Base Load Power Hub (BLPH)

CYBERSECURITY SAT PROCEDURE

Document Number: 1724000594-QC-PRO-00044

Document Class: 2

00	27/05/2025	Issue for Review (IFR)	CB	AB	SC
Rev.	Date	Description	Prepared	Reviewed	Approved
YOKOGAWA Co-innovating tomorrow™					

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

Revision / Change Log

Rev.	Description
00	Issue for Review (IFR)

HOLDS LIST

No.	Description
1	
2	
3	
4	

Table of contents

1 Introduction 8
1.1 General 8
1.2 Scope and Objective 8
2 Reference Documents 8
2.1 Input Documents 8
2.1.1 Project Reference Documents 9
2.1.2 YOKOGAWA Project Document 9
2.2 Approved Document List (Detail Design Specification) 9
3 DEFINITIONS AND ABBREVIATIONS 10
4 Responsibility 11
4.1 CUSTOMER 11
4.2 CONTRACTOR 11
4.3 MAC 11
5 General Administration 13
5.1 SAT Venue 13
5.2 SAT Organization Chart 13
5.3 Kick-off Meeting 13
5.4 Daily Working Schedule 13
5.5 SAT Wrap-up Meeting 13
6 SAT Overview 14
6.1 SAT Documentation 14
6.2 Method of Testing 14
6.3 Punch Record 15
6.4 SAT Completion Certificate & System Acceptance Certificate 15
6.5 Safety at work 15
6.6 Test Equipment 15
7 Windows Domain Environment SAT Procedures 16
7.1 Document Update and Configuration Verification 16
7.2 Domain and forest Functional Level 17
7.3 Forward Lookup and reverse lookup Zone 18

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

7.4 Name Resolution 19
7.5 Active Directory Replication 20
7.6 Active Directory Redundancy 21
7.7 Name Resolution Redundancy 22
7.8 Organizational Unit and Group Structure 23
7.9 Verify User Account Compliancy, including non-repudiation 24
7.10 Group Policy Object Structure 25
8 YOKOGAWA Antivirus Software SAT Procedures 26
8.1 Document Update and Configuration Verification 26
8.2 Virus Definition Update 27
8.2.1 The Trellix ePO Server (DMZ) and source site Synchronization 27
8.2.2 YOKOGAWA Antivirus Software Management Virus Definition Update 28
8.3 YOKOGAWA Antivirus Software Management 29
8.3.1 YOKOGAWA Antivirus Software Clients Communication 29
8.3.2 ePolicy Orchestrator Exclusion List 30
8.3.3 YOKOGAWA Antivirus Software Full Scan Impact 31
8.4 Trellix ePolicy Orchestrator Server 32
8.4.1 Trellix ePO Server Policy Verification 32
9 YOKOGAWA Application Whitelisting SAT Procedures 33
9.1 Document Specification and Configuration Verification 33
9.2 Protection from Execution of Unmanaged Program in enable mode 34
9.3 Change Operation Mode of Whitelisting 35
9.3.1 Changing to Observe Mode and Enable Mode 35
9.4 Trellix ePolicy Orchestrator Server 36
9.4.1 Trellix ePO Server Policy Verification 36
10 S Patch Management SAT Procedures 37
10.1 Document Update and Configuration Verification 37
10.2 OS Patch Management Server 38
10.2.1 OS Patch Management Server Verification 38
10.2.2 OS Patch Management Server Configuration Verification 39
10.2.3 WSUS Synchronization Check 40
10.3 OS Patch Management Client 41
10.3.1 Client Configuration 41
10.3.2 Patch Approval 42

10.3.3 Installed Patch Verification 43
11 BRS (Backup Recovery System) 44
11.1 Document Verification 44
11.2 Backup Software Version Verification 45
11.3 Backup and Recovery System - Schedule Backup Policies 46
11.4 Backup and Recovery System - Image Backups 47
11.5 Backup and Recovery System - Image Recovery 48
11.6 Backup and Recovery System - Report 49
12 Network Management SAT Procedures 50
12.1 WUG Software Version & License 50
12.2 NMS Log Management 51
12.3 Network Status 52
12.4 Resource Management and Utilization 53
12.5 Network Device Resource Management and Utilization 54
12.6 WUG Configuration Backup Test 55
12.7 WUG Configuration Restore Test 56
12.8 Network Scan to Discover Systems 57
13 Network INFRASTRUCTURE SAT Procedures 58
13.1 Document Update and Configuration Verification 58
13.2 Network Architecture Verification 59
13.3 Login Banner Verification 60
13.4 VLANs 61
13.5 Un-used ports management 62
13.5.1 Physical Locks at network devices/components 62
13.6 Pin switch redundency 63
13.6.1 1 Turning off one of the Redundant Pair Network Switch and check the Network Connectivity 64
13.6.3 Disabling un-used ports 63
14 Firewall SAT Procedures 65
14.1 Document Update and Configuration Verification 65
14.2 Default Policy Configuration Deny All - Allow by Exception 66
14.3 Firewall "Objects" Configuration 67
14.4 Firewall Network Segmentation 68

14.5 Firewall "Fail Close" 69
14.6 Firewall Login Banner Verification 70
15 Switch SAT Procedures 71
15.1 Document Specification and Configuration Verification 72
15.2 Switch configuration 73
16 Remote Access Facility SAT Procedures 74
16.1 Document Specification and Configuration Verification 74

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

List of tables

Table 1 – Definitions and Abbreviations 11
Table 2 – Daily Working Time 13

1 INTRODUCTION

1.1 GENERAL

The purpose of this document is to define the methods and documentation that will be used to carry out the Site Acceptance Test (SAT) on YOKOGAWA's Network Security. The SAT is performed to ensure that the system is properly configured, assembled and functional in accordance with the intended design as specified in the approved documents.

The Objective of SAT is to demonstrate to CROSSWIND that the system hardware and software is built in accordance with requirements as specified in the approved documents.

CROSSWIND and Rosetti Marino would witness to verify the test. Upon successful completion of the test, a SAT Test Certificate to be signed for the acceptance of the test.

1.2 SCOPE AND OBJECTIVE

The Site Acceptance Test referred to as SAT applies to the Network Hardware and Software supplied by YOKOGAWA.

The objective of the SAT is to verify the conformance of the system against the approved specifications and SAT procedure before delivery to site. The SAT shall be conducted to test and verify the main items listed below:

- Security and Administration
- Windows Domain and Account Management
- Antivirus Management
- OS Patch Management
- Backup and Recovery Management
- Network Management System
- Network Infrastructure
- Application Whitelisting
- Firewall
- Switch
- Remote Access Facility

2 REFERENCE DOCUMENTS

2.1 INPUT DOCUMENTS

The OT Network and Systems security is configured by the reference of these documents in the below listed table.

2.1.1 Project Reference Documents

Doc. No.	*Description*
123A90-DDL-IN-DD-40019 Rev.00	Data Network Architecture Drawings
123A90-DDL-IN-DD-40029 Rev.00	Automation Detailed Design and Construction Package
123A90-DDL-IN-RE-40023 Rev. 00	Cyber Security Design Philosophy
123A90-DDL-IN-RE-40093 Rev. 00	Control System Philosophy

2.1.2 YOKOGAWA Project Document

Doc. No.	*Description*
1724000594-IN-RE-00041 Rev00	Cyber security Workshop Preparation
1724000594-QC-ITP-00002 Rev01	INSPECTION AND TEST PLAN
1724000594-QC-PRO-00031 Rev00	SW FACTORY ACCEPTANCE TEST (FAT) PROCEDURE
1724000594-IN-SP-00018 Rev02	PCS and SAFETY SYSTEMS Software Functional Design Specification (FDS-SW)
1724000594-IN-DG-00023 Rev01	NETWORK AND SERVER CABINETS IN OER ROOM WIRING DIAGRAMS AND TERMINAL STRIPS
1724000594-IN-RE-00035 Rev01	Cyber Security Risk Assessment REPORT
1724000594-IN-RE-00043 Rev00	CYBER SECURITY SETTINGS
1724000594-IN-DA-00011 Rev02	NETWORK AND SERVER CABINETS IN ITER ROOM GENERAL ARRANGEMENT DRAWINGS AND INTERNAL LAYOUT
1724000594-IN-DA-00012 Rev01	NETWORK AND SERVER CABINETS IN OER ROOM GENERAL ARRANGEMENT DRAWINGS AND INTERNAL LAYOUT
1724000594-IN-DD-00015 Rev03	System Architecture
1724000594-IN-DG-00016 Rev01	Network Connection Diagram
1724000594-IN-LIS-00007 Rev01	Systems Cables List
1724000594-IN-DG-00022 Rev01	NETWORK AND SERVER CABINETS IN ITER ROOM WIRING DIAGRAMS AND TERMINAL STRIPS

2.2 APPROVED DOCUMENT LIST (DETAIL DESIGN SPECIFICATION)

The Detail Design Specification used for construction shall be listed in this approved document list, and shall be used as reference in the SAT. In principle, the Detail Design Specification documents as included in this list shall form the basis for checking the Network system. The approved Detail Design Specification document list used for construction is listed in 2.1.2.

3 DEFINITIONS AND ABBREVIATIONS

COMPANY or Client (CPY):	Crosswind
CONTRACTOR (CTR):	ROSETTI MARINO
PROJECT:	HOLLANDSE KUST NOORD WIND PARK Project

Doc. No.	Description
• ICS	Industrial Control System
• IACS	Industrial Automation & Control System
• AD DS	Active Directory Domain Services
• DC	Domain Controller
• DNS	Domain Name System
• GPO	Group Policy object
• RID	Relative Identifier
• PDC	Primary Domain Controller
• PIN	Plant Information Network
• OU	Organizational Unit
• CMD	Command Prompt
• SQL	Structured Query Language
• SFP	Small Form-factor Pluggable
• HIS	Human Interface System
• Vlan	Virtual LAN
• USB	Universal Serial Bus
• GPS	Global Positioning System
• ePO	ePolicy Orchestrator
• DMZ	Demilitarized Zone
• ENS	End Point Network Security
• FTP	File Transfer Protocol
• NTDS	NT Directory Service
• SSL	Secure Socket Layer
• EPC	Engineering Procurement and construction Contract
• HTTPS	Hyper Text Transfer Protocol Secured
• VBR	Veeam Backup & Replication
• BRS	Backup and Recovery Server
• WL	Whitelisting

• WUG	WhatsUp Gold
• TCP	Transmission Control Protocol
• UDP	User Datagram Protocol
• SNMP	Simple Network Management Protocol
• ACL	Access Control List
• NMSSVR	Network Management Server
• DCSVR01	Domain Controller Server 1
• DCSVR02	Domain Controller Server 2
• AVSVR	Antivirus Server
• WSUS	Windows Server Update Service
• CISVR01 & CISVR02	CI Server
• FDS	Functional Design Specification
• FAT	Factory Acceptance Test
• SAT	Site Acceptance Test

Table 1 – Definitions and Abbreviations

4 RESPONSIBILITY

Responsibilities for each party involved in the SAT are defined here-under to ensure that the SAT is carried out in accordance with the agreed procedure. It also ensures that there shall be authorized personnel(s) from Rosetti Marino, CROSSWIND and YOKOGAWA to facilitate any decisions and schedule changes that have resulted from the SAT.

4.1 CUSTOMER

The full participation of CROSSWIND in the SAT is essential. CROSSWIND shall appoint an Inspector cum Test Approver to witness the SAT. The Test Approver would have the authority to sign-off the check sheets on successful completion of all tests. Once signed off, the test will be deemed accepted and the decision will be final. The Test Approver shall participate in the test and observe the test results daily. The Test Approver shall approve the inspection items based on the test results recorded.

4.2 CONTRACTOR

Rosetti Marino shall appoint a SAT Manager for the SAT. Rosetti Marino SAT manager shall co-ordinate with CROSSWIND and YOKOGAWA SAT Managers to facilitate the smooth execution of the SAT activities and schedule. The role of the SAT Manager is also to resolve SAT issues on a regular basis.

4.3 MAC

YOKOGAWA as MAC shall appoint a Test Conductor to organize and manage all aspects of SAT. Yokogawa shall be responsible for carrying out the testing and recording the test results on a daily basis together with Rosetti Marino representative and CROSSWIND Inspector.

The Site Manager representing YOKOGAWA shall be the SAT Manager and co-ordinate with Rosetti Marino SAT Manager and adjusts the test schedule whenever necessary to ensure the smooth running of the SAT. The SAT Manager shall also ensure that all tests are conducted in accordance with the SAT documents. If changes / modifications are required, the SAT Managers from YOKOGAWA and Rosetti Marino shall discuss and determine the action plan YOKOGAWA

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

5 GENERAL ADMINISTRATION

5.1 SAT VENUE

All the Network Security equipment will be installed by Site Construction Contractor selected by Rosetti Marino. The tests shall be conducted on-site.

5.2 SAT ORGANIZATION CHART

A detailed Organization Chart shall be issued for SAT, with all positions and names filled in. In addition, a SAT roster of the participants shall be issued, with following details for each person: full name, company, responsibility, samples of the signature and initials, actual start and finish date of participation in the SAT. Rosetti Marino shall be responsible for maintaining the roster and keeping it updated.

Refer to Appendix-19.1 for SAT organization chart and SAT roster.

5.3 KICK-OFF MEETING

An initial kick-off Meeting will be held prior to starting the SAT to brief the participants, confirm the organization and responsibilities, and review the SAT schedule. At the same time HSE briefing for all participants will be provided by Rosetti Marino/CROSSWIND. YOKOGAWA SAT Manager will prepare the presentation and explain the organization and work practices.

All SAT documentation prepared by Rosetti Marino/CROSSWIND prior to SAT will be inspected for completeness.

5.4 DAILY WORKING SCHEDULE

The SAT will be conducted in Project Site premises from Monday to Friday (working days). The following timing is recommended for the testing:

0900 to 1200 hrs	Inspection and test
1200 to 1300 hrs	Lunch
1300 to 1700 hrs	Inspection and test
1700 to 1730 hrs	Daily review meeting including next day's schedule planning

Table 2 – Daily Working Time

5.5 SAT WRAP-UP MEETING

At the completion of the SAT, a final wrap-up meeting will be held. The overall status of the SAT shall be reported. Upon all parties' agreement that the SAT is completed satisfactorily, Rosetti Marino/CROSSWIND shall sign off SAT Completion Certificate and System Acceptance Certificate.

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

6 SAT OVERVIEW

Cyber security solutions is a part of SAT. This SAT procedure describes the activities and the requirements that are necessary to confirm that all the cyber security solutions installed on-site meets the project standards and functions as per the approved design engineering / construction drawings. The main objectives of performing the SAT is to facilitate Rosetti Marino/CROSSWIND to check and verify the following.

There are no physical (visible) damages (during shipping and installation) to the system that was inspected during FAT and IFAT.

All manufacturing and assembly that were inspected during the FAT and IFAT remain so and are not affected during the shipment.

The Network components that were inspected during FAT and IFAT do function properly and are not affected during the shipment.

To ensure that all carried over punch items identified as per FAT and IFAT report are addressed.

The Software with proper revisions has been loaded on the respective systems.

All equipment and system cables that have been disconnected for shipment are properly reconnected and is working as expected.

The Site Acceptance Test (SAT) shall be conducted in accordance with the test procedures detailed in this document. The test results shall be recorded in the Check sheet. Each Check sheet shall be given a unique reference number.

6.1 SAT DOCUMENTATION

YOKOGAWA shall prepare all SAT documentation prior to the start of SAT of a particular plant or area. All forms, Check-sheets, sign off sheets, drawings, etc. as listed in this procedure shall be organized in indexed binders. A master index for the area will be provided and maintained by the individual site team(s).

The documentation for hardware checks shall include all relevant documents for each individual cabinet in a separate indexed binder or a binder section.

All SAT reference documents (latest issue) as listed in this procedure originated by other parties, which were issued formally to YOKOGAWA, will form a part of the SAT documentation and shall be printed out, and organized in indexed binders by YOKOGAWA.

All SAT reference documents as mentioned above shall be stamped “SAT MASTER” on every page/sheet (or printed with a watermark). Any additional documents as may be necessary and generated later during SAT shall also be stamped, and indexes amended accordingly.

6.2 METHOD OF TESTING

Detailed test procedure for each test item is described in this document. Check-sheet shall be provided, listing the equipment to be tested. All test results shall be recorded in the Check-sheets. The following color codes shall be used in the testing:

a) Yellow marker – Items that were checked and cleared

b) Pink marker – Items that were having issues

c) Green marker – Items that were checked after completion of recovery/resolution of issue

6.3 PUNCH RECORD

Any deficiency found during the test shall be noted in the SAT Punch Record. Each punch Record shall cover one punch item/fault. A Punch Record Ledge shall be used to summarize all the punch records. Punch record items shall be classified as follows:

M = Modification, item is to be modified, deleted, added due to design input changes.

C = Correction, item is to be corrected by YOKOGAWA.

If the recovery work involves change/modification, it is to be recorded on the punch record and the recovery shall be carried out after the agreement of both the SAT managers. YOKOGAWA shall clear all correction items (Code C) as per the identified resolutions. For recovery work that involves modification (Code M), the item will be jointly reviewed by all parties on a daily basis and determined whether to be implemented during SAT or later, depending on complexity and potential schedule and/or cost impact. After verification, all concerned parties in the punch record will sign off the same.

The punch record will be reviewed during the daily meeting and the action to be taken will be discussed and finalized. If the modification request were deemed deviated from the original design, it would be considered as variation order.

6.4 SAT COMPLETION CERTIFICATE & SYSTEM ACCEPTANCE CERTIFICATE

Upon completion of the SAT, a SAT Completion Certificate and System Acceptance Certificate will be signed by CROSSWIND, Rosetti Marino and YOKOGAWA. The purpose of these two documents is to certify that the SAT has been completed and accepted by Rosetti Marino/CROSSWIND. Both Rosetti Marino/CROSSWIND and YOKOGAWA agree that the system is in order and can be released for the next stage of site activities. However, if the tested system is to be accepted in partial for whatever reasons, Rosetti Marino shall advise and issue the SAT documents accordingly.

6.5 SAFETY AT WORK

CROSSWIND site safety procedures shall form the basis for YOKOGAWA to conduct the SAT. Rosetti Marino/CROSSWIND shall provide necessary safety orientation to YOKOGAWA site team so that YOKOGAWA site engineers can follow the safety rules while working on-site.

6.6 TEST EQUIPMENT

Rosetti Marino/CROSSWIND will provide all test equipment (e.g. Digital Multimeter, Calibrator, Signal Generators, etc.) for the SAT.

7 WINDOWS DOMAIN ENVIRONMENT SAT PROCEDURES

7.1 DOCUMENT UPDATE AND CONFIGURATION VERIFICATION

Objective	To verify that FDS is up-to-date and is compliant with the actual configuration.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Check FDS used is the latest version and approved by EPC or End User. 2. Check that current Domain Controller configurations are compliant with FDS documents.
Criteria	1. The following is true; FDS is of the latest version

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

7.2 DOMAIN AND FOREST FUNCTIONAL LEVEL

Objective	To verify the Domain and Forest functional level.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. In the Domain controller, go to Start -> All Programs -> Administrative Tools -> Active Directory Domains and Trusts. 2. Right-click on the name of the domain -> click Properties. 3. Verify the Domain and Forest Functional Level.
Criteria	The result should show that the Domain and forest Functional level is Windows Server 2016

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

7.3 FORWARD LOOKUP AND REVERSE LOOKUP ZONE

Objective	To verify that DNS is installed on the domain controllers and the Forward and Reverse Lookup Zone is integrated to Active Directory.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Forward Lookup Zone 1. On the Domain controller, go to Start -> All Programs -> Administrative Tools -> DNS -> Forward Lookup Zone. 2. Right-click on the zone which is the name of the domain and select properties. 3. Repeat steps on the redundant domain controller 4. Also check whether dynamic updates are in secure only mode Reverse Lookup Zone 1. On Domain controller, go to Start -> All Programs -> Administrative Tools -> DNS -> Reverse Lookup Zone. 2. Right-click on the zone which is the name of the domain and select properties. 3. Click on the Reverse Lookup Zone>[IP].in-addr.arpa 4. Repeat steps on the redundant domain controller. 5. Also check whether dynamic updates are in secure only mode
Criteria	1. The zone, which is the name of the domain, should be present under Forward Lookup Zone. 2. The properties of the zone, which is the name of the domain, should show Active Directory-Integrated. 3. The properties of the zone, which is the name of the domain, should show that it is configured to replicate to all DNS servers in the same Active Directory domain. 4. Hostname and IP should match as mentioned in FDS 5. Verify that all IP subnets should show in-addr.arpa under Reverse Lookup Zones 6. Verify whether dynamic updates are in secure only mode

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

7.4 NAME RESOLUTION

Objective	To verify that hostnames can be resolved by the Active Directory DNS.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Open the command prompt on one of the domain controllers. 2. Type nslookup <LookupName/IP> <Nameserver/IP> 3. Type the name of the other domain controller. 4. Type the name of any other domain members. 5. Type in the IP address of the other domain controller. 6. Type the IP address of any other domain members.
Criteria	1. The nslookup should be able to resolve the name of the domain controller and other domain members to their correct IP addresses. 2. The nslookup should be able to resolve the IP address of the other domain controller and other domain members to its correct hostnames.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

7.5 ACTIVE DIRECTORY REPLICATION

Objective	To verify that replication can occur between 2 domain controllers.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. On domain controllers, go to Start -> All Programs -> Administrative Tools -> Active Directory Sites and Services. 2. Go to Default-First-Site-Name -> Servers 3. Expand the icon of the domain controller and select NTDS Settings. 4. On the right pane, right-click on the Automatically Generated connection -> Replicate Now. 5. Expand the icon of the redundant domain controller and select NTDS Settings. 6. On the right pane, right-click on the Automatically Generated connection -> Replicate Now.
Criteria	The dialog box "Active Directory has replicated the connections" should pop up when replication is successful.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

7.6 ACTIVE DIRECTORY REDUNDANCY

Objective	To verify that a user account can still log on to domain members if one of the domain controllers fails.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Shut down any one of the domain controllers. 2. Use a created account to log on to any of the domain members. 3. Log off the test account from the domain member. 4. Turn on the domain controller used in step 1.
Criteria	The test account should still be able to log on to the domain members.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

7.7 NAME RESOLUTION REDUNDANCY

Objective	To verify that hostnames and IP addresses can still be resolved even if one of the DNS fails.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Shut down any one of the domain controllers. 2. On any of the domain members, open a command prompt and run "ipconfig /flushdns" to clear any cached entries. 3. Type ping. 4. Type the Hostname of any other domain member. 5. Type ping. 6. Type the IP address of any other domain member. 7. Turn on the shut domain controller.
Criteria	The host names and IP addresses should be resolved if either of them fails.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

7.8 ORGANIZATIONAL UNIT AND GROUP STRUCTURE

Objective	To verify that the OU and group structure is according to the project requirement as defined in the FDS.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Open the Active Directory Users and Computers tool on one of the domain controllers. 2. Verify that the structure of the OU is as mentioned in the FDS. 3. Navigate to the OU containing groups. 4. Verify that the proper descriptions are given under each of the group properties. 5. Verify proper group nesting as per FDS. 6. Verify that specified users as per FDS are created in the system
Criteria	1. The OU structure should be the same as what mentioned in the FDS. 2. All Microsoft OS workstations and servers are part of the domain. 3. Description of group and group nesting should be as per FDS. 4. Make evidence that there are no temporary users in the system.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

7.9 VERIFY USER ACCOUNT COMPLIANCY, INCLUDING NON-REPUDIATION

Objective	Verification of user account compliance and non-repudiation.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	To verify that the current system user account and password are equal to the specification document, generic accounts are not created (default generic accounts are disabled). * Check: Login all account
Criteria	The current system user account and password tally with the specification document, no generic account is present.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

7.10 GROUP POLICY OBJECT STRUCTURE

Objective	To verify that the GPO structure is created according to the project requirement as defined in the FDS.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Open the Group Policy Management Console (GPMC) tool on the domain controllers. 2. Verify that the naming conventions of the GPOs are as per FDS. 3. Verify that the unneeded GPO configuration category (Computer configurations or User Configurations) is disabled. 4. Verify that the default GPOs (default Domain and Domain Controllers GPOs) are not linked to any OUs and be modified upon. 5. Verify that the GPOs are linked to the appropriate OUs in the OU structure.
Criteria	1. The naming convention of the GPOs should be as per the FDS. 2. Unneeded GPO configuration category should be disabled to allow faster GPO processing. 3. Default Domain and Domain Controllers GPOs should not be modified and assigned to any OUs. 4. All GPOs should be linked to the appropriate OUs as per FDS for correct IT environment hardening on domain members.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

8 YOKOGAWA ANTIVIRUS SOFTWARE SAT PROCEDURES

8.1 DOCUMENT UPDATE AND CONFIGURATION VERIFICATION

Objective	To verify that the FDS document is up-to-date and are compliant with the actual configuration.
Reference	• 1724000594-IN-RE-00043-Cyber Security Settings • 1724000594-IN-MAN-00037_R01
Procedure	1. Verify that the FDS used is the latest version and approved by EPC or End User. 2. Verify that the current anti-virus server and client configuration are compliant with FDS documents.
Criteria	1. The FDS is the latest version. 2. Anti-virus server and client configuration are compliant with the FDS document.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

8.2 VIRUS DEFINITION UPDATE

8.2.1 The Trellix ePO Server (DMZ) and source site Synchronization

Objective	To verify that the Trellix ePO Server (DMZ) can synchronize the virus definition update from the defined source sever(Crosswind)
Reference	• 1724000594-IN-RE-00043-Cyber Security Settings • 1724000594-IN-MAN-00037_R01
Procedure	Verifying virus definition download between Trellix ePO Server (DMZ) and Trellix ePO Server (Office Domain) 1. On the Trellix ePO Server (DMZ), launch the Trellix ePolicy Orchestrator Console. 2. Go to the Master Repositor and click the "Pull Now" button. 3. Select the AMCore Content Package for YOKOGAWA Antivirus Software Management under the Signatures and Engines of Package Types. 4. Click Next and run the Update.
Criteria	The AMCore Content Package of the Trellix ePO Server (DMZ) Master Repository shall be updated following the Trellix ePO Server source site server version.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

8.2.2 YOKOGAWA Antivirus Software Management Virus Definition Update

Objective	To verify that the YOKOGAWA Antivirus Software Management on the PIN and DMZ clients can download the virus definition update from the Trellix ePO Server (DMZ)
Reference	• 1724000594-IN-RE-00043-Cyber Security Settings • 1724000594-IN-MAN-00037_R01
Procedure	Verifying virus definition download between YOKOGAWA Antivirus Software Management PIN, DMZ clients and Trellix ePO Server (DMZ) 1. On the client, launch the YOKOGAWA Antivirus Software Console. 2. Open YOKOGAWA Antivirus Software Console. 3. Click the "Update Now" button. 4. Go to Server task menu in order to check whether updates are pushed to the systems
Criteria	The virus definition update on the PIN, DMZ client must be updated following the AV Server (DMZ) virus definition update version.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

8.3 YOKOGAWA ANTIVIRUS SOFTWARE MANAGEMENT

8.3.1 YOKOGAWA Antivirus Software Clients Communication

Objective	To verify that the YOKOGAWA Antivirus Software Management clients are reporting to the Trellix ePO Server (DMZ)
Reference	• 1724000594-IN-RE-00043-Cyber Security Settings • 1724000594-IN-MAN-00037_R01
Procedure	Verifying communication between YOKOGAWA Antivirus Software Management DMZ, PIN clients and Trellix ePO Server (DMZ) 1. On the Trellix ePO Server (DMZ), launch the ePolicy Orchestrator Console. 2. Go to the System Tree view. 3. Click the System Properties tab and select the target client, 4. Verify the "Last Communication" value.
Criteria	The last communication shows the client's last reporting scheduled date and time. The last communication value should show a recent date (approx. +/- 1 day) to confirm that the clients are communicating with the Trellix ePO server.

TEST RESULT: PASS / FAIL
Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

8.3.2 ePolicy Orchestrator Exclusion List

Objective	To verify that exclusion policy is configured in the AV Server
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Go to AV Server, and open the ePO console 2. Check the exclusion policy configuration.
Criteria	The current McAfee Product Version is tally with Project FDS.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

8.3.3 YOKOGAWA Antivirus Software Full Scan Impact

Objective	To verify that YOKOGAWA Antivirus Software Management Full Scan impact is at an acceptable level.
Reference	• 1724000594-IN-RE-00043-Cyber Security Settings • 1724000594-IN-MAN-00037_R01
Procedure	Verifying virus definition download between YOKOGAWA Antivirus Software Management of DMZ, PIN clients and Trellix ePO Server (DMZ) 1. On the DMZ & PIN client, launch the YOKOGAWA Antivirus Software Console. 2. Open YOKOGAWA Antivirus Software Console. 3. Click the "Scan System" button and run a "Full Scan". 4. Using the Windows inbuilt Performance monitor. 5. Check the Memory and CPU utilization.
Criteria	Confirm that the YOKOGAWA Antivirus Software Full scan impact is at an acceptable level following the FDS document.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

8.4 TRELLIX EPOLICY ORCHESTRATOR SERVER

8.4.1 Trellix ePO Server Policy Verification

Objective	To verify the YOKOGAWA Antivirus Software Policy is assigned to the YOKOGAWA System Group
Reference	• 1724000594-IN-RE-00043-Cyber Security Settings • 1724000594-IN-MAN-00037_R01
Procedure	Verifying the required YOKOGAWA Antivirus Software policy is assigned to the YOKOGAWA System Group 1. On the Trellix ePO Server (DMZ), launch the ePolicy Orchestrator Console. 2. Under the System Tree, click the YOKOGAWA System group. 3. Click the Assigned Policies tab and verify that the YOKOGAWA Advanced policy is applied.
Criteria	The YOKOGAWA Advanced policy is applied to the YOKOGAWA system group following the FDS document

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

9 YOKOGAWA APPLICATION WHITELISTING SAT PROCEDURES

9.1 DOCUMENT SPECIFICATION AND CONFIGURATION VERIFICATION

Objective	To verify that FDS is up-to-date and is compliant with the actual configuration.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Verify that the FDS used is the latest version and approved by EPC or End User. 2. Verify that the current application whitelisting configuration is compliant with FDS document.
Criteria	FDS is of the latest version.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

9.2 PROTECTION FROM EXECUTION OF UNMANAGED PROGRAM IN ENABLE MODE

Objective	To verify that the Whitelisting service can prohibit from execution of unmanaged programs during Enable Mode
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Verify to execute additional program 1. On the client machine, copy a test program/installer to the target machine's hard drive. (Ensure Solidcore status is enabled) 2. Execute the program. 3. Check the result
Criteria	The test program cannot execute

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

9.3 CHANGE OPERATION MODE OF WHITELISTING

9.3.1 Changing to Observe Mode and Enable Mode

Objective	To verify that the Whitelisting status changes to update mode
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Verify Whitelisting status mode changes to "Observe Mode" 1. Open the System Tree from the ePO management console and select the target machine from the System Tree. 2. Run a client task (YOKOGAWA Standard WL – Begin Update) on the selected station. 3. Once the agents apply the new policy, confirm that the systems have moved to observe mode. 4. Review the system's Solidcore status in the **ePO Console**. Verify Whitelisting status mode changes to "Enable Mode" 1. Open the System Tree from the ePO management console and select the target machine from the System Tree. 2. Run a client task (YOKOGAWA Standard WL – Begin Update) on the selected station. 3. Once the agents apply the new policy, confirm that the systems have moved to Enable mode. 4. Review the system's Solidcore status in the **ePO Console**.
Criteria	Verify if **Whitelisting Status** changes to Observe mode and Enable Mode

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

9.4 TRELLIX EPOLICY ORCHESTRATOR SERVER

9.4.1 Trellix ePO Server Policy Verification

Objective	To verify the YOKOGAWA Application Whitelisting policy is assigned to the YOKOGAWA System Group
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Verifying the required YOKOGAWA Application Whitelisting policy is assigned to the YOKOGAWA System Group 1. On the Trellix ePO Server, launch the ePolicy Orchestrator Console. 2. Under the System Tree, click the YOKOGAWA System Group
Criteria	The Standard YOKOGAWA policy is applied to the YOKOGAWA system group following the FDS.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

10 S PATCH MANAGEMENT SAT PROCEDURES

10.1 DOCUMENT UPDATE AND CONFIGURATION VERIFICATION

Objective	To verify that FDS is up-to-date and is compliant with the actual configuration.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Check FDS used is the latest version and approved by EPC or End User. 2. Check that current WSUS servers and client's configurations are compliant with FDS.
Criteria	1. FDS is of the latest version. 2. WSUS servers and client's configurations are compliant with FDS.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

10.2 OS PATCH MANAGEMENT SERVER

10.2.1 OS Patch Management Server Verification

Objective	To verify the WSUS server product version
Reference	• 1724000594-IN-RE-00043-Cyber Security Settings • 1724000594-IN-MAN-00037_R01
Procedure	WSUS Downstream Server Version Verification 1. On the WSUS server, click on Start and go to All Programs 2. Go to Administrative Tools and click on Windows Server Update Services. 3. Go to Help. 4. Click on the About Update Services 5. Look for the version number. WSUS Upstream Server Version Verification 1. On the WSUS server, click on Start and go to All Programs 2. Go to Administrative Tools and click on Windows Server Update Services. 3. Go to Help. 4. Click on the About Update Services 5. Look for the version number.
Criteria	The current WSUS server tallys with the project FDS.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

10.2.2OS Patch Management Server Configuration Verification

Objective	To verify the WSUS Server (DMZ) configuration
Reference	• 1724000594-IN-RE-00043-Cyber Security Settings • 1724000594-IN-MAN-00037_R01
Procedure	1. Log on to the AV/WSUS Server. 2. From Start menu navigate to All Programs > Administrative Tools and click on Windows Server Update Services. 3. Click on Options > Product and Classifications 4. Verify the configuration setup.
Criteria	The current WSUS server setup tallys with the project FDS.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

10.2.3 WSUS Synchronization Check

Objective	To verify that the WSUS servers are synchronized;
Reference	• 1724000594-IN-RE-00043-Cyber Security Settings • 1724000594-IN-MAN-00037_R01
Procedure	Login to the WSUS Upstream Server 1. Start the WSUS Administration Console. 2. From the Update Services menu, click on Synchronizations. 3. From Synchronizations, check that all scheduled synchronizations have been completed. Login to the WSUS Downstream Server 1. Start the WSUS Administration Console. 2. From the Update Services menu, click on Synchronizations. 3. From Synchronizations, check that all scheduled synchronizations have been completed.
Criteria	Automatic or manual synchronizations should be successful if the configuration has been done properly.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

10.3 OS PATCH MANAGEMENT CLIENT

10.3.1 Client Configuration

Objective	To verify that all clients have been configured properly and report back to the dedicated WSUS server.
Reference	• 1724000594-IN-RE-00043-Cyber Security Settings • 1724000594-IN-MAN-00037_R01
Procedure	Login to the WSUS Downstream Server 1. Start the WSUS Administration console. 2. Click on All Computers on the submenu of Computers. 3. From the list, verify that all clients have reported back to a WSUS Server based on the last maintenance window time. Login to the WSUS Upstream Server 1. Start the WSUS Administration console. 2. Click on All Computers on the submenu of Computers. 3. From the list, verify that all clients have reported back to the WSUS Server based on the last maintenance window time.
Criteria	The clients should report to WSUS servers based on project requirements.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

10.3.2 Patch Approval

Objective	To verify that the selected patch can be downloaded into clients and that clients are notified for installation.
Reference	• 1724000594-IN-RE-00043-Cyber Security Settings • 1724000594-IN-MAN-00037_R01
Procedure	1. From the approved YOKOGAWA Validation Report, Select one patch for approval to the client-server and client workstation. 2. From the Updates menu, search for the selected patch on the WSUS server. 3. Right-click on the selected patch and approve the groups that the client-server and client workstation are members of. 4. Login to the client server and client workstation. 5. Click on Start and Run, type CMD, and enter the command prompt window. 6. Type wuauclt.exe /detect now to force the client-server and client workstation to detect the approved patch. 7. Wait for the Windows Update Icon [Yellow Icon] to appear on the right-hand side of the taskbar. 8. Verify that the downloaded patch is the correct patch. 9. Install the downloaded patch onto the Client Server and Client Workstation. 10. Check from Add and Remove Software that the patch has been installed.
Criteria	The patch should be available and can be approved for installation onto selected clients.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

10.3.3 Installed Patch Verification

Objective	To verify that all recommended patches are installed on all clients.
Reference	• 1724000594-IN-RE-00043-Cyber Security Settings • 1724000594-IN-MAN-00037_R01
Procedure	1. From the approved YOKOGAWA Validation Report, list up all relevant patches whose recommended status is "Install". 2. Compare the above list with installed patches in all clients from the WSUS Administration Console or each client's control panel to verify that all the applicable patches are installed to the clients properly. 3. Create all installed patches list in all clients. Note: • If a new patch or not installed patch update is required while SAT is based on the site contract, a patch update list for each client should be created or updated and approved by the EPC or end user before installing the patches. • If the above new or not installed patch will require a reboot machine, confer with the EPC or end user about how to handle that patch before installing that patch.
Criteria	All recommended patches should be installed to all clients correctly.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

11 BRS (BACKUP RECOVERY SYSTEM)

11.1 DOCUMENT VERIFICATION

Objective	To verify that FDS document is up-to-date and is compliant with the actual configuration.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Check FDS used is the latest version 2. Check that the current BRS configuration is compliant with FDS document.
Criteria	FDS is of the latest version.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

11.2 BACKUP SOFTWARE VERSION VERIFICATION

Objective	To verify the backup software product version.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Open Veeam backup and replication console 2. Connect as local host. 3. Click on Help at the left top most corner>click on 'about'. 4. Verify the version
Criteria	The result should display Veeam backup software product & version.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

11.3 BACKUP AND RECOVERY SYSTEM - SCHEDULE BACKUP POLICIES

Objective	To verify that all the systems deployed with backup agent are covered under Backup Policies.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Launch the Veeam Backup console. 2. Verify the Image backup policies and their schedules as well as their retention rules.
Criteria	All the systems shall be covered under backup policies.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

11.4 BACKUP AND RECOVERY SYSTEM - IMAGE BACKUPS

Objective	Objective is to create image backup plans.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Select the desired machine in the list which you need to take the backup. 2. For full backup select the desired machine, right click and select active full. 3. For incremental backup select the desired machine, right click and select start button 4. The backup will be scheduled.
Criteria	System Image Backup plan created, and backup job completed.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

11.5 BACKUP AND RECOVERY SYSTEM - IMAGE RECOVERY

Objective	Objective is to recover a system from disaster.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Boot from the Veeam Recovery Media. 2. Select the network adapter & configure appropriate settings 3. Launch the Veeam Recovery Media wizard and click Bare Metal Recovery 4. Specify the backup file location. 5. Select the remote storage type. 6. Specify remote storage settings. 7. Select a backup. 8. Select a restore point. 9. Select the data restore mode. 10. Map the restored disks. 11. Resize the restored volumes. 12. Start the restore process.
Criteria	Bare Metal Recovery is successful.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

11.6 BACKUP AND RECOVERY SYSTEM - REPORT

Objective	To Verify the Report generation of the BRS.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Open the Veeam Backup & Replication console. 2. In the **Home** view, expand the **Jobs** node in the inventory pane and click **Applications Plug-ins**. 3. In the working area, select the necessary job and click **Report** on the ribbon. You can also right-click the job and select **Report**.
Criteria	The Report is Generated successfully.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

12 NETWORK MANAGEMENT SAT PROCEDURES

12.1 WUG SOFTWARE VERSION & LICENSE

Objective	To verify the Whatsup Gold product Version & License.
Reference	• 1724000594-IN-RE-00043-Cyber Security Settings • E366772C00-BOM_Rev.03
Procedure	1. Login to NMS Server using administrator privilege. 2. Run the 'WhatsUp Gold Admin Console' from desktop. 3. Click on 'Help' and select 'About Whatsup'. 4. Verify the followings. 5. License Type: WhatsUp Gold Total Plus 6. Version: 24.x.x
Criteria	The shown Whatsup Gold software version should match as per BOM.

TEST RESULT: PASS / FAIL
Remarks:

YOKOGAWA Representative : _____ Date: _____
Rosetti Marino Representative : _____ Date: _____
Crosswind Representative : _____ Date: _____

This document undergoes an issuance cycle within EDMS Fusionlive". Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

12.2 NMS LOG MANAGEMENT

Objective	To verify that the NMS Server is implemented with Log Management.
Reference	• 1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Verifying the NMS Server (PIN) is using Log Management. 7. Login to the host server where WhatsUp® Gold is hosted. 8. Go to Settings>Log management>Log Management Source setup and check that all devices and software are configured. 9. Go to ANALYZE>Log Management>Log Viewer or Log Management dashboard to verify the logs from the assigned device.
Criteria	1. Confirm that the NMS Server is implemented with a Log Management Feature. 2. Validate that unsuccessful login attempts are logged by the Log Management Feature. 3. Validate that all used devices and software send the logs to NMS Log Management.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

12.3 NETWORK STATUS

Objective	To verify network status alert will be captured by NMS.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Network Interconnection Test 1. Physically disconnect cables that are specified as monitoring targets. 2. Check if the Network icon on the System Architecture Network 3. Explorer window will change its color from Green to Red color. 4. Check the Web Alarm list of alerts. 5. Physically reconnect the cable. Check the Web Alarm if there is a list with a UP message or status, and the System Architecture screen will back to green color. 6. Repeat the above steps for all the target cables of respective monitoring targets specified in the FDS.
Criteria	NMS should be able to display the device interface; UP or DOWN, and its detailed information.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

12.4 RESOURCE MANAGEMENT AND UTILIZATION

Objective	To verify server resource management and utilization will be captured by NMS.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Monitoring the CPU/Memory/Hard Disk Utilization 1. Select DC01 on the Network Explorer right-click and select Device Status Report. 2. Open the task manager select the performance tab on the DC01 and confirm the CPU and memory usage. 3. Open Windows Explorer on DC01 and confirm the HDD usage. 4. Confirm the CPU/Memory/Hard Disk usage shown in the Device Status Report under Performance Monitor. 5. Repeat the above steps for all the target servers respectively which are specified in the FDS.
Criteria	NMS should be able to display the server's CPU, Memory, and Hard Disk usage on the NMS Device Status Window – Utilization Window.

TEST RESULT: PASS / FAIL
Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

12.5 NETWORK DEVICE RESOURCE MANAGEMENT AND UTILIZATION

Objective	To verify network device resource management and utilization captured by NMS.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Monitoring the CPU/Memory/Port Interface Utilization 1. Select any network device on the Network Explorer, right-click on the device icon, and select Device Status Report 2. Confirm the CPU/memory/port interface usage shown in the Device Status Report under Performance Monitor. 3. Repeat the above steps for all the target network devices respectively which are specified in the FDS.
Criteria	NMS should be able to display the network device's CPU, Memory, and Port Interface usage on the NMS Device Status Window – Utilization Window.

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

12.6 WUG CONFIGURATION BACKUP TEST

Objective	To verify that WUG server backup is preforming successfully
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Login to NMS Server using administrator privilege. 2. Run the 'WhatsUp Gold Admin Console' from desktop 3. Click on Tools>Database Utility>Backup WhatsUp SQL Database 4. Mention the name and location to save backup file.
Criteria	Verify if the backup is done successfully. Message will be displayed regarding successful backup.

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

12.7 WUG CONFIGURATION RESTORE TEST

Objective	To verify that WUG server restores successfully from backup.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Login to NMS Server using administrator privilege. 2. Run the 'WhatsUp Gold Admin Console' from desktop 3. Click on Tools>Database Utility>Restore WhatsUp SQL Database 4. Mention the name and location of the database file to be restore.
Criteria	Verify if the restore is done successfully. Message will be displayed regarding successful restore.

TEST RESULT: PASS / FAIL
Remarks:

YOKOGAWA Representative : _____ Date: _____
Rosetti Marino Representative : _____ Date: _____
Crosswind Representative : _____ Date: _____

12.8 NETWORK SCAN TO DISCOVER SYSTEMS

Objective	To verify the network is not connected with unnecessary network devices or computers.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Network Scan 1. Before starting the network scan, obtain the approval of the NMS network scan function from the EPC or END User. The approval should include the possible impact caused by network scan such as network delay or application delay. 2. Select "Discover Devices" from File in the toolbar. Set the proper IP address range. Click "Start a discovery session". 3. Check all existing devices are shown and any newly discovered devices in the Devices Discovered Window. 4. If there is a newly discovered device, MAC should verify the reason.
Criteria	The network should not have unnecessary devices.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

13 NETWORK INFRASTRUCTURE SAT PROCEDURES

13.1 DOCUMENT UPDATE AND CONFIGURATION VERIFICATION

Objective	To verify that Network FDS is up-to-date and is compliant with the actual configuration.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Check FDS used is the latest version and approved by EPC or End User.
Criteria	FDS is of the latest version.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

13.2 NETWORK ARCHITECTURE VERIFICATION

Objective	To verify the network architecture is implemented according to Network FDS (as per SL requirements)
Reference	• 1724000594-IN-RE-00043-Cyber Security Settings • 1724000594-IN-DD-00015_System Architecture_Native_R4
Procedure	1. Check if the Network implementation matches the design. 2. Check if the Safety Zone is separated from the DCS zone with VLANs and Firewalls.
Criteria	Network implementation is matching the approved design architecture from Network FDS

TEST RESULT: PASS / FAIL
Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

13.3 LOGIN BANNER VERIFICATION

Objective	To verify that Network devices and components are configured with a Login Banner
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Login at all network devices and components: Switches, Workstations, Servers, 2. After login, a banner with disclaimer information about unauthorized access and its consequences.
Criteria	All network devices and components are configured to display a Login Banner.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

13.4 VLANS

Objective	To verify that VLANs are implemented according to Cyber Security Settings FDS specifications.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. From Network FDS VLANs properties, test one VLAN implementation at a time. For each VLAN, check that the IP addresses of all devices connected to the respective VLAN are part of the Network IPs defined in the table. 2. Check IP Address in the Firewalls, Switches, Workstations, Servers, Printers, and Time Synchronization GPS Clock.
Criteria	1. The network devices are assigned to the proper VLAN based on Network Segmentation specifications. 2. All network devices and components (Firewalls, Switches, Workstations, Servers, Printers, and Time Synchronization GPS Clock) have an assigned IP address for communication and/or management purposes.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

13.5 UN-USED PORTS MANAGEMENT

13.5.1 Physical Locks at network devices/components

Objective	Check all unused ports are restricted from physical access.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Check all un-used Ethernet ports, SFP ports, and USB ports from Firewalls, Switches, Workstations, Servers, Printers, and Time Synchronization GPS Clock are blocked with a dedicated physical lock (RJ45 lock, Fiber Optic lock, USB lock).
Criteria	All unused Ethernet ports, SFP ports, and USB ports are blocked accordingly.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

13.5.2 Disabling unused ports

Objective	Check all unused ports are restricted from logical access.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Login to all Firewalls, Switches, Workstations, Servers, Printers, and Time Synchronization GPS Clock. Check that all unused Ethernet ports, SFP ports, and USB ports are disabled from the software configuration.
Criteria	All unused Ethernet ports, SFP ports, and USB ports are disabled accordingly.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

13.6 SWITCH REDUNDANCY

13.6.1 Turning off one of the Redundant Pair Network Switch and check the Network Connectivity

Objective	Turn of the any one switch in the Network which is Redundant
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Ping the Any End Devices in the Redundant Network continuously. 2. Turn off the Power supply for any one of the Switch in the Redundant pair. 3. Check for Continuous Network Connectivity and Ping. (1-4 ICMP Packet Drop may be observed) 4. Turn on the Testing Device of the Redundant Pair of the Network Switch. 5. Repeat the test for the other Network Device Note: Applicable Switches are PINSWL2-001, PINSWL2-002, PINSWL2-003, PINSWL2-004, PINSWL2-005, PINSWL2-006, MODSWL2-001, MODSWL2-002, IECSWL2-001. IECSWL2-002, COMSWL2-001, COMSWL2-002, CNSWL2-001, CNSWL2-002, SNSWL2-003, SNSWL2-004, SERVSWL2-001, SERVSWL2-002, SERVSWL2-003, SERVSWL2-004
Criteria	Continuous Ping of the end device is Observed with little to no Packet drop

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

14 FIREWALL SAT PROCEDURES

14.1 DOCUMENT UPDATE AND CONFIGURATION VERIFICATION

Objective	To verify that FDS document is up-to-date and are compliant with the actual configuration.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Check FDS is the latest version and approved by EPC or End User. 2. Check that the current firewall configuration is compliant with FDS.
Criteria	1. FDS is the latest version. 2. Firewall configuration is compliant with FDS document.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

14.2 DEFAULT POLICY CONFIGURATION DENY ALL - ALLOW BY EXCEPTION

Objective	To verify that deny all - Allow by exception is applied on firewalls.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	L3.5 Firewall 1. Login in L3.5 Firewall with an administrative account. 2. Checking "deny all" policy is present and active at the bottom of the policies configuration list. 3. Check firewall policies (allowed by exception) are configured above the default "deny all" policy in the configuration list. Vnet/IP Firewalls 1. Login in Vnet/IP Firewalls with administrative account 2. Checking "deny all" policy is present and active at the bottom of the policies configuration list. 3. Check firewall policies (allowed by exception) are configured above the default "deny all" policy in the configuration list.
Criteria	1. The L3.5 Firewall is configured with deny all - allow by exception policies. 2. The Vnet/IP Firewalls are configured with deny all - allow by exception policies.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

14.3 FIREWALL "OBJECTS" CONFIGURATION

Objective	To verify that the firewall objects (devices: workstations, servers, other network components with an IP address) are properly configured.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	L3.5 Firewall 1. Login in the L3.5 Firewall with an administrative account. 2. Navigate to Configuration -> Firewall -> Objects. 3. Check Objects configuration is implemented as per design documentation, with hostname and following IP Addressing scheme and Network Architecture. Vnet/IP Firewalls 1. Login in Vnet/IP Firewalls with an administrative account. 2. Navigate to Policy & Objects -> Addresses. 3. Check Objects configuration is implemented as per design documentation, with hostname and following IP Addressing scheme and Network Architecture.
Criteria	1. The L3.5 Firewall objects (devices) are configured according to design documents. 2. The Vnet/IP firewall objects (devices) are configured according to design documents.

TEST RESULT: PASS / FAIL
Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

14.4 FIREWALL NETWORK SEGMENTATION

Objective	To verify that the firewall is configured using the Network segmentation agreed design.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	L3.5 Firewall 1. Login in the L3.5 Firewall with an administrative account. 2. Check interfaces and VLANs configuration is implemented as per design documentation, following IP Addressing scheme and Network Architecture. Vnet/IP Firewalls 1. Login into Vnet/IP Firewalls with administrative account 2. Check interfaces and VLANs configuration is implemented as per design documentation, following IP Addressing scheme and Network Architecture.
Criteria	1. The L3.5 Firewall interfaces and Vlans are configured according to design documents. 2. The Vnet/IP firewall interfaces and Vlans are configured according to design documents.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

14.5 FIREWALL "FAIL CLOSE"

Objective	To verify that after the shutdown of Vnet/IP firewalls, the Safety systems will continue to safeguard the plant.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Vnet/IP Firewalls 1. Shutdown Vnet/IP Firewalls. 2. Check that the Safety System shall not move to Emergency Shutdown mode, due to lost communication with DCS, as per IACS Engineering design function.
Criteria	Safety System shall continue to function without moving to Shutdown mode if DCS communication is lost at Vnet/IP Level.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

14.6 FIREWALL LOGIN BANNER VERIFICATION

Objective	To verify that Firewalls are configured with a Login Banner
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Using NMS station, login to all firewalls. 2. After login, a banner with disclaimer information about unauthorized access and its consequences.
Criteria	All firewalls are configured to display a Login Banner.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

14.7 FIREWALL REDUNDANCY

14.7.1 Shut down any one of the firewall pairs to check the network redundancy.

Objective	Shut down any one firewall in the firewall pair which hosting the Redundant connections
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	1. Ping any end devices in the **Redundant Network** continuously. 2. Turn off the power supply for any one of the firewalls. 3. Check for Continuous Network Connectivity and Ping. (1-4 ICMP Packet Drop may be observed) 4. Turn on the Testing Device. 5. Repeat the test for the other firewall. Note: **Applicable to all the firewalls supplied by Yokogawa.**
Criteria	Continuous Ping of the end device is Observed with little to no Packet drop

TEST RESULT: PASS / FAIL

Remarks:

15 SWITCH SAT PROCEDURES

15.1 DOCUMENT SPECIFICATION AND CONFIGURATION VERIFICATION

Objective	To verify that FDS document is up-to-date and is compliant with the actual configuration.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Check FDS used is the latest version and approved by EPC or End User.
Criteria	FDS is of the latest version.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____

15.2 SWITCH CONFIGURATION

Objective	To efficiently direct and manage data traffic between devices within a network, ensuring secure, reliable, and optimized communication by forwarding data to the correct destinations based on MAC addresses.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Check that the current switch configuration is compliant with the FDS document. 1. Confirm Switches are in managed state. 2. Confirm Hostnames are defined. 3. Confirm VLAN are configured as per IP addressing scheme. 4. Confirm Interface description is defined. 5. Confirm Switch ports are allocated as per the port allocation plan. 6. Confirm Switch ports access mode is configured. 7. Confirm network monitoring is enabled.
Criteria	Confirm that all the switch functions are compiled as per FDS

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative	:	Date:	
Rosetti Marino Representative	:	Date:	
Crosswind Representative	:	Date:	

16 REMOTE ACCESS FACILITY SAT PROCEDURES

16.1 DOCUMENT SPECIFICATION AND CONFIGURATION VERIFICATION

Objective	To verify that FDS document is up-to-date and is compliant with the actual configuration.
Reference	1724000594-IN-RE-00043-Cyber Security Settings
Procedure	Check FDS used is the latest version and approved by EPC or End User.
Criteria	FDS is of the latest version.

TEST RESULT: PASS / FAIL

Remarks:

YOKOGAWA Representative : _____ Date: _____

Rosetti Marino Representative : _____ Date: _____

Crosswind Representative : _____ Date: _____