with customers shall be established. |
| Customer Relationship Management  Customer service reviews | PR-7.4 | Service reviews with the customers shall be conducted at planned intervals. |
| Customer Relationship Management  Managing customer complaints | PR-7.5 | Service complaints from customers shall be managed. |
| Customer Relationship Management  Managing customer satisfaction | PR-7.6 | Customer satisfaction shall be managed. |
| Supplier Relationship Management  Supplier base | PR-8.1 | Suppliers shall be identified. |
| Supplier Relationship Management  Supplier contact points | PR-8.2 | For each supplier, there shall be a designated contact responsible for managing the relationship with the supplier. |
| Supplier Relationship Management  Communication mechanisms | PR-8.3 | Communication mechanisms with suppliers shall be established. |
| Supplier Relationship Management  Monitoring supplier performance | PR-8.4 | Supplier performance shall be monitored. |
| Incident & Service Request Management  Registration, classification and prioritization | PR-9.1 | All incidents and service requests shall be registered, classified and prioritized in a consistent manner. |
| Incident & Service Request Management  Prioritization based on service targets | PR-9.2 | Prioritization of incidents and service requests shall take into account service targets from SLAs. |
| Incident & Service Request Management  Escalation | PR-9.3 | Escalation of incidents and service requests shall be carried out in a consistent manner. |
| Incident & Service Request Management  Closure | PR-9.4 | Closure of incidents and service requests shall be carried out in a consistent manner. |
| Incident & Service Request Management  Access to relevant information | PR-9.5 | Personnel involved in the incident and service request management process shall have access to relevant information including known errors, workarounds, configuration and release information. |
| Incident & Service Request Management  Keeping users informed | PR-9.6 | Users shall be kept informed of the progress of incidents and service requests they have reported. |
| Incident & Service Request Management  Major incidents | PR-9.7 | There shall be a definition of major incidents and a consistent approach to managing them. |
| Problem Management  Problem identification | PR-10.1 | Problems shall be identified and registered based on analysing trends on incidents. |
| Problem Management  Problem investigation | PR-10.2 | Problems shall be investigated to identify actions to resolve them or reduce their impact on the services. |
| Problem Management  Known errors and workarounds | PR-10.3 | If a problem is not permanently resolved, a known error shall be registered together with actions such as effective workarounds and temporary fixes. |
| Problem Management  Known error database | PR-10.4 | Up-to-date information on known errors and effective workarounds shall be maintained. |
| Configuration Management  CI type definitions | PR-11.1 | Configuration item (CI) types and relationship types shall be defined. |
| Configuration Management  Appropriate level of detail | PR-11.2 | The level of detail of configuration information recorded shall be sufficient to support effective control over CIs. |
| Configuration Management  CMDB | PR-11.3 | Each CI and its relationships with other CIs shall be recorded in a configuration management database (CMDB). |
| Configuration Management  Change control and tracking | PR-11.4 | CIs shall be controlled and changes to CIs tracked in the CMDB. |
| Configuration Management  Configuration verification | PR-11.5 | The information stored in the CMDB shall be verified at planned intervals. |
| Configuration Management  Configuration baselines | PR-11.6 | Before a new release into a live environment, a configuration baseline of the affected CIs shall be taken. |
| Change Management  Registration and classification | PR-12.1 | All changes shall be registered and classified in a consistent manner. |
| Change Management  Assessment and approval | PR-12.2 | All changes shall be assessed and approved in a consistent manner. |
| Change Management  Post implementation review | PR-12.3 | All changes shall be subject to a post implementation review and closed in a consistent manner. |
| Change Management  Emergency changes | PR-12.4 | There shall be a definition of emergency changes and a consistent approach to managing them. |
| Change Management  Acceptance of requests for changes | PR-12.5 | In making decisions on the acceptance of requests for change, the benefits, risks, potential impact to services and customers and technical feasibility shall be taken into consideration. |
| Change Management  Change schedule | PR-12.6 | A schedule of changes shall be maintained. It shall contain details of approved changes, and proposed deployment dates, which shall be communicated to interested parties. |
| Change Management  Fallback plans | PR-12.7 | For changes of high impact or high risk, the steps required to reverse an unsuccessful change or remedy any negative effects shall be planned and tested. |
| Release & Deployment Management  Release policy | PR-13.1 | A release policy shall be defined. |
| Release & Deployment Management  Release planning | PR-13.2 | The deployment of new or changed services and service components to the live environment shall be planned with all relevant parties including affected customers. |
| Release & Deployment Management  Release build and test | PR-13.3 | Releases shall be built and tested prior to being deployed. |
| Release & Deployment Management  Acceptance criteria | PR-13.4 | Acceptance criteria for each release shall be agreed with the customers and any other relevant parties. Before deployment the release shall be verified against the agreed acceptance criteria and approved. |
| Release & Deployment Management  Fallback plans | PR-13.5 | Deployment preparation shall consider steps to be taken in case of unsuccessful deployment to reduce the impact on services and customers. |
| Release & Deployment Management  Monitoring releases for success | PR-13.6 | Releases shall be evaluated for success or failure. |
| Continual Service Improvement Management  Identification and registration | PR-14.1 | Opportunities for improvement shall be identified and registered. |
| Continual Service Improvement Management  Evaluation and approval | PR-14.2 | Opportunities for improvement shall be evaluated and approved in a consistent manner. |

1. Document control

|  |  |
| --- | --- |
| Document ID | [Unique document identifier] |
| Document title | Audit plan – Process and management system audit based on FitSM-1 (Edition 2015) |
| Definitive storage location | n/a |
| Document owner | Jack Smith (lead auditor) |
| Version | 1.0 |
| Last date of change | 2016-05-22 |
| Next review due date | n/a |
| Version & change tracking | n/a |