**Operational Runbook**

System: Cloudscape

Updated: JULY 2020

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 *Cloudscape tool.* 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 is personnel responsible for managing and operating the system.

## Scope

*The Runbook will provide the complete details of the Architecture, Data Handling, Security, Process of Data Collection, What Data is collected and Troubleshooting of Cloudscape Tool.* *Also the process flow diagram and other relevant details will also be incorporated in this document in detail.*

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

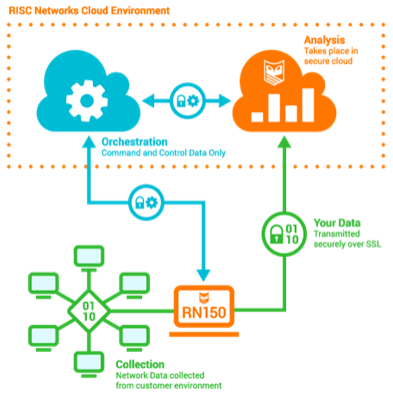
This document contains information that is proprietary to Equinor ASA. Neither the document nor the information contained therein should be disclosed or reproduced in whole or in part, without express written consent of Equinor ASA.

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

# Architecture

## Architecture Overview

*Data is collected by the RN150- the on-prem VM deployed at the Norway location and periodically exported, encrypted, and securely transmitted via TLS to the RISC Networks Secure Cloud Environment (SCE) which is the data repository for the engagement. The data is then accessed by browsing to www.riscnetworks.com and logging in to the assessment portal.The virtual appliance runs an advanced proprietary embedded operating system. This system was developed based on the widely adopted 2.6 Linux Kernel. No access to the appliance is allowed with any protocol with the exception of a RISC Networks management session and those connections initiated by the appliance itself. SSH and ICMP are allowed but are used solely for connectivity testing and troubleshooting. Technology built into RISC Networks’ system allows for a stateful operating system on the virtual appliance for the duration of the assessment. The virtual appliance will be deleted at the successful completion of an assessment following the customer’s process for data handling and deletion.*



## Hardware

*The RN150 Virtual Appliance is a CentOS/Linux Virtual Appliance. It is deployed on on-prem VMware ESX or ESXi Server (Hardware Ver. 8), VMware Player, or VMware Workstation.*

*Resource Default Requirements*

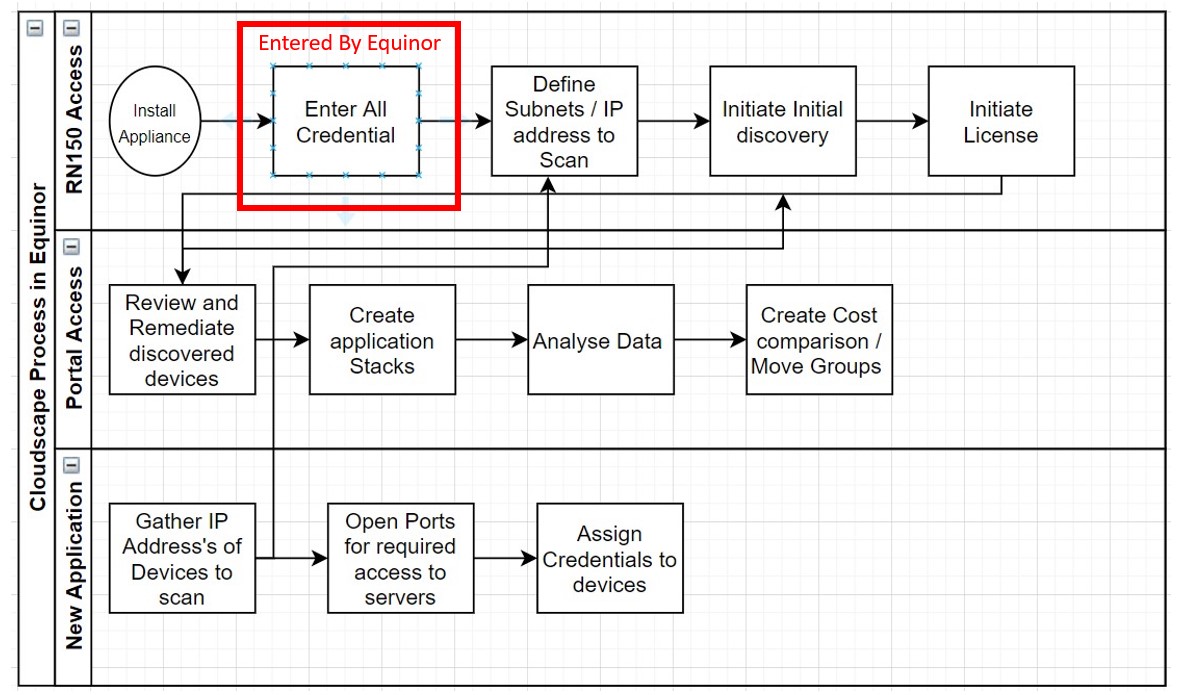
* *8 GB of RAM (minimum 4 GB)*
* *2 vCPUs (minimum 1 vCPU)*
* *50 GB Hard drive (Thin Provisioned)*
* *Internet Access (TCP Port 443 outbound) to the following:*

1. *orchestration.riscnetworks.com ( 34.192.184.110, 34.192.195.90*
2. *initial.riscnetworks.com ( 34.192.43.78, 34.192.198.28) dataup.riscnetworks.com ( 34.192.12.37, 34.192.197.132 )*
3. *app1.riscnetworks.com (34.192.198.73 )*
4. *Backup & Growth (34.192.99.153, 34.192.185.36)*

*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

*The Virtual appliance collects data in three distinct stages: Discovery, Inventory, and Performance. The Process Flow Diagram of the data collection is created. Detailed information on software can typically be found in* [*DRM*](https://drm.statoil.com) *and* [*Services@Equinor*](https://statoil.service-now.com/)*.*



## Information

*Data is collected by the RN150- on-prem VM at the Equinor Norway location and periodically exported, encrypted, and securely transmitted via TLS to the RISC Networks Secure Cloud Environment (SCE) which is the data repository for the engagement.*

## Interfaces and Dependencies

*There are no interfaces or dependencies of Cloudscape on other applications. It will just be used for assessment of on-prem servers for Cloud Migration.*

## Test and Quality Assurance

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

*The Security Team lead by Morten Somby has reviewed the Cloudscape application and approved. Matthew Smith has performed the security risk assessment and vendor risk assessment.*

**

## 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.*

*Cloudscape is a pre-configured third-party tool. As part of initial configuration, static IP should be assigned to the RN 150 virtual appliance and the following ports needs to opened in order to connect and to collect the performance matrix of on-prem server infrastructure for cloud assessment.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Protocol** | **Port** | **Source** | **Destination** | **Usage** |
| TCP | 443 | RN150 | Internet | For communication from the RN150 to the RISC Networks Cloud Orchestration layer |
| ICMP | — | RN150 | Local Networks | By the RN150 for base discovery for available devices |
| TCP | 135 | RN150 | Local Networks | By the RN150 to obtain WMI information from Windows hosts discovered |
| TCP | 1024-65535 | RN150 | Local Networks | RPC Dynamic Port Allocation used for WMI communication. |
| TCP | 80 | RN150 | Local Networks | By the RN150 to obtain HTTP |
| UDP | 161 | RN150 | Local Networks | Used for gathering SNMP information from devices on the Network |
| TCP | 443 | RN150 | Local Networks | Used for gathering VMware guest information directly from vCenter. |
| TCP | 22 | RN150 | Local Networks | By the RN150 to collect from Linux/UNIX servers over the SSH protocol |
| TCP | \* | RN150 | Local Networks | Collection from Linux/UNIX servers via SSH user supplied non-standard TCP ports |
| TCP | 445 | RN150 | Local Networks | SMB over TCP/IP used for application socket collection |
| TCP | 139 | RN150 | Local Networks | SMB over NetBIOS used for application socket collection |
| TCP | 8443 | RN150 | Local Networks | Used for discovering Tomcat and Cisco UC servers\* |
| TCP | 62078 | RN150 | Local Networks | Used for discovering Apple products (iPhone) – iTunes sync over air port |
| TCP | 22 | RN150 | Local Networks | For command line discovery of Cisco Switches and Routers |
| TCP | 1433\*\* | RN150 | Local Networks | For MSSQL database collection only |
| TCP | 1521\*\* | RN150 | Local Networks | For Oracle database collection only |
| TCP | 3306\*\* | RN150 | Local Networks | For MySQL database collection only |

## 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.*

*Privacy and security of Customer’s information, including personal data, are a primary concern for RISC Networks. RISC Networks’ data centers adhere to strict regulatory compliance standards such as:*

* *PCI DSS Level 1*
* *SAS 70*
* *ISO 27001*

*At the end of any engagement, RISC Networks anonymizes data for aggregation reporting. RISC Networks does not collect personal user data such as:*

* *User logins or passwords*
* *Data Files (office documents, text files, etc)*
* *Email Files*
* *Database Files*
* *Any files containing user information*
* *Application payload information*

*RISC Networks is classified as a “Data Processor” under EU privacy laws and shall act only on instructions from its Customer and will have adequate technical and organizational security measures in relation to the processing of any personal data.*

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

* ***Access control****: Access will be granted to Mubashar Hussain, Nupur Biswas and Gangadhar G from HCL Cloud Operating Team and the tool will be accessed via logging into* [www.riscnetworks.com](http://www.riscnetworks.com)
* ***Authentication:*** *Multi-factor Authentication system is in place for logging into the Tool Portal*
* ***Authorization:*** *Managed by Flexera Inc.*
* ***Data segregation:*** *Confidential*
* ***Malware protection:*** *Managed by vendor Flexera Inc.*
* ***Network security:*** *Compliant with security requirements* <https://documentation.riscnetworks.com/overview/architecture%252C-data-handling%252C-and-security/>
* ***Removal of unused services and accounts:*** *Raw customer assessment data is held in RISC Networks’ SCE for a period of up to 35 days past the subscription end date. After the subscription expires, the data is deleted*
* ***Password policies:*** *Credentials are encrypted via AES-256 immediately upon being entered through the appliance web interface. Credentials remain encrypted on the appliance for the duration of the assessment and will be deleted at the time the appliance image is delete from memory. Credentials are NEVER uploaded to RISC Networks’ SCE. RISC Networks delivery engineers never know or have access to the credentials used to bootstrap the appliance.*
* ***Security logging:*** *The encrypted raw data is accessed by the RISC Networks’ platform and is decrypted, stored in transient database instances and accessed for report generation. The portal can be logged in by the users who have been granted the access via MFA.*

# Operations

## Change Management

*The process for making changes to the system.*

*Not Applicable*

## 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.*

*Access will be granted to Mubashar Hussain, Nupur Biswas and Gangadhar G of HCL COP Team from the Cloudscape Portal. Equinor IT Team will not be involved in the access management process.*

## Operational Monitoring

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

*Operational monitoring will be done via accessing into the assessment portal of Cloudscape. The reports will be created for the assessed applications and will be published to the respective application technical owners.*

## 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.*

*Updates are done by Vendor and features are incorporated in the tool. The details of the features of the release notes are published in the vendor website.*

<https://documentation.riscnetworks.com/using-the-platform/release-notes/>

## Capacity Management

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

*Not Applicable.*

## Backup and Restore

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

*Not Applicable.*

## Decommissioning

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

*Raw customer assessment data is held in RISC Networks’ SCE for a period of up to 35 days past the subscription end date. After the subscription expires, the data is deleted and the storage device that data was stored on returns to the pool of data storage available for other RISC Networks’ engagements. When a storage device has reached the end of its useful life, procedures include a decommissioning process that is designed to ensure customer data are not exposed to unauthorized individuals. RISC Networks storage device are decommissioned using the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures the device will be degaussed or physically destroyed in accordance with industry-standard practices. The on-prem VM on which RN-150 appliance was installed will be decommissioned by the server team of HCL after the completion of the assessment.*

# Troubleshooting

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

***Collection Validation***

*The Collection Validation feature is the primary troubleshooting tool for issues relating to data collection for Discovery or Performance collection.*

*The Collection Validation feature is available on the RN150 Virtual Appliance. It allows the user an in-depth review of what data collection activities are performed against a device, and details about any operations that are not successful. The Collection Validation feature is a compliment to the existing Credential Test feature on the RN150, and a crucial part of troubleshooting during the Discovery stage of an engagement.*

*Currently, the Collection Validation feature is only available for the SSH Collection Module, for Linux/UNIX devices using SSH, and for the Windows Collection module, using the WMI and SMB protocols for collection from Windows servers and workstations.*

***Credential Test***

*For each credential type, the Test button is available when entering a new credential or editing an existing credential. The Credential Test feature accepts the IP address of a device, and runs a simple connection and authentication test against that device using the credential entry being operated on. The Credential Test does not test whether the device will respond to ICMP, and only runs the minimum operations required to confirm whether the credential can be used to communicate with the device. The Collection Validation feature has been introduced to go beyond this simple test and to provide extensive detailed feedback, although the Credential Test feature remains a valuable tool in many conditions. The Credential Test feature will, upon a successful test, automatically add the new credential entry or apply a modification to the existing credential entry.*

***Collection Validation of Performance Data***

*The Collection Validation feature, like the Credential Test, can be used when entering a new credential entry or editing an existing credential entry. Selecting the Validate button will open a dialog where the IP address of a device you would like to test against is entered. Once the validation process is complete, a report will be displayed on the screen detailing each operation that was performed, the level of success of that operation, and details on any operations that failed. Unlike the Credential Test feature, Collection Validation will not automatically add a credential entry or update an existing entry.*

*The Collection Validation process is run in the context of a particular credential entry, against a particular device. Once the Validate button has been selected, you will be asked to enter the IP address of a device that you would like to run the Validation process against. Make sure that the IP address you select corresponds to the proper type of device. For instance, if running Collection Validation from the Windows credential section, select a Windows Server or Workstation.*

*The process may take up to a couple of minutes to complete. The Discovery, Inventory, and Performance collection processes will be run against the selected IP address. These processes exactly match the operations that are run during the normal scanning and performance collection stages of the engagement, although the Collection Validation feature does not store any collected data and will not affect any aspect of the platform, such as Assets or reported performance analytics.*

*The validation process will start by confirming that the device will be discovered during a scan of the environment. This involves an ICMP Echo Request (ping) to determine if the device exists on the network, combined with a TCP/UDP port test to discover what protocols are available on the device. If an ICMP Echo Reply is not received, then the validation process will stop. Similarly, if the type of protocol associated with the type of credential being tested is not available, for instance if WMI (TCP 135) is not available when testing a Windows credential, then the validation process will stop, as it will not be able to communicate with the device.*

*Next, the Inventory process will run, which is responsible for collecting the data from the device that is shown in the Assets page. This may include data such as the Operating System type and version, network interfaces and addresses, disk storage, etc. The operations that collect this data will be logged, and the result of each collection operation will be shown. Details on the result codes are provided below. The Discovery process checks to see whether the relevant protocol is reported to be available, but the Inventory process tests the ability to communicate and authenticate with that device using the appropriate protocol. If communication or authentication fails, then the validation process will be stopped, and any available details on why the attempt failed will be displayed.*

*Finally, the Performance collection process will run. When a device is licensed for performance collection, this process is periodically run against that device for the duration of the performance collection period, typically as long as the device is licensed. Like the Inventory process, each operation that is issued to the device for data collection will be logged, along with the result of that operation.*

*Once the collection processes have finished, a report is then presented to provide the details of what operations were performed, the Result Code of each operation, an Overall Status describing how complete the collection activity was, and any available details for operations that did not complete successfully. See below for details on the Overall Status, and the failure details section. This report can also be copied into the clipboard, in case the report needs to be saved or copied to one of our support staff. In order to do this, the Text Version button should be selected, which displays the report as plain text, and then the Copy button should be selected to copy the text into your clipboard.*

***Overall Status***

*The Overall Status provides a high-level status of how complete the data collection activity was. The possible Overall Statuses, and their descriptions are:*

|  |  |
| --- | --- |
| ***Overall Status*** | ***Description*** |
| *SUCCESS* | *All collection operations completed successfully, and the device is fully prepared for participation in the engagement. No further action is required.* |
| *PARTIAL* | *Some non-critical operations did not complete successfully. The device is prepared for participation in the engagement, but some further action may be required to ensure the best possible data. Further action is at the user's discretion.* |
| *FAIL* | *At least one critical operation failed. The device may not be prepared for participation in the engagement, or some critical data will not be available for the device. Further action is required.* |

***Result Codes***

*For each operation run during the validation process, what operation is performed and the result of that operation is logged. Understanding the result codes is the key to understanding the output of the Collection Validation feature.*

*All operations may result in the SUCCESS code, which indicates that the operation completed successfully and collected the associated data. Any other result code shows the manner in which the operation failed, in respect to the outcome of that failure.*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Result Code*** | ***Description*** | ***Overall Status*** | ***Cause for Concern*** |
| *SUCCESS* | *The operation was successful.* | *-* | *No* |
| *FAIL* | *The operation failed, where either the collection attempt was not successful, or data was not returned. A FAIL code is always cause for concern and further action.* | *FAIL* | *Yes* |
| *EXPLORE* | *The operation failed, but the specific operation or the data it is intended to collect is not critical. Often, this indicates an operation that tests for the availability of some data or collection method.* | *-* | *No* |
| *FALLBACK* | *The operation failed, but a fallback operation to collect equivalent data will immediately follow. Used in cases where a preferred operation may not be available, and an alternative method is available.* | *-* | *Maybe (see below)* |
| *INCOMPLETE* | *The operation failed, which results in a failure to collect non-critical data. Correcting the issue is recommended for the best experience with the platform, but not required.* | *PARTIAL* | *User Discretion* |

*Any operation that reports a FAIL result should be investigated and corrected. Under normal collection activity, this may prevent data collection activity for the device or critical data will be missing from the platform.*

*Operations that result in an EXPLORE status can be safely ignored. A failure from an EXPLORE operation will not negatively affect data collection, and is shown in the Collection Validation report for logging purposes.*

*Operations that result in INCOMPLETE may or may not be an issue, depending on what data is interesting in the context of a specific engagement. An operation related to critical data for the platform will never result in an INCOMPLETE. For instance, a failure to collect hardware platform information from a Linux/UNIX device using the SSH Collection Module is not critical for the core value of the platform, but in cases where this data is important for the goals of an engagement further action to correct the issue may be necessary.*

*The FALLBACK result warrants the most explanation. This is reported for an operation that failed, but another (typically less preferred) operation is available to be run immediately afterwards to attempt to collect equivalent data. This means that the operation that is logged immediately following one that reported a FALLBACK result will indicate whether further action is required. If a FALLBACK is immediately followed by a SUCCESS, then the second operation was successful and no further action is required. If a FALLBACK is immediately followed by a FAIL, then all attempts to collect particular critical data were exhausted, and the issue must be corrected. If a FALLBACK is immediately followed by an INCOMPLETE, then all attempts to collect particular non-critical data were exhausted, and further action to correct the issue is at the user's discretion. Collection of particular data may have multiple fallback operations, so a FALLBACK may be immediately followed by another FALLBACK. Such a string of operations will always terminate with a result code other that FALLBACK, which indicates the ultimate outcome of the attempt to collect that data.*

# Security

## Risk Assessment

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

*Risk assessment has been performed by Matthew Smith.*

* *

## 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>

*Not Applicable. It is not a business-critical tool/application. There is no impact on the business, so resilience may not be applicable (in the case of any issues, it can re-installed) and there is no impact to the business or to any other applications.*

## 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 updates will be managed by vendor. The security health-checkup has been performed by HCL COP Team and has been approved by Jorgen Moum and Pradeep Venu Rao from Equinor.*

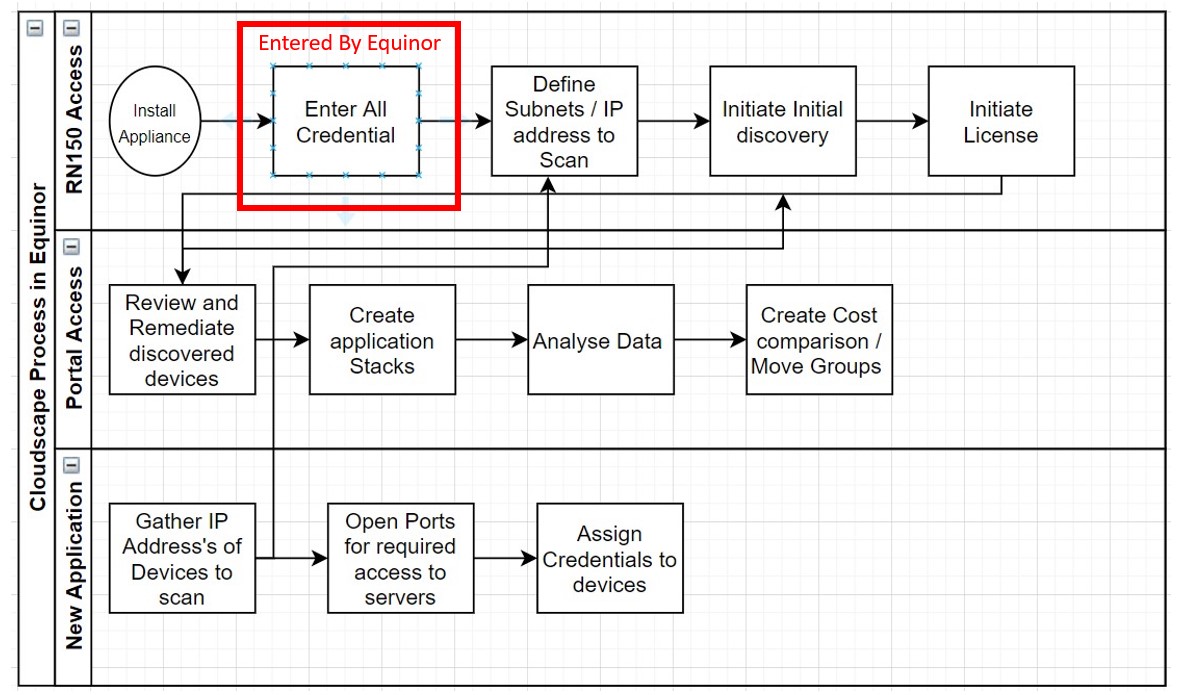
**

## 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).*

*Security will be monitored by Vendor. However a process flow diagram has been created by Mubashar Hussain and shared with Jorgen Moum and Morten Somby.*



## 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)*.*

*Not Applicable. Vendor managed tool.*

# 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.*

*Not applicable. In case of any issues, the Cloudscape tool can be re-installed.*

## Business Continuity

*Description of the business continuity plans.*

*On-going process till the Cloud Migration is completed for in-scope applications.*

# Service Level Agreements

*Reference to SLAs relevant to the system.*

*Not Applicable.*

# 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.*

*Privacy and security of Customer’s information, including personal data, are a primary concern for RISC Networks. RISC Networks’ data centers adhere to strict regulatory compliance standards such as:*

* *PCI DSS Level 1*
* *SAS 70*
* *ISO 27001*

*At the end of any engagement, RISC Networks anonymizes data for aggregation reporting. RISC Networks does not collect personal user data such as:*

* *User logins or passwords*
* *Data Files (office documents, text files, etc)*
* *Email Files*
* *Database Files*
* *Any files containing user information*
* *Application payload information*

*RISC Networks is classified as a “Data Processor” under EU privacy laws and shall act only on instructions from its Customer and will have adequate technical and organizational security measures in relation to the processing of any personal data.*

*Cloudscape is not a SOX Critical Application.*

## Sarbanes-Oxley Act (SOX)

To make sure SOX critical applications are handled according to external requirements, follow this process as the application is set SOX critical in ServiceNow:

[Establish handling of SOX Critical Application](https://statoilsrm.sharepoint.com/:p:/r/sites/CorporateIT-Informationsecurity201/Shared%20Documents/SOX/Handling%20applications/Process%20-%20Handling%20SOX%20Crit%20Apps.pptx?d=we4a572c78bdf4b30b81f31575524e2d4&csf=1&e=etpZgY)

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

Use  to select an option.

|  |  |
| --- | --- |
| Application name: | {Enter name as it’s written in ServiceNow, unambiguously} |
| Application location: | On prem.  Cloud (see KC0835 performance bellow) Other: |

If location is **“Cloud”**, an assessment needs to be conducted regarding the coverage of the audit report provided – if it covers risks described in “KC1500 IT Controls”, is conducted according to standard, is issued at correct time and covers correct period. See “KC0835 Review of internal control environment at suppliers” for more information.

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

|  |  |
| --- | --- |
| Application uses Single Sign-On (SSO): | Yes No |
| User provisioning (roles & access): | AccessIT Other: Link to procedure: Link |
| Is provisioning considered dis./connected? | Connected Disconnected |
| Application identified as SOX Critical date\*: |  |
| Who (process) nominated the application\*: |  |
| 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.

|  |  |  |
| --- | --- | --- |
| **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. | | |
| 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: |
| Database: | Brand: | N/A Oracle MS SQL Other: |
| Names of DBs: |  |
| OS: | Platform: | MS Windows Unix/Linux Other: |
| Other (g-disks, terminal server, teamsites, development environment, etc): | | N/A Other: |
| Batch jobs/Interfaces: | | N/A Other: {Scope batch jobs as defined in “KC0739 Review of batch jobs”. List relevant batch jobs and interfaces here.} |

**Control Mapping: Consider all controls in** [**KC1500 IT Controls**](http://aris.statoil.no/?modelguid=39b23401-a2e7-11e0-55af-005056bb0331) **and decide which controls to perform and which are not relevant.** For any controls that you deem not relevant, document the rationale behind that decision. Contact line manager and collaborate on mapping controls to resources. Line managers perform “KC0179 Completeness in the control mapping and control master data”. Document in the table below who performs which key control for the application.

|  |  |  |  |
| --- | --- | --- | --- |
|  | KC theme: | KC | Application |
| Application Controls | IAM Oversight | KC0006 | {Name of ctrl performer or rationale why no need for ctrl performance} |
| IAM Config | KC0302 | {Name of ctrl performer or rationale why no need for ctrl performance} |
| Joiners | KC0004 | {Name of ctrl performer or rationale why no need for ctrl performance} |
| Leavers | KC0007 | {Name of ctrl performer or rationale why no need for ctrl performance} |
| Special Access | KC0306 | {Name of ctrl performer or rationale why no need for ctrl performance} |
| Development | KC0803 | {Name of ctrl performer or rationale why no need for ctrl performance} |
| Ext Ctrl Env | KC0835 | {Name of ctrl performer or rationale why no need for ctrl performance} |
| Batch | KC0739 | {Name of ctrl performer or rationale why no need for ctrl performance} |
| ChgMgmt\* | KC0203 | {Name of ctrl performer or rationale why no need for ctrl performance} |

\*: Control is not part of KC1500 but essential in Change Management

In addition, you must make sure that risks are handled for supporting application layers. Describe briefly outcome from discussions with representatives from the supporting application layers. In the meeting you need to discuss the risks in the table above and you need to be satisfied with the way the risks are handled:

|  |  |
| --- | --- |
| Middleware: | {Briefly described who was in discussion, when and why risks are handled satisfying at this supporting application layer} |
| DB/Storage: | {Briefly described who was in discussion, when and why risks are handled satisfying at this supporting application layer} |
| OS: | {Briefly described who was in discussion, when and why risks are handled satisfying at this supporting application layer} |
| Other: | {Briefly described who was in discussion, when and why risks are handled satisfying at this supporting application layer} |

The rest of the key controls in KC1500 (KC0104, KC0207, KC0208, KC0419, KC0551, KC0552, KC0586, KC0703, KC0740) are either already mapped to performers or are mapped in projects, and you do not need to explicitly map them for the application.

|  |
| --- |
| **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} |

The performer of “KC0739 Monitoring of automated system jobs” needs to fill in the system job inventory for the application. This can be found here: [Automated System Jobs](https://statoilsrm.sharepoint.com/:x:/r/sites/CorporateIT-Informationsecurity201/Shared%20Documents/SOX/Batch%20job%20inventory/Automated%20System%20Jobs.xlsx?d=w23290754c51a4f1b930c00a02d7b1e95&csf=1&e=sPS46k).

Further, the performer of the control needs to adhere to the template found in this folder: [Templates](https://statoilsrm.sharepoint.com/sites/corporateit-informationsecurity/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2Fcorporateit%2Dinformationsecurity%2FShared%20Documents%2FSOX%2FKC%20performance%20documentation%2F%5Ftemplates)

The document “KC0739 [period] [SOX Crit Apps] [performer] template.docx” serves as a template for control documentation of the control.

The performer of “KC0835 Review of internal control environment at suppliers” needs to adhere to the template found in this folder: [Templates](https://statoilsrm.sharepoint.com/sites/corporateit-informationsecurity/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2Fcorporateit%2Dinformationsecurity%2FShared%20Documents%2FSOX%2FKC%20performance%20documentation%2F%5Ftemplates)

The document “KC0835 [Year] [applicationName] documentation template.xlsx” serves as a template for control documentation of the control.

The SGR coordinator will need periodic support for SGRs (System Generated Reports) in the application (if any). See an overview of currently scoped SGRs for the application in the [SGR Portal](http://team-2.statoil.com/sites/ts-98156/SGR/Lists/SGR%202016/SGRsperApplication.aspx). On the portal’s [homepage](http://team-2.statoil.com/sites/ts-98156/SGR/SitePages/SGRPortal.aspx) you will find brief descriptions of what the SGR coordinator needs support for.

Things to be aware of regarding SOX, performance of key controls and the performance of self-assessments:

* Each control needs to be performed on the frequency described in the control characteristics table in each control
* The frequency of self-assessments (quarterly) in SPC/SAP Process Control are independent of the control frequency
* The control mapping above is the basis for self-assessment of control performance in SPC
* When the control mapping is modified, please contact [CIT IS](mailto:jahand@equinor.com?subject=Update%20Control%20Mapping%20for%20Application)
* All control performances need to be documented and all documentation shall be kept in [KC1500 control performance documentation](https://statoilsrm.sharepoint.com/sites/corporateit-informationsecurity/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2Fcorporateit%2Dinformationsecurity%2FShared%20Documents%2FSOX%2FKC%20performance%20documentation%2FKC0419%2F2019) teamsite under BA subfolders

Key controls referenced ([KC1500 IT Controls](http://docmap.statoil.no/DocMap/page/doc/dmDocIndex.html?DOCVIEW=FALSE?DOCID=1040387)):

KC0419 Identify SOX Critical applications

KC0835 Review of internal control environment at suppliers

KC0739 Monitoring of automated system jobs

KC0179 Completeness in the control mapping and control master data

\_