110 - NORWEGIAN OIL AND GAS RECOMMENDED GUIDELINES FOR IMPLEMENTATION OF INFORMATION SECURITY IN PROCESS CONTROL, SAFETY AND SUPPORT ICT SYSTEMS DURING THE ENGINEERING, PROCUREMENT AND COMMISSIONING PHASES

Norsk olje&gass

Guideline title: Implementation of information security in PCSS/ICT systems during the engineering, procurement and commissioning phases

Entry into force:	01.01.2008
Revision no: 01	Revision date: 01.11.2007
Revision no: 02	Revision date: 15.01.2009
Relevant committee: Operations	Sanction date: 01.01.2008
Norwegian Oil and Gas Guideline 104 approved by: Steering Group Integrated Operations	Approval date: 08.12.2006

Objective of the guideline:
To contribute to the improvement of the overall information security of the offshore industry on the Norwegian Continental Shelf (NCS), specifically safety, regularity and integrity of operations. To ensure that information security is addressed in all relevant phases of an implementation project which includes Information Communication and Technology (ICT) systems in a petroleum production environment.

Status with the authorities:
This guideline has no formal relations to any authority. However, the Petroleum Safety Authority Norway (PSA) and the Norwegian Petroleum Directorate (NPD) have had one observer each in the Work Group Information Security (WG IS) who prepared this document.

Web site location:
This guideline can be downloaded for free from the Norwegian Oil and Gas web site:
http://www.norskoljeoggass.no/retningslinjer/category180.html

TABLE OF CONTENTS

Introduction

The "Information Security Baseline Requirements for Process Control, Safety and support ICT Systems" (ISBR) guideline was issued in June 2006. The guideline consists of 16 requirements to operators and suppliers within the oil and gas industry on the NCS.

ISBR #8 demands that information security of ICT components shall be integrated in the engineering, procurement, and commissioning processes. This document focuses on the activities which need to be performed during the different phases of engineering, procurement and commissioning, with respect to the different ISBR requirements in the Norwegian Oil and Gas Guideline no. 104.

The document lists the typical phases that are included in the engineering, procurement, and commissioning processes. The name of the phases may vary from company to company, and the activities may be shifted in time during a project depending on the companies' methodologies. The companies may have different approaches to the implementation of information security depending on the risk picture and the scope of the project. This document will not specify in detail how the baseline requirements shall be fulfilled, but rather take an overview of the topics which need to be considered by the project organisation as well as the operating organisation.

The target audience for this document include personnel responsible for implementation activities in ISBR #8:

- Project Managers
- Managers responsible for "Call for Tender" and "Request for Proposal"
- Procurement/Purchasing Officers
- Operations Managers

Furthermore the following groups should be acquainted with the document for contribution to timely implementation:

- System and Data Owners
- Design Engineers
- Information Security Managers
- Vendors and suppliers of PCSS/ICT systems and services
- Consultants

Scope

This guideline applies to all ICT systems for Process Control, Safety and Support (PCSS) which are part of any production facility.

The guideline does not apply to deliveries controlled by the corporate office domain. However, if systems needed to sustain production are planned, or by earlier practice, are placed on the corporate office domain, they should be included in the risk assessment to evaluate any measures needed. Typical systems in this category might be weather systems, telecommunication systems, simulators, engineering systems, integrated operations work places, plant production optimizers, information management systems and remote services.

This document addresses the typical phases in a large project, but may also serve as a guideline for smaller modification projects with the difference being that many of the phases already may have information security measures implemented for the activities identified in this document. It is important for all project types on an existing installation to use the guideline in order not to compromise the information security of the installed systems or as a measure to improve existing design or practices.

A note on semantics

This document describes a suggested implementation of ISBR #8 in the Norwegian Oil and Gas Guideline no. 104. Even though it is not mandatory to implement ISBR #8 in accordance with this specification, you will find the word *shall* used in many places throughout the document. *Shall* is used when quoting the requirements listed in the Norwegian Oil and Gas Guideline no. 104. When not referring to the main ISBR document, *should* is used.

Reference

For terms and definitions refer to Appendix C in Norwegian Oil and Gas Guideline no. 104 - Information Security Baseline Requirements for Process Control, Safety and Support ICT Systems. The guideline can be downloaded for free from the Norwegian Oil and Gas website:
http://www.norskoljeoggass.no/retningslinjer/category180.html

Activity timeline

The activities needed for timely implementation of information security are identified in Table 1. The table provides a simplified overview of a project's typical phases from *Process Engineering* with a Functional Design Specification to *Start up* with handover to Operations. The table identifies when the referenced Information Security Baseline Requirements (ISBR) should be addressed.

Two main stakeholders are listed in the table. The Project Organisation should start to address the requirements in the Functional Design Specification. The Organisation for Operations should interface with the Project Organisation and also take ownership of the activities as the organisation is expanding and support services are established.

	Proc. Eng.	Detail Eng.	Build	IAT	FAT	Installation at site	Power on	SAT	Commis-sioning	Start Up
Timeline										→
	FDS	DFDS								WP
Project Organisation	#1 #2	#4 #14 #16	#6 #9 #10 #13[1] #15[2] #16	#11	#12		#12 #13 #15			
Organisation for Operations		#2 #7			#3[3] #9[4] #13 #15		#12 #13 #15		#5	#9[5] #1

Table 1: Implementation timeline with starting point for the different ISBR requirements

NOTE: The ISBR # identifies the *start* of the implementation activity mapped to the delivery phase and the responsible organisation. The ISBR requirements are carried through into the consecutive phases. The responsibility for implementing specific ISBRs may alternate between the two organisations during the entire process. Some ISBRs are explicitly mentioned in more than one phase as different aspects of the ISBR need to be implemented at different times.

[1] Individual vendor/supplier solution and test
[2] Standard manual of operations available for Organisation for Operations
[3] Focus on Roles, Responsibilities and Authorities part of ISBR #3
[4] Focus on Scope of Work (SoW) and preparations for the Service Level Agreement (SLA)
[5] Focus on Service Level Agreement (SLA) for daily operation with the Organisation for Operations having responsibility for all ISBRs with governance from the site Information Security Policy

Detail Eng. = Detail Engineering (Vendor/Supplier is selected)
DFDS = Detail Functional Design Specification
FAT = Factory Acceptance Test
FDS = Functional Design Specification
IAT = Internal Acceptance Test
Proc. Eng. = Process Engineering (Vendor/Supplier might not be selected)
SAT = Site Acceptance Test

WP = Work Permit (Is also applicable in several phases according to company procedures)

Information Security Baseline Requirements

1. An Information Security Policy for process control, safety and support ICT systems environments shall be documented.
2. Risk assessments shall be performed for process control, safety and support ICT systems and networks.
3. Process control, safety and support ICT systems shall have designated system and data owners.
4. Infrastructure shall be able to provide segregated networks, and all communication paths shall be controlled.
5. Users of process control, safety and support ICT systems shall be educated in the information security requirements and acceptable use of the ICT systems.
6. Process control, safety and support ICT systems shall be used for designated purposes only.
7. Disaster recovery plans shall be documented and tested for critical process control, safety and support ICT systems.
8. Information security requirements for ICT components shall be integrated in the engineering, procurement and commissioning processes.
9. Critical process control, safety and support ICT systems shall have defined and documented service and support levels.
10. Change management and work permit procedures shall be followed for all connections to and changes in the process control, safety and support ICT systems and networks.
11. An updated network topology diagram including all system components and interfaces to other systems shall be available.
12. ICT systems shall be kept updated and patched when connected to process control, safety and support networks.
13. Process control, safety and support ICT systems shall have adequate, updated and active protection against malicious software.
14. All access requests shall be denied unless explicitly granted.
15. Required operational and maintenance procedures shall be documented and kept current.
16. Procedures for reporting of security events and incidents shall be documented and implemented in the organisation.

For more guidance on implementation of each ISBR, please refer to Norwegian Oil and Gas Guideline No. 104.

Process Engineering

This phase defines functional requirements and need for information for the PCSS/ICT systems. The system vendors and suppliers have not necessarily been selected at this stage, but the system architecture has been decided and a budget price estimated. The Functional Design Specification is created and used to call for tender from one or more vendors or suppliers. External resources may be used to write the requirements for this phase.

Project Organisation

ISBR #1:	An Information Security Policy for process control, safety and support ICT systems environments shall be documented.
ISBR #2:	Risk assessments shall be performed for process control, safety and support ICT systems and networks.

Information Security Policy applicability to a given project/site should be studied in this phase, because some exceptions might be necessary or reasonable for a given site. Decisions on such exceptions should only be made after careful consideration and the conclusions should be recorded. Exceptions from the policy should only be allowed if fundamental requirements differ from those for which the policy was formulated. Even if no Information Security Policy has been developed for the facilities, the implementation of the remaining ISBRs should still be carried forward.

During this phase a risk assessment should be performed to categorize and prioritize the information needed to control and support the production environment. The process engineering stage should, as a result of the risk assessment, define the functional requirements to support and protect the information assets identified.

The results from the risk assessment should be addressed throughout the subsequent delivery phases. The information asset specifications and requirements should be part of the Call for Tender documentation and be input to the Detail Engineering Phase.

Organisation for Operations

The Organisation may not yet have been established. However, representatives from Operations will typically participate in the Process Engineering phase.

The Organisation for Operations should take responsibility for implementing ISBR #2, starting at the Detail Engineering phase.

Detail Engineering

System vendors and suppliers are in many cases selected prior to this stage as a result of the *Call for Tender* process. The Detail Engineering phase includes specifications for:

- the detail functional design for the various systems;
- architectures and ICT systems in the production environment; and
- networks with interconnections and interfaces to other ICT systems.

The solutions described are often based on the selected vendor's system design and previous practice. This phase is important when implementing good designs, supporting the information security of the plant and information assets. Changes to the system specifications after this point will generally have both cost and time impact.

Project Organisation

ISBR #4:	Infrastructure shall be able to provide segregated networks, and all communication paths shall be controlled.
ISBR #14:	All access requests shall be denied unless explicitly granted.
ISBR #16:	Procedures for reporting of security events and incidents shall be documented and implemented in the organisation.

Vendors and/or suppliers have often been selected at this stage. The Detail Engineering phase describes the system structures and components as well as the functional specifications in processing the information assets. The information asset categorization which is part of the functional requirements will be used as input in the detailed system design.

The system design should address the need for network segregation and communication controls in order to support the information asset categorization and functional requirements.

The design should address continuity aspects and fast recovery in the event of malfunction, degradation modes and planned maintenance.

User access and accounts should be designed according to information asset classification and categorisation.

Security monitoring and incident management should be addressed. Focus should be on the requirements specifying which controls and security measures should be monitored, starting at the Build phase. This should be in place in order to perform the required logging and reporting.

Organisation for Operations

ISBR #2: Risk assessments shall be performed for process control, safety and support ICT systems and networks.

ISBR #7: Disaster recovery plans shall be documented and tested for critical process control, safety and support ICT systems.

Operations representatives should be part of the Project Organisation and work together with the vendors and suppliers to assure a robust and secure design.

The operations representatives should be responsible for action points resulting from the initial information security risk assessment and for creating disaster recovery plans. This work should provide input requirements for the Detail Design phase. In addition, plans for specific ICT system operational procedures should be drafted in line with the requirements specified in ISBR #15.

The functional requirements are defined at an earlier stage, but it is important to follow up the detailed design specifications with proposals for improvements to assure a good design and plans which support the initialisation activities for operations support services and tools.

Build

The build phase implements the Detail Functional Design Specifications. Production environment system components such as computer equipment, network devices and software are purchased, configured and programmed. The information assets are being routed through the various components based on the implemented user and security role specifications.

Project Organisation

ISBR #6: Process control, safety and support ICT systems shall be used for designated purposes only.

ISBR #9: Critical process control, safety and support ICT systems shall have defined and documented service and support levels.

ISBR #10: Change management and work permit procedures shall be followed for all connections to and changes in the process control, safety and support ICT systems and networks.

ISBR #13: Process control, safety and support ICT systems shall have adequate, updated and active protection against malicious software.

ISBR #15: Required operational and maintenance procedures shall be documented and kept current.

ISBR #16: Procedures for reporting of security events and incidents shall be documented and implemented in the organisation.

The build phase is an opportunity to gain operational experience with the selected equipment and software tools in a controlled offsite environment. Multiple system technologies from multiple vendors will be realized at many locations. A complete system integration test with integrated service support tools is not feasible at this stage. Good planning and preparation for the integration tests are important activities which can be performed for the Organisation for Operations if the requirements are part of the Project Organisation scope.

The Project Organisation should ensure that the *Scope of Delivery* includes, as a minimum, that:

- the ICT systems are used for the designated purposes only;
- the suppliers specify recommended service and support levels required for safe and secure operations the ICT system;
  The recommendations are input to the decisions the Organisation for Operations should take when starting the implementation of the ISBR #9 during the FAT phase.
- the requirement for a change management process is initiated in this phase and continued in order to document all changes prior to the hand-over of the responsibility for the systems to the Organisation for Operations;
- the suppliers plan for and perform installation of tools for active protection against malicious software;

Each supplier should test for normal operations with the tools installed and active. In many cases it is not possible to perform the tests with one uniform tool for all suppliers. The tests should be conducted to reduce the risk of control malfunction when configuring the operations phase tools at a later stage when the systems are integrated. The supplier should include plans for removing the preliminary tools in collaboration with the Project Organisation.

- the vendors and suppliers make available and keep track of software updates for optional patch and upgrades as required by the Organisation by Operations;
  A programme for software license maintenance should be included in scope of delivery to assure continued access to updates in subsequent phases.
- the vendors and suppliers provide standard manuals of operations as a minimum at this phase;
  This activity will enable the Organisation for Operations to better plan scope of work in assembling and creating plant specific operating procedures.
- plans are made for granting the Organisation for Operations access to the systems during integration phase at site;
  This is necessary so that the required work processes can be established and the supporting tools can be installed before start up.
- a system for monitoring and reporting security events and incidents is implemented. Logging functionality should be designed and implemented at this stage.

A plan for information security awareness should also be developed and implemented for the Project Organisation.

Organisation for Operations

The responsibility for focused implementation of the information security requirements in the Build project phase is placed on the Project Organisation, and hence there are no specific requirements for the Organisation for Operations in this phase. However, the system owners of the Organisation for Operations should participate in the Project Organisation activities.

IAT – Internal Acceptance Test

Internal Acceptance Tests are performed by each vendor and supplier at their location. The Project Organisations often has a right to witness the testing activities or receive results of the tests.

Project Organisation

ISBR #11:	An updated network topology diagram including all system components and interfaces to other systems shall be available.

The project engineering team should track changes to the ICT systems which are part of the delivery.

A network topology diagram should be created and updated during the change processes.

Organisation for Operations

The Organisation for Operations should start the planning of implementing the Operations philosophies. The implementation of plans will further be performed in the next phases as scope of work for service support is defined. Particular focus should be put on any need for remote services and planning for such integration into the site specific activities. The functional requirements for such services are most likely to be part of the initial function design specification. However, the Organisation for Operations is most often responsible for the work processes, procedures and work instructions which will not be covered by the project deliverables.

FAT – Factory Acceptance Test

The Factory Acceptance Test is performed by the Project Organisation at the vendor or supplier location. However, the ownership resides with the Organisation for Operations with planned access to Project deliverables.

The Organisation for Operations is operative, and System and Data owners participate in the Project Organisation during acceptance tests. The Organisation for Operations can start to implement the operations and maintenance philosophy with respect to service needs, roles and responsibility, and authority definitions.

Project Organisation

ISBR #12: ICT systems shall be kept updated and patched when connected to process control, safety and support networks

The project should install patches against known weaknesses.

Organisation for Operations

ISBR #3: Process control, safety and support ICT systems shall have designated system and data owners.

ISBR #9: Critical process control, safety and support ICT systems shall have defined and documented service and support levels.

ISBR #13: Process control, safety and support ICT systems shall have adequate, updated and active protection against malicious software.

ISBR #15: Required operational and maintenance procedures shall be documented and kept current

Good maintenance and operating practices require adequate implementation time with tuning of tools and procedures well ahead of Start up phase and normal operations.

The Organisation for Operations should define roles, responsibilities and authorities for all system and data owners.

The overall plant operations should be coordinated and supported by documented service and support levels for each system.

The Organisation for Operations should define Scope of Work for the support services. On-site resource strategy together with current off-site resources must be complemented with support services from the various vendors and suppliers.

The combined needs for service and support should be documented and implementation plans made. In particular activities to implement tools, processes and work procedures for operational maintenance should be started and agreed with the Project Organisation.

Earlier phases have assured that the Organisation for Operations has access to the configuration items at site prior to start up.

Installation at site

This phase is included in the description to raise awareness of the asynchronous delivery of system parts.

A long time may have passed from the system were tested at FAT to the equipment is available for installation at site. No practical work can be performed on the equipment in this transit period.

Systems and equipment may have aged with respect to upgrades and patches. It is important that the Project Organisation established update services in earlier phases in order to account for any required changes after installation at site.

Work on existing ISBR activities will be carried forward.

Particular focus on the vendor support agreements will be needed in this phase to take advantage of the time lapse and prepare to implement tools and routines.

Project Organisation

The Project organisation should work together with the Organisation for Operations to further detail on-site activities in the next phases.

Organisation for Operations

Continue work on ISBR #9 to initialise needed data in the support service tools and to make implementation plans and training for work processes covering Change Management and Incident Management. Incident management should include information security incidents as well as functional and service incidents.

Power On

Power On is performed after the equipment has been placed in the local equipment rooms. The network infrastructure may not be complete at this stage. Loop testing and parts of systems may be checked and prepared for *Site Acceptance Testing*. The systems will typically be changed during the next phases. A lot of activities with ad hoc network connectivity will be performed using portable media and temporary service computers. Good routines for change management and routines for clearing media for use with the production equipment must be enforced.

Project Organisation

ISBR #12: ICT systems shall be kept updated and patched when connected to process control, safety and support networks

ISBR #13: Process control, safety and support ICT systems shall have adequate, updated and active protection against malicious software.

ISBR #15: Required operational and maintenance procedures shall be documented and kept current.

Continue established routines in earlier phases or establish on site routines to reduce the risk of introducing malicious code which might be undetected until the systems are interconnected. Tools used during FAT may need to be replaced with the tools selected as part of the support services.

Note: The activities below may need to be carried out after SAT – according to contractual ownership of the equipment.

- The project should perform patches against known weaknesses which may have arisen during the preservation time after FAT.
- The project should support the Organisation for Operations with access to equipment for any changes in tools as required before start up.
- The project should support the Organisation for Operations in making any site specific operating manuals.

Organisation for Operations

ISBR #12: ICT systems shall be kept updated and patched when connected to process control, safety and support networks

ISBR #13: Process control, safety and support ICT systems shall have adequate, updated and active protection against malicious software.

ISBR #15: Required operational and maintenance procedures shall be documented and kept current

The Organisation for Operations is responsible for establishing routines and tools as defined in the ISBR implementation plans. Existing installed tools might need to be replaced. Existing control and systems software may need to be updated or upgraded.

Note: the activities below may need to be carried out after SAT – depending on contractual ownership of the equipment.

- The organisation should work closely with the Project Organisation to make the required changes.
- The organisation should initiate Change Management and Incident Management procedures in preparation for Start up and Operation.

SAT – Site Acceptance Test

In many cases the responsibility for the system equipment delivery is handed over to the Project Organisation after FAT or SAT. The particular procedure may depend on the system. If responsibility is handed over after SAT, it may be difficult to perform the changes specified in the previous Power On phase. Thus, the identified activities may need to be postponed until after the SAT and subsequent handover to the Project Organisation.

Project Organisation

Perform *Site Acceptance Test*. Perform the activities in the previous phase (*FAT*) if the vendor responsibility is handed over to customer at this time.

Organisation for Operations

Perform the activities in the previous phase (*FAT*) if the vendor responsibility is handed over to customer at this time.

Commissioning

The Commissioning phase consists of interconnecting the systems and checking the functionality of the control and safety systems in combination with simulated test runs. Often the phase is conducted with simulated or stimulated input at the field instrument level in order to fully check the functionality of each signal loop up to and including the process operator or information user.

Project Organisation

Continue activities started at *FAT* or after *SAT*.

Organisation for Operations

ISBR #5: Users of process control, safety and support ICT systems shall be educated in the information security requirements and acceptable use of the ICT systems

Prepare the Organisation for Operations for the operational phase by conducting initial training on acceptable use of the systems. In many cases incidents are traced to erroneous operation of the systems. Training schedules should be established and maintained in order to mitigate this risk.

Train personnel on site, any remote sites and support service organisations on the information security requirements and acceptable use of the equipment. In particular any remote connectivity and work processes should have relevant training sessions documented and training schedules should be maintained.

Start Up

A plant is started up in phases. Support systems or package deliveries are started first to support the larger systems. Handover to Organisation for Operations is performed on a subsystem or package level. Thus, the Organisation for Operations should have an active Service Level Agreement in place for this phased start up.

Project Organisation

Continue activities started at Power on or after SAT. Perform handover to Organisation for Operations.

Organisation for Operations

ISBR #1:	An Information Security Policy for process control, safety and support ICT systems environments shall be documented.
ISBR #9:	Critical process control, safety and support ICT systems shall have defined and documented service and support levels.

Ownership of the processes ensuring compliance with the ISBRs is handed over to the Organisation for Operations.

The overall responsible for the operations should ensure that all System and Data owners have reported their need for service and support levels. This activity started in the Build phase for the Project Organisation and the Factory Acceptance phase for the Organisation for Operations.

Work processes, procedures and work instructions for operations, changes and maintenance should be common for all disciplines working in the production environment and also include the service providers.