**Operational Runbook**

System: System Name

Updated: Month, year

Contents

[1 Introduction 3](#_Toc517856783)

[1.1 Purpose of this template 3](#_Toc517856784)

[1.2 Scope 3](#_Toc517856785)

[1.3 Using the template 3](#_Toc517856786)

[1.4 Legal 3](#_Toc517856787)

[2 Architecture 4](#_Toc517856788)

[2.1 Architecture Overview 4](#_Toc517856789)

[2.2 Hardware 4](#_Toc517856790)

[2.3 Software 4](#_Toc517856791)

[2.4 Information 4](#_Toc517856792)

[2.5 Interfaces and Dependencies 4](#_Toc517856793)

[2.6 Test and Quality Assurance 4](#_Toc517856794)

[3 Configuration 5](#_Toc517856795)

[3.1 System Configuration 5](#_Toc517856796)

[3.2 Security Configuration 5](#_Toc517856797)

[4 Operations 6](#_Toc517856798)

[4.1 Change Management 6](#_Toc517856799)

[4.2 Access Management 6](#_Toc517856800)

[4.3 Operational Monitoring 6](#_Toc517856801)

[4.4 Functional Updates 6](#_Toc517856802)

[4.5 Capacity Management 6](#_Toc517856803)

[4.6 Backup and Restore 6](#_Toc517856804)

[4.7 Decommissioning 6](#_Toc517856805)

[5 Troubleshooting 7](#_Toc517856806)

[6 Security 8](#_Toc517856807)

[6.1 Risk Assessment 8](#_Toc517856808)

[6.2 Vulnerability Assessment 8](#_Toc517856809)

[6.3 Security Updates 8](#_Toc517856810)

[6.4 Security Monitoring 8](#_Toc517856811)

[6.5 Incident Handling 8](#_Toc517856812)

[7 Disaster Recovery 9](#_Toc517856813)

[7.1 Disaster Recovery 9](#_Toc517856814)

[7.2 Business Continuity 9](#_Toc517856815)

[8 Service Level Agreements 10](#_Toc517856816)

[9 Regulatory Compliance 11](#_Toc517856817)

[9.1 Sarbanes-Oxley Act (SOX) 11](#_Toc517856818)

# Introduction

## Purpose of this template

This runbook provides the complete operational documentation of *System Name***.** The document should be used to understand how the system is configured and functions, including how to perform system administrative tasks.

The primary audience for this document are personnel responsible for managing and operating the system.

## Scope

*Detailed description of what the operational runbook covers. If there are any limitations on the system in scope, this must be specified here.*

## Using the template

To assist in filling out the runbook correctly, the following applies:

* Highlighted, italicized text throughout the template is provided as background information to assist in creating the document. In the final version of the document, this text must be removed and/or replaced by system-specific information.
* Existing chapters or subchapters shall not be deleted. If a subchapter is considered irrelevant for the system, this must be specified in the body text of the subchapter.
* New subchapters can be added as required. When doing so, the table of contents must be updated.
* Linking to SOPs and information stored in other systems is encouraged.
* No confidential information shall be entered in the runbook itself (although referenced SOPs, with appropriate access control, can contain this type of information).

If the operational documentation is stored in another format than this word document (such as a dedicated system for managing system documentation), the bulleted list above still applies.

## Legal

This document contains information that is proprietary to Equinor ASA. Neither the document nor the information contained therein should be disclosed or reproduced in whole or in part, without express written consent of Equinor ASA.

The document and the information it contains shall be handled according to Equinor’s information classification scheme.

# Architecture

## Architecture Overview

*The overall system architecture and description. If available, provide a link to the relevant system landscape diagram in* [*Equinor EA*](http://eita.statoil.no/companyea/?oid=b1b18bd9-9cca-45a7-9289-9eacf4c7f462/)*.*

## Hardware

*Hardware architecture and inventory for the system, including virtual servers/appliances. Should also include an overview of which components are critical for the system operation. Detailed information on hardware can typically be found in* [*DRM*](https://drm.statoil.com) *and* [*Services@Equinor*](https://statoil.service-now.com/)*.*

## Software

*Software architecture and inventory for the system. Should also include an overview of which components are critical for the system operation. Detailed information on software can typically be found in* [*DRM*](https://drm.statoil.com) *and* [*Services@Equinor*](https://statoil.service-now.com/)*.*

## Information

*Information architecture and inventory for the system. Should describe where information is stored, as well as the information flows within the system.*

## Interfaces and Dependencies

*Interfaces and dependencies towards other systems, both internal and external, regardless of the dependency direction.*

## Test and Quality Assurance

*Description of the test and/or quality assurance environment.*

# Configuration

## System Configuration

*Description of how the system is and shall be configured. Should include details on all configuration done throughout the lifecycle of the system, not just during initial installation.*

## Security Configuration

*Description of how the system is configured in terms of security (system hardening). Should include details on all configuration done throughout the lifecycle of the system, not just during initial installation.*

*Equinor’s information security governance, WR1211, contains topics relevant for this chapter. These include, but are not limited to:*

* *Access control*
* *Authentication*
* *Authorization*
* *Data segregation*
* *Malware protection*
* *Network security*
* *Removal of unused services and accounts*
* *Password policies*
* *Security logging*

# Operations

## Change Management

*The process for making changes to the system.*

## Access Management

*Management and procedures for handling access to the system (joiners, movers and leavers). This description shall cover all accesses provided by IT, both for privileged and unprivileged users.*

## Operational Monitoring

*Monitoring of aspects related to system health and stability.*

## Functional Updates

*Operational procedures for identifying, implementing and verifying updates to the system. This does not include security updates, as these are covered in chapter 7.*

## Capacity Management

*Procedures for scaling the system according to business needs. These procedures should cover both up- and downscaling of the system.*

## Backup and Restore

*Procedures for managing backup and restore of the system.*

## Decommissioning

*Procedures* for decommissioning the system or parts of the system.

# Troubleshooting

*All procedures related to handling of errors and faults in the system.*

# Security

## Risk Assessment

*Link to the current information security risk assessment for the system.*

## Vulnerability Assessment

*Procedures for assessing vulnerabilities in the system. For systems managed by Equinor, the following standard procedure will in most cases apply:* <http://team-2.statoil.com/sites/ts-47273/_layouts/DocIdRedir.aspx?ID=be9d78d4-3704-47b4-9ee9-881b87b7feb9&HintUrl=Metodikk%2fVuln+mgmt+SOP.docx>

## Security Updates

*Procedures for identifying, implementing and verifying security updates to the system. These procedures shall cover both planned and unplanned (out-of-band) security updates.*

*An overview of the considerations which should be made when creating such a patch management program can be found in* [*KB0035618*](https://statoil.service-now.com/selfservice/knowledge_detail.do?sysparm_document_key=kb_knowledge,6a5048ba4f97e2c0bd03ce318110c7f9) *(if the link redirects to the Services@Equinor front page, copy/paste the link into your browser).*

## Security Monitoring

*Description on how security monitoring is performed in the system. This description shall as a minimum cover which events are logged, and how relevant security logs are monitored and/or reviewed.*

*A guide to achieving compliance with Equinor’s logging requirements can be found in* [*KB0035619*](https://statoil.service-now.com/selfservice/knowledge_detail.do?sysparm_document_key=kb_knowledge,5f90007e4f97e2c0bd03ce318110c7f3) *(if the link redirects to the Services@Equinor front page, copy/paste the link into your browser).*

## Incident Handling

*Description of how information security incidents are handled. For systems managed by Equinor, the procedure should be aligned with* [*SF103 - Handle safety and security incident*](http://aris.statoil.no/?objectguid=f9469e01-b2be-11e0-43e7-828060af7619)*.*

# Disaster Recovery

## Disaster Recovery

*Description of the disaster recovery procedures. There is no requirement for a system-specific plan if the system is part of a larger DR plan for the datacenter, and this is considered sufficient.*

## Business Continuity

*Description of the business continuity plans.*

# Service Level Agreements

*Reference to SLAs relevant to the system.*

# Regulatory Compliance

*Description of how the system complies with regulatory requirements. Please verify whether the system in question is subject to the requirements before filling out the sections below.*

## Sarbanes-Oxley Act (SOX)

(Please move content from system’s file in [SOXcritApps](http://team.statoil.com/sites/ts-4248/govdoc/Shared%20Documents/KC1500/SOXcritApps) into this chapter)

|  |  |
| --- | --- |
| Application location: | On prem. Cloud Other: {Specify} |
| User provisioning (roles & access): | AccessIT Other: {Specify}, link to procedure: {Link} |
| Is provisioning considered dis./connected\*? | Connected Disconnected |
| Access approval performed by…\*\* | Statoil Outsourced/3rd party, link to report: {Link} |
| Consider all key controls in KC1500. Would you say any of the controls are performed by a 3rd party for the application?\*\*\* | No Yes I don’t know |

\*: Approval performed in AccessIT, but users manually provisioned in target application/system.

\*\* and \*\*\*: If access approval performed by 3rd party or if your answer is **Yes** or **I don’t know** on control performance, we need to consider running “KC0835 Review of internal control environment at suppliers”. Contact CIT IS to discuss if this is applicable.

|  |  |
| --- | --- |
| Application identified as SOX Critical date\*: | {Enter date} |
| Who (process) nominated the application\*: | {List of processes} |
| Why was it nominated as SOX Critical\*: | SGR Functionality Data processing Automatic CTRL |

\*: This information can be found in the “KC0419 Identify SOX Critical Applications” documentation.

If “Application location” is **“On prem.”** or **“Other”**, continue to fill this table:

|  |  |  |
| --- | --- | --- |
| **Briefly describe the program stack** (application, middleware, DB, OS and other relevant interfaces/batch jobs) **the application operates in.** The purpose of describing the entire program stack is to use that to identify which key controls are relevant to perform for the application and underlaying stack. The scope for any key control is the entire program stack. It is not of interest which technology is used outside Statoil’s domain (at 3rd parties). | | |
| Application stack | | Technology/System (Indicate with “N/A” if not applicable) |
| Application |  | (Same as application above) |
| Middleware |  | N/A Cisco Information Server IBM MQ IBM WebSphere MS BizTalk OAQ SAP BPC SAP NetWeaver SSIS Tibco Web-Services  Other: {specify} |
| Database | Brand | N/A Oracle MS SQL Other: {specify} |
| Names of DB | {Fill in comma separated list of db names} |
| OS | Platform | MS Windows Unix/Linux Other: {specify} |
| Other (g-disks, terminal server, teamsites, develop- ment environment, etc) | | N/A Other: {Briefly describe other components included in the solution} |
| Batch jobs/Interfaces | | N/A Other: {Scope batch jobs as defined in “KC0xyz Periodic review of batch jobs”. List relevant batch jobs and interfaces here.} |

|  |
| --- |
| **Conduct a meeting with the author of** [**IT900 appendix**](http://aris.statoil.no/?modelguid=e961e8b0-8ae4-11e1-44fb-005056bb14af) **(for the process that nominated the application.)**  Purpose of meeting is to identify any risks associated with the application that needs to be added to an appendix. Add a brief statement describing the outcome of this meeting including any changes that needs to be made to appendices. This step is part of the annual part of KC0006. |
| {Brief statement describing meeting outcome and which changes to perform in IT900 appendix} |

Practical info after steps above are completed:

|  |
| --- |
| Name the file: **SOX Crit app -** {**application name as in ServiceNow**}.docx  e.g.:  SOX Crit app - Dispatch Europe.docx  SOX Crit app - AccessIT - Applications and SAP Roles.docx |
| File and keep document updated in this team site: [SOX Critical Applications](http://team.statoil.com/sites/ts-4248/govdoc/Shared%20Documents/KC1500/SOXcritApps)  For team site issues, contact [me](mailto:jahand@statoil.com?subject=Regarding%20SOX%20Crit%20app%20team%20site). |

Key Controls referenced:

KC0419 Identify SOX Critical applications

KC0835 Review of internal control environment at suppliers

KC0xyz Periodic review of batch jobs (correct KC-number will be supplied as soon as control is published)

KC0179 Completeness in the control mapping and control master data