FUJ00080805

Document Title: Local Security Audit Report - Networks - 2009

Audit Result Status Amber
See section 1.1

Document Reference: LOC/PBU/RMG/SCY/0017

Document Type: Security Document, Report

Release: Not Applicable

Abstract: Audit mainly to ISO 27001 sections A.10.6, A11.4 and A.12.3

Document Status: APPROVED

Author & Dept: Nigel Hatcher, RMGA Quality Manager

External Distribution: To be summarised in the Corporate Assessment Database [CAD] **Irrelevant** **Irrelevant** with a copy of the Approved report being sent to Group Quality for storage and linking to from the CAD.

Security Risk Assessment Confirmed YES. See section 0.10, Security Risk Assessment.

Approval Authorities:

Name	Role	Signature	Date
Nigel Hatcher	RMGA Quality Manager		

Note: The Reviewers/Approvers Role Matrices (PGM/DCM/ION/0001) & (CM/ION/078) do not include this type of document.

FUJ00080805

0 Document Control

0.1 Table of Contents

FUJ00080805

Figures (Sketches) and Tables

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
V0.1 Nigel Hatcher	28-Jul-2009	Initial drafting from local quality audit template. Insertion of draft notes on Document Reviews and Interviews. Individual forms populated. Circulated to Ian Mills and Mark Jarosz for comments on interview notes.	N/A
V0.2 Nigel Hatcher	31-Jul-2009	Corrections to v0.1. Interview notes consolidated to only Observation areas (see v0.1 for 'dump' of interview notes).	N/A
V1.0 Nigel Hatcher	18-Aug-2009	Raised to Approved following nil return of comments	N/A

0.3 Review Details

Review Comments by :	V0.2 by 14-Aug-2009
Review Comments to :	nigel.hatcher GRO
Mandatory Review	
Role	Name
RMGA Quality Manager (if not the author)	
Optional Review	
Role	Name
Business Assurance Security Consultant (Auditor)	John Wright
RMGA Technical Security Consultant (Auditor)	Bill Membery
Penetration Testers	Jeff Pridmore Mark Havard
RMGA Operations Director (or Nominee)	~~Wendy Warham~~ Dave Keeling
RMGA CISO	Howard Pritchard
RMGA Security Information Governance	Brian Pinder and Neneh Lowther

FUJ00080805

RMGA Security – Project Manager	Marion Chave-Jones
Interviewees (or remote contacts)	----------
RMGA Operational Security Manager	Peter Sewell
RMGA Operational Security	Andy Dunks
RMGA SDM for Networks	Ian Mills
HNG-X Networks Design, Development & Implementation Project Management	Steve Ashlin – Project Manager Chris Credland - Project Leader
HNG-X – Lead Network Architect	Mark Jarosz
RMGA SSC	Steve Parker
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name

(*) = Reviewers that returned comments

0.4 Associated Documents (General & to Template)

[Ref] & Doc Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)			RMGA HNG-X Generic Document Template	Dimensions
[ADUG] Q&CS/ADB/001	**	**	Fujitsu (UK & Ireland) Assessment Database Users Guide. (can be accessed via [CAD] Irrelevant Irrelevant "Database Information")	Café-vik
[CAD]	n/a	-------	(Corporate) Assessment Database Irrelevant Irrelevant	Café-vik
[CARP] I-AB1.5 *author: Alan Clapson*	1.2	01/06/07	(Corporate) Assess & Review BMS Process (can be accessed via 'Quality Portal' Irrelevant Irrelevant ""Policies and Processes")	Café-vik
[CART] none apparent *author: Alan Clapson?*	None	Jun 2007	(Corporate) Assessment Report Template (Word Format) (can be accessed via 'Quality Portal' Irrelevant Irrelevant "Assessment Database…"	Café-vik
[IAS] PGM/PAS/PLA/0014	**	As version	RMGA - Integrated Audit Schedule	Dimensions

FUJ00080805

[SCQA] none apparent *author: Alan McFall?*	2.0	28 10 05	(Corporate) guide 'Standard for Conducting Quality Audits' (can be accessed via 'Quality Portal' Irrelevant Irrelevant "Policies and Processes")	Café-vik
[TLQAR] PGM/PAS/TEM/0004 (Do Not Remove)			Local Quality Audit Report template	Dimensions & RMGA Portal

***** Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.***

0.5 Associated Documents (specific to audit)

[Ref] & Doc Reference	Version	Date	Title	Source
ISO 27001 : 2005		© 18-Oct-2005	Information security management systems — Requirements	IT Security on Café-vik
[QUE] none		27-Mar-2008?	ISO, ISO/IEC 27001 audit guidance.	ISO
[LSAP] SVM/SEC/PLA/0014	1.0 to 1.2		Local Security Audits Plan - 2009	Dimensions
SVM/SEC/POL/0003	V4.0	12-Feb-2009	RMGA Information Security Policy	Dimensions & RMGA Portal
SVM/SDM/PRO/0018 - Appendix A	V2.2	14-Apr-2009	RMGA Customer Service Incident Management Process Details - Security Incident Reporting	Dimensions
SVM/SDM/SD/0012			Central Network Service Description	Dimensions
DES/NET/HLD/0016	V2.0	07-Oct-2008	Network Security High Level Design	Dimensions
[HTNA] ARC/NET/ARC/0001	V0.7	29-Jan-2009 onwards?	HNG-X Technical Network Architecture	Dimensions
ARC/SEC/ARC/0003			HNG-X Technical Security Architecture	Dimensions
Various			Various others – mentioned in text	

***** Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.***

0.6 Abbreviations

FUJ00080805

Abbreviation	Definition
[aaaa]	See "Associated Documents" section
BMS	Business Management System
CCD	Contract Controlled Document
HLD	High Level Design
HNG-X	Horizon Next Generation – project X
ISO	International Organization for Standardization
LLD	Low Level Design
OOH	Out Of Hours
RAG	Red Amber Green
RMGA	Royal Mail Group Account
SRS	System Requirements Specifications

0.7 Glossary

Term	Definition

0.8 Changes Expected

Changes
Corrections after review

0.9 Accuracy

This document is not a Contract Controlled Document (CCD).

Fujitsu (UK & Ireland) endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.10 Security Risk Assessment

Security risks have been assessed and it is considered that there are no security risks relating specifically to this document.

FUJ00080805

1 Introduction

This Local Security Audit Report presents the outcome of a planned audit of Networks and Cryptographic Controls to ISO 27001 in the RMGA and considered:

a) The compliance of those functions with the Fujitsu (UK & Ireland) Business Management System (BMS) and Security Policies and RMGA Policies and Procedures;
b) The compliance of those functions with relevant aspects of the ISO 27001:2005 standard;
c) Any areas suitable for promotion as good business practice across the RMGA Account and/or Fujitsu (UK & Ireland).

However 'trails' led the auditors to a number of other areas of the standard.

The work was conducted using the principles and process defined in the Corporate Assessment Process [ref CARP] and the guide Standard for Conducting Quality Audits [ref SCQA] with reference to the questions set out in ISO, ISO/IEC 27001 [ref QUE] audit guidance .

The audit was identified in the Integrated Audit Schedule [ref IAS] V9.0 as being scheduled to have been conducted in July 2009 and more detailed planning was set out in Local Security Audits Plan – 2009 [ref LSAP] V1.0.

1.1 Audit Result Status guidance

A Red Amber Green (RAG) indication in the 'Audits Results Status' field on the report's front sheet takes one of the following values:

Red - Urgent Corrective Action is required because Audit results indicate at least one risk has been identified which will have a serious impact upon Account/Programme/Project deliverables or on the integrity of possible ISO 27001 registration.

Amber - Corrective Action is required because audit results indicate that a risk has been identified which will impact upon Account/Programme/Project deliverables or which is a non-conformance against ISO 27001.

Green - The audit has not identified any risks and no action is required.

2 Scope and Conduct of Audit

The scope and objectives of the audit were to examine RMGA Security of Networks in regard to the requirements of ISO 27001 : 2005.

The audit was conducted by
Nigel Hatcher (NH) – RMGA Quality Manager mainly during the period 6th to 17th July 2009.
with the assistance of:
John Wright (JW) - Business Assurance Consultant at BRA01 on 15th July 2009:
Bill Membery (BM) - RMGA Technical Security Consultant at IRE11 on 17th July 2009

9 members of the RMGA team were interviewed or contacted as part of the audit:

FUJ00080805

Andy Dunks – Security Team by email 2nd July with reply received on 16th July;
Ian Mills – RMGA Networks Service Delivery Manager (SDM) on 7th & 15th July;
Steve Parker – RMGA SSC by email on 9th July;
Peter Sewell – RMGA Operational Security Manager by email on 9th July;
Steve Ashlin – Project Manager)
Chris Credland - Project Leader) Networks Design, Development & Implementation on 15th July;
Howard Pritchard – CISO 15th July;
Mark Jarosz – Lead Network Architect on 16th July;
and
in addition the independent auditor, John Wright, interviewed Nigel Hatcher – RMGA Quality Manager.

Documents listed in Section 0.5 - "Associated Documents (specific to audit)" were used or viewed.

Any "Observations" raised are categorised as Non-conformities and Formal Observations in the forms in Annex B.

Corrective action plans co-ordinated by the RMGA Security Team are required for all Non-conformities and Formal Observations raised and should be recorded within the Corporate Assessment Database [CAD].

Note: The assessment was based on random samples and therefore nonconformities may exist which have not been identified.

3 Management Summary

This Local Security Audit Report presents the outcome of an audit of security of Networks, mainly to ISO 27001 sections Annex A.10.6, A.11.4 and A.12.3, in the RMGA although 'trials' led the auditors to rasie observations in other areas of the standard.
7 Formal Observations were raised and therefore Corrective Actions (plans) are required to be co-ordinated by the RMGA Security Team.

4 Results Summary

Major Non-Conformances	- none
Minor Non-Conformances	- none
Formal Observations	- 7

Summary of Formal Observations:

1) *Ob1)* To ISO 27001 - A.10.6.1: Little evidence could be found that regular 'sweeps' for detecting un-authorised Bluetooth or wireless connections, as required by the RMGA Security Policy section 10.6.1, have been planned, suitable equipment obtained, scans carried out, investigated and records kept.

2) *Ob2)* To ISO 27001 - A.11.4.1: The Out of Hours (OOH) password changing process (RS/PRO/047) will no longer be necessary as access for support will be via the iKey authentication. So that document will not be taken forward.
Preparation needs to be made:
a) to be ready to mark it Withdrawn in PVCS;
b) amend the reference in the Security Policy.

FUJ00080805

3) *Ob3)* To ISO 27001 – 4.3.3 (Records) & A.11.4.3: No record was found that automatic equipment detection had been considered.

4) *Ob4)* To ISO 27001 – 4.3.2 (Control of Documents): The document "Network Security High Level Design" (DES/NET/HLD/0016) appears to have been started before the RMGA Security Policy (SDM/SEC/POL/0003) was written and hence in its Section 4.1.1 talks of a Security Policy that has no reflection on the policy document.
One or other of the two documents needs to be amended to clarify this.

5) *Ob5)* To ISO 27001 – 4.3.2 (Control of Documents - Review): The "RMGA HNG-X Document Reviewers / Approvers Role Matrix" (PGM/DCM/IOM/0001) was checked at times during the audit to clarify if Security was being asked to review documents It became apparent that they (CSPOA.security **Irrelevant**) are not on the 'listing' for Low Level Designs, which it was considered by the auditor that they should at least be amongst Optional Reviewers. And hence should be requested to be added to the Matrix.

6) *Ob6)* To ISO 27001 4.2.1 d) 1) (Identify Assets) & A.7.1.2 (Ownership of Assets): It was noted that Limited secure ID log in is authorised by the Networks SDM to Cable & Wireless by email. This is Ownership of an Asset and should be recorded.

7) *Ob7)* To ISO 27001 0.2 a) (Understanding Security Requirements) It is possible that the 'detail' of ISO 27001 may not have been fully addressed in Requirement capture, rather just an entry about being compliant. This needs to be clarified.

The audit results status is therefore considered to be:

Amber - Corrective Action is required by the RMGA Security Management Team because audit results indicate that a risk has been identified which will impact upon Account/Programme/Project deliverables or which is a non-conformance against ISO 27001.

Therefore Corrective action plans, co-ordinated by the RMGA Security Team, from the various RMGA staff /teams are required for all Formal Observations raised.

5 Audit Notes and Findings

The criteria that the auditors kept in mind, whilst conducting the audit, is set out in Annex A.

5.1 Document Reviews

As preparation for and follow up to interviews a number of document were reviewed.

5.1.1 RMGA Security Policy

Parts of the "RMGA Security Policy" (SVM/SEC/POL/0003) are set out to mirror the requirements of ISO 27001 : 2005 Annex A.

10.6 (A.10.6) covers Network Security Management:
Within 10.6.1 the policy states that:
Regular sweeps must be carried out within the Data Centres and Support Centres to detect Wireless and Bluetooth devices connected to HNG-X and the results documented.

FUJ00080805

But during the period of the audit that could not be confirmed as being in place.
Formal Observation *Ob1)* raised.

11.4 (A.11.4) covers Network Access Controls:
Within 11.4.1 there is reference to an Out of Hours password changing process (RS/PRO/047). When that was viewed it was discovered to have a classification that is no longer supported at Corporate level. Andy Dunks the last author of the Out of Hours (OOH) password changing process (RS/PRO/047) was contacted by email regarding the classification of the document. He replied that this process for OOH support will no longer be necessary as access for support will be via the iKey authentication.
So this document will not be taken forward. Therefore reference to it in the Security Policy needs to be amended. Formal Observation *Ob2)* raised.

Within Section 11.4.3 of the policy it has the opened ended statement:
Automatic equipment identification will be considered as a means to authenticate connections from all locations and equipment within the RMGA.
But during the period of the audit no record of if this having been done and recorded could be found.
Formal Observation *Ob3)* to ISO 27001 - 4.3.3 (Records) & A.11.4.3 raised.

12.3 (A.12.3) covers Cryptographic Controls:
Within 12.3.1 a policy for cryptographic controls is set out.
Within 12.3.2 it set out how Key Management will be implemented.

5.1.2 RMGA Customer Service Incident Management Process Details.

The document "RMGA Customer Service Incident Management Process Details" (SVM/SDM/PRO/0008) Appendix A sets out how Security Incident Reporting should be conducted.

5.1.3 HNG-X Technical Network Architecture

The document "HNG-X Technical Network Architecture" (ARC/NET/ARC/0001), which is at present 150 pages long, was viewed on line, mainly during the interview with Mark Jarosz (see Architects for Networks section).

5.1.4 Network Security High Level Design

The document "Network Security High Level Design" (DES/NET/HLD/0016) provides a High Level overview of the network security components and appliances and positioning required to secure the HNG-X solution. It is a derivative of the parent documents found within Dimensions, namely HNG-X Technical Network Architecture ARC/NET/ARC/0001 (150 pages) and HNG-X Technical Security Architecture ARC/SEC/ARC/0003.

This was scanned to see if Automatic Equipment Identification was considered. Nothing was found on the subject. See Formal Observation *Ob3).*

This document was started before the RMGA Security Policy (SDM/SEC/POL/0003) and hence in its Section 4.1.1 talks of a Security Policy that has no reflection on the policy document. One or other of the two documents needs to be amended to clarify this. Formal Observation *Ob4)* raised.

5.1.5 HNG-X Reviewers and Approvers Roles Matrix

This document "RMGA HNG-X Document Reviewers / Approvers Role Matrix" (PGM/DCM/IOM/0001) was checked at times during the audit to clarify if Security was being asked to review documents.

FUJ00080805

It became apparent that they (CSPOA.security GRO) are not on the 'listing' for Low Level Designs (LLD), which it was considered by the auditor that they should at least be amongst Optional Reviewers. And hence should be requested to be added to the Matrix.
Auditor's Notes:
a) For all documents to review, the use of the joint email security team mailbox should be re-enforced (awareness cascade) as some documents viewed were being addressed to particular members of the security team only and hence might not get reviewed properly.
b) A request should be made to amend the Matrix to list Peter Sewell as the Operational Security Manager and not just Security.
Formal Observation *Ob5)* raised.

5.2 Interviews

During the allotted timeframe of the audit a number of interviews (see Scope and Objectives section) were conducted, either face to face or by email correspondence, to check that documented policy and processes (procedures, guidelines) were being followed.

Only the points relevant to Observations are recorded.

5.2.1 SDM for Networks

RMGA Security Policy section 10.6.1: Networks monitored for breaches by protection from Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).
SDM for Networks, Ian Mills had no information as to whether 'Sweeps' for Bluetooth and wireless connections are being conducted as is stated in the Security Policy. Add to Formal Observation *Ob1*)

ISO 27001, A.11.4.3
Has automatic terminal identification been considered?
The SDM had no knowledge if this had/was being done. (see *Ob3)*)

Limited secure ID log in is authorised by Ian to C&W by email
(this is Ownership of an Asset re A.7.1.2). Formal Observation *Ob6)* raised

5.2.2 Chief Information Security Officer (CISO)

Howard Pritchard – CISO was briefly interviewed by JW on 15th July.
The main topics covered were the handling of Assets and Risks.

A further point about Requirements was followed up via email by NH on the 21st July, that it had became apparent to the auditor that information on the requirements of the ISO 27001 "Control" areas may not have filtered down to staff that might need to consider them.
The 'detail' of ISO 27001 may not have been fully addressed in Requirement capture, rather just an entry about being compliant.
The CISO replied that it had been requested earlier in the year, but after going through all the documentation online, it appears that nothing has happened. Although updates are received from the Requirements Team. Formal Observation *Ob7)* raised.

5.2.3 Operational Security

Andy Dunks the last author of the Out of Hours (OOH) password changing process (RS/PRO/047) was contacted by email regarding the classification of the document. He replied that this process for OOH support will no longer be necessary as access for support will be via the iKey authentication.

FUJ00080805

So this document will not be taken forward. See Formal Observation No. *Ob2)*

Peter Sewell - Operational Security Manager was contacted via email regarding sweeps for un-authorised Bluetooth and Wireless connections.
His reply was: "As yet I am not aware of any organised 'sweeping' taking place, and I don't think we currently hold a meter, but almost any laptop can actually provide this facility. Need to check with the Data Centre as this will need to be carried out on a regular basis for HNGX."
Added to Formal Observation *Ob1)*

5.2.4 Software Support Centre

Steve Parker of the SSC on the secure floor at BRA01 was contacted by email to see if the 'requirement' for sweeps for un-authorised Bluetooth and/or wireless connections was being carried out there.

Steve reported back that it wasn't to his knowledge and asked how should it be done.

Added to Formal Observation No. *Ob1)*

5.2.5 Project Managers for Networks Design & Development.

Steve Ashlin (SA) – Project Manager
and Chris Credland (CC) – Project Leader

No Observation have been recorded from interviews

5.2.6 Architects for Networks

Mark Jarosz – Lead Network Architect

Referring to the document "HNG-X Technical Network Architecture" [HTNA] (ARC/NET/ARC/0001), 150 pages, on line Mark explained the main sections that effect security related items.
It was noted that Bill Membery is listed as a Mandatory Reviewer rather than it being directed to the CSPOA.security GRO mail box.
Add as Notes to Formal Observation No. *Ob5)*

A.11.4.3: Has automatic terminal identification been considered?
This is covered by the document HNG-X Branch Router Topic Architecture (ARC/NET/ARC/0003).
Add as Notes to Formal Observation No. *Ob2)*

5.3 Visit to Data Centre

5.3.1 Sweeping for unauthorised connections

Whilst Bill Membery was at the Irish Data Centre IRE11, Jeff Pridmore – Penetration Tester undertook a Wireless scan using the tools within Backtrack on a Linux platform nothing internal was detected but whilst walking around externally quite a few full signals were detected none of which were connected to 'target' equipment. Mark Havard – Penetration Tester is producing a report,
Information added as Notes to Formal Observation *Ob1).*

FUJ00080805

A. Annex – Additional Information

A.1. ISO 27001 - Criteria

The wording throughout ISO 27001 : 2005 was used as guidance for question especially paragraphs A.10.6, A.11.4 and A.12.3
Also used were the suggestions for Audit Criteria from the ISO/IEC 27001 Audit Guidance [ref QUE]:

FUJ00080805

B. Annex – Individual "Observation" Forms

B.1. LOC/PBU/RMG/SCY/017 Sequence No. 1 "Ob1)"

Irrelevant

Raised Date	28 Jul 09	**Category**	Observation	**Standard**	ISO 27001-A.10.6.1
Unit	PSD – RRMT - RMGA	**Location**	Various	**Country**	United Kingdom
Division / Community	UK Private Sector	**Interviewee**	Various	**Interviewee's Role**	various
Area Contact	Nigel Hatcher / Nench Lowther	**Assessor**	Nigel Hatcher	**Process** Corporate / Local	Manage Security / Security Policy

Observation details
Little evidence could be found that regular 'sweeps' for detecting un-authorised Bluetooth or wireless connections, as required by the RMGA Security Policy section 10.6.1, have been planned, suitable equipment obtained, scans carried out, investigated and records kept.

Notes
Whilst Bill Membery was at the Irish Data Centre IRE11, Jeff Pridmore – Penetration Tester undertook a Wireless scan using the tools within Backtrack on a Linux platform nothing internal was detected but whilst walking around externally quite a few full signals were detected none of which were connected to 'target' equipment. Mark Havard – Penetration Tester is producing a report.

Clearance Details

Corrective Action To Be Taken			
Actionee		**Reviewing Manager**	
Forecast Completion Date		**Date Completed**	
Verified By		**Verified Date**	

Based on the blank form copied from the Corporate Database in June 2007.

FUJ00080805

B.2. LOC/PBU/RMG/SCY/017 Sequence No. 2 "Ob2)".

Irrelevant

Raised Date	28 Jul 09	**Category**	Observation	**Standard**	ISO 27001-A.11.4.1
Unit	PSD – RRMT - RMGA	**Location**	Various	**Country**	United Kingdom
Division / Community	UK Private Sector	**Interviewee**	Document Review & Andy Dunks (by email)	**Interviewee's Role**	Operational Security
Area Contact	Nigel Hatcher / Neneh Lowther	**Assessor**	Nigel Hatcher	**Process** Corporate / Local	Manage Security / Security Policy

Observation details

The Out of Hours (OOH) password changing process (RS/PRO/047) will no longer be necessary as access for support will be via the iKey authentication. So that document will not be taken forward. Preparation needs to be made:
a) to be ready to mark it Withdrawn in PVCS;
b) amend the wording/reference in the Security Policy (SVM/SEC/POL/0003).

Notes

Clearance Details

Corrective Action To Be Taken			
Actionee		**Reviewing Manager**	
Forecast Completion Date		**Date Completed**	
Verified By		**Verified Date**	

Based on the blank form copied from the Corporate Database in June 2007.

B.3. LOC/PBU/RMG/SCY/017 Sequence No. 3 "Ob3)"

Irrelevant

FUJ00080805

Raised Date	28 Jul 09	**Category**	Observation	**Standard**	ISO 27001-4.3.3 & A.11.4.3
Unit	PSD – RRMT - RMGA	**Location**	Various	**Country**	United Kingdom
Division / Community	UK Private Sector	**Interviewee**	Document Review & Interviews	**Interviewee's Role**	Various
Area Contact	Nigel Hatcher / Neneh Lowther	**Assessor**	Nigel Hatcher	**Process** Corporate Local	Manage Security Security Policy

Observation details

No record was found that automatic equipment detection had been considered as required by ISO 27001 A.11.4.3. (and Control of Records. 4.3.3)

Notes

This is possibly covered by the document HNG-X Branch Router Topic Architecture (ARC/NET/ARC/0003). "presence can be detected through the results obtained from the 'ATI5' command that retrieves version details for managed objects in the unit."

Clearance Details

Corrective Action To Be Taken			
Actionee		**Reviewing Manager**	
Forecast Completion Date		**Date Completed**	
Verified By		**Verified Date**	

Based on the blank form copied from the Corporate Database in June 2007.

FUJ00080805

B.4. LOC/PBU/RMG/SCY/017 Sequence No. 4 "Ob4)"

Irrelevant

Raised Date	28-Jul-2009	**Category**	Observation	**Standard**	ISO 27001-4.3.2
Unit	PSD – RRMT - RMGA	**Location**	BRA01	**Country**	United Kingdom
Division / Community	UK Private Sector	**Interviewee**	Document Review	**Interviewee's Role**	N/A
Area Contact	Nigel Hatcher / Neneh Lowther	**Assessor**	Nigel Hatcher	**Process** Corporate / Local	Manage Security / Security Policy

Observation details
The document "Network Security High Level Design" (DES/NET/HLD/0016) appears to have been started before the RMGA Security Policy (SDM/SEC/POL/0003) was written and hence in its Section 4.1.1 talks of a Security Policy that has no reflection on the policy document. One or other of the two documents needs to be amended to clarify this.

Notes

Clearance Details

Corrective Action To Be Taken			
Actionee		**Reviewing Manager**	
Forecast Completion Date		**Date Completed**	
Verified By		**Verified Date**	

Based on the blank form copied from the Corporate Database in June 2007.

B.5. LOC/PBU/RMG/SCY/017 Sequence No. 5 "Ob5)"

Irrelevant

FUJ00080805

Raised Date	28-Jul-2009	**Category**	Observation	**Standard**	ISO 27001-4.3.2
Unit	PSD – RRMT - RMGA	**Location**	BRA01	**Country**	United Kingdom
Division / Community	UK Private Sector	**Interviewee**	Document Review	**Interviewee's Role**	N/A
Area Contact	Nigel Hatcher / Neneh Lowther	**Assessor**	Nigel Hatcher	**Process** Corporate / Local	Manage Security / Reviewer's Matrix

Observation details
RMGA HNG-X Document Reviewers / Approvers Role Matrix (PGM/DCM/IOM/0001) was checked at times during the audit to clarify if Security was being asked to review documents. It became apparent that they (CSPOA.security GRO) are not on the 'listing' for Low Level Designs, which it was considered by the auditor that they should at least be amongst Optional Reviewers. And hence should be requested to be added to the Matrix.
Notes
a) For all documents to review, the use of the joint email security team mailbox should be re-enforced (awareness cascade) as some documents viewed were being addressed to particular members of the security team only and hence might not get reviewed properly. b) A request should be made to amend the Matrix to list Peter Sewell as the Operational Security Manager and not just Security.

Clearance Details

Corrective Action To Be Taken			
Actionee		**Reviewing Manager**	
Forecast Completion Date		**Date Completed**	
Verified By		**Verified Date**	

Based on the blank form copied from the Corporate Database in June 2007.

B.6. LOC/PBU/RMG/SCY/017 Sequence No. 6 "Ob6)"

Irrelevant

Raised Date	28-Jul-2009	**Category**	Observation	**Standard**	ISO 27001-

FUJ00080805

					A.7.1 (& 4.2.1 d) 1))
Unit	PSD – RRMT - RMGA	**Location**	BRA01	**Country**	United Kingdom
Division / Community	UK Private Sector	**Interviewee**	Ian Mills	**Interviewee's Role**	Networks SDM
Area Contact	Nigel Hatcher / Neneh Lowther	**Assessor**	John Wright	**Process** Corporate Local	Manage Security Security Asset Management

Observation details
It was noted that Limited secure ID log in is authorised by the Networks SDM to Cable & Wireless by email. This is Ownership of an Asset (re ISO 27001 4.2.1 d) 1) & A.7.1.2) and should be recorded.
Notes

Clearance Details

Corrective Action To Be Taken			
Actionee		**Reviewing Manager**	
Forecast Completion Date		**Date Completed**	
Verified By		**Verified Date**	

Based on the blank form copied from the Corporate Database in June 2007.

B.7. LOC/PBU/RMG/SCY/017 Sequence No. 7 "Ob7)"

Irrelevant

Raised Date	28-Jul-2009	**Category**	Observation	**Standard**	ISO 27001-0.2 a)
	PSD – RRMT - RMGA	**Location**	BRA01	**Country**	United Kingdom

FUJ00080805

Unit					
Division / Community	UK Private Sector	**Interviewee**	Howard Pritchard	**Interviewee's Role**	RMGA CISO
Area Contact	Nigel Hatcher / Neneh Lowther	**Assessor**	Nigel Hatcher	**Process** Corporate / Local	Manage Security Capture of Requirements

Observation details
(Understanding Security Requirements) It appeared to the auditor that information on the requirements of the ISO 27001 "Control" areas may not have filtered down to staff that might need to consider them. It is possible that the 'detail' of ISO 27001 may not have been fully addressed in Requirement capture, rather just an entry about being compliant. This needs to be clarified.

Notes
The CISO reported that it had been requested earlier in the year, but after going through all the documentation online, it appears that nothing has happened. Although do get updates from Requirements Team.

Clearance Details

Corrective Action To Be Taken			
Actionee		**Reviewing Manager**	
Forecast Completion Date		**Date Completed**	
Verified By		**Verified Date**	

Based on the blank form copied from the Corporate Database in June 2007.