FUJ00080528

Business Assurance
Internal Assessment - PSD

FUJITSU

Internal Assessment Report

PSD - RMGA

Royal Mail Group Account

ISO 27001 - Readiness Review

FUJITSU

Report Number: GHQ/PSD/RMGA/Royal Mail BRA01/080610

Fujitsu UK & Ireland Internal Assessment of RMG Account, and associated Core Division delivery units,

FUJ00080528

MANAGEMENT SUMMARY

During this Assessment of Royal Mail Group Account 5 Non-conformities and 2 Observations were raised against the PSD. No Non-conformities or Observations were raised against the relevant Core Division Capability Units.

In summary, the main findings and recommendations, as appropriate, were as follows:

1.1

This assessment has been conducted to ensure that the ISMS is sufficiently developed to undertake an ISO 27001 assessment from an external body.

Significant progress has been made in developing the risk approach and assessment. The ISMS manual is generally compliant with the requirements of the international standard. There are a few areas where it would be beneficial to improve the content.

The supporting systems are deployed. Controls were sampled but the level of control sampling is only an indicator as the sample activity was restricted to limited review.

The issues raised at this assessment against ISO27001 need to be addressed prior to the assessment and those raised against ISO9001 need to have a plan in place to address the issues. There are some general improvement comments and it would be beneficial if these were to be reviewed and plans put in place where appropriate.

The outcome of this report indicates that the account is ready for its ISO27001 part 1 assessment.

PSD

- **The ISMS Manual** - defines the security system and provides the scope, objectives, risk methodology and general guidance to the security approach. The documentation structure is not well defined and navigation of the system would be improved by a suitable map or diagram.
  Please see Observation Ref 1 in section 5 and section 4.1 for further details.
- **Risk Management –** The risk methodology has been defined within the ISMS manual. A security risk assessment has been conducted using the STREAM toolset. Controls have been selected and a Statement of Applicability (SOA) produced within the toolset showing the application of those controls. The SOA does not meet the version control and documentation requirements of the International Standard.
  Please see Non-conformance Ref 2 in section 5 and section 4.2 for further details.
- **Documentation Requirements -** Documents & records are generally available and version controlled in Dimensions. Documentation is controlled in accordance with Q&BE/08. *Please section 4.3 for further details.*
- **Key ISMS processes & activities –** processes have been defined. There is a need to ensure that management review activities are fully covered. Training and education is in place, internal audits are planned but records are inconsistent, corrective actions are still to be reviewed and closed from previous years assessments., Measures of effectiveness are not aligned to the security objectives.
  Please see Non-conformities Ref 3, Ref 4 and Observation Ref 5 in section 5 and section 4.4 for further details.
- **BMS & Quality management (ISO 9001) –** a number of BMS requirements were noted as incomplete or not in place. This included integrated audit schedule, process lets and the update of the Implementation Approach Document (IAD).
  Please see Non-conformance Ref 6 in section 5 and section 4.5 for further details.
- **Sampled Security Controls –** a walkthrough of selected processes was conducted. Minimal evidence was reviewed. This was approached in this manner to minimise the operational impact on staff. Processes were noted to be generally in place. The Incident management process was not linking to the Corporate Incident management system which is a requirement of the Security Policy (CPM20)
  Please see Non-conformance Ref 7 in section 5 and section 4.6 for further details.

FUJ00080528

FUJ00080528

Business Assurance
Internal Assessment - PSD

FUJITSU

1. ASSESSMENT CONTROL

Assessment Type	Internal	Assessment Reference	GHQ/PSD/RMGA/080610
1.1 Area	UKPSD - RMGA	Processes Assessed	Various (See Scope of Assessment)
Contact(s)		Process Owner(s)	Various (See Scope of Assessment)
Planned Date	08/06/2010	Lead Assessor	John E Wright
Start Date	08/06/2010	Issue	1.0

2. OBJECTIVES OF THIS ASSESSMENT

2.1 Objectives

This Fujitsu UK & Ireland Internal Assessment focused on key business functions performed in Royal Mail Group Account, and associated Core Division delivery units, and considered, through the assessment of local processes and working practice:

- The compliance of those functions with the Fujitsu UK & Ireland Business Management System (BMS).
- The compliance of those functions with relevant aspects of the ISO 9001 & ISO 27001.
- Any areas suitable for promotion as good business practice across Fujitsu UK & Ireland.

In addition, every opportunity was taken to give advice and guidance on ISO 27001 and corporate process deployment.

FUJ00080528

3. SCOPE

This Fujitsu UK & Ireland Internal Assessment concentrated on the Royal Mail Group Account, and associated Core Division delivery units, and was conducted over 1.5 days, within the Fujitsu Services BRA01 office, and involved the following members of staff:

1.1

3.1 Interviewees

Function / Role	Interviewee
Top Management / CISO	Tom Lillywhite
Quality Management & Corrective Action / Quality Manager	David Parker
Risk Management (Security) / Technical Security Specialist	Bill Membery
Change Management / Customer Services Director	Sarah Bull
Security in S/W Development / Software & Solution Designer/Developer	John Hulme
Security in S/W Development / Solution Delivery Manager	Ian Turner
Business Continuity / Business Continuity Manager	Adam Parker
Secure Areas / Security / Crypto Key Manager	Andy Dunks
System Updates & Malicious Code / Transition Leader - Operational Security	Donna Munro

3.2 Assessment Sampling

The assessment was based on random samples and therefore non-conformities may exist which have not been identified. Observations raised are categorised as Non-conformities and Observations.

3.3 Corrective Action

Following the Assessment, corrective action plans are required for all Non-conformities and Observations raised and should be recorded within the Assessment Database, by the Quality Representative, within 10 working days of the issue of the Assessment Report.

Corrective action plans should also be sent to the Lead Assessor for review and agreement.

The normal target for the implementation of corrective action plans is 60 days from the date of issue of the Assessment Report.

FUJ00080528

4. ASSESSMENT COMMENTARY

4.1 The ISMS Manual

Assessment Criteria: *Establish the ISMS, Implement & operate the ISMS, Monitor and review the ISMS.*

ISO 27001 sections 4.2.1, 4.22, 4.2.3.

- The ISMS manual has already been reviewed at a pre-assessment by BSI.
    - The ISMS manual provides the linkage to the Corporate Policies and Fujitsu UK&I Security Manual.
    - The ISMS manual is SVM/SEC/MAN/0003 is at version 1.6
    - ISMS objectives include:- Management commitment, risk, improvement, Legal & regulatory and education.
    - An operational improvement plan in place
- The ISMS manual has no indication of the documentation structure, *please see Observation Ref 1.* Improvement in the navigating the system could be achieved and it is recommended that the following be considered:-
    - Add a documentation map or diagram
    - Improve linkage to the CCD documents and local procedures.
    - Boundaries & Interface diagram be added to the manual
- Measures of effectiveness are not structured or aligned to the objectives and security process outputs. Most measures are not SMART. Improvement is recommended. See also *section 4.4.* **DONE**
    - Objectives, Measures & targets are expressed in sections 3 -3.2 of the ISMS manual.
    - Measurement & effectiveness is in section 3.2 and the measures do not all relate to the objectives and measures in section 3.1.
    - Consideration needs to be given to SMART measures.
- The high level security organisation, roles and responsibilities are defined in the ISMS manual.
    - The security responsibilities for core roles is currently not defined at community level within the generic Job descriptions etc. This is being followed up outside this assessment. (It is suggested that RMGA may wish to review and discuss this with HR).
- ISMS Scope has been defined.
    - It is difficult to identify technology and functions since its revamp by BSI and it is suggested that a link is added to Appendix 1 so that the coverage is clearer. **DONE**
    - Exclusions to scope are clearly defined.
- Discussion is required as to whether or not interface agreements are required for Core and HR functions as they are represented and managed by the account.

FUJ00080528

- The version of SOA should be removed from the scope statement for ease of maintenance and perhaps replaced with a hotlink to the latest SOA.

4.2 Risk Management, Control selection and SOA

Assessment Criteria: D*efine Risk Approach, Identify risk, Analyse and evaluate risks, sect control objective and controls for the treatment of risk, manage residual risks.*

ISO 27001 sections:4.2.1 (d-g)

- A local Manage Risk process is operated. It is stated that this has been mapped to the local Manage Risk process and that the risk process owner has been consulted in the development of the process.
    - There is no let for this alternative process.IT APPEARS AS THOUGH WE DO NOT NEED ONE
    - It is believed that IAD does not reflect this variation
- The risk approach diagram in the ISMS Manual requires update to ensure that the regulatory aspects are fully expanded (i.e. that there is link to contractual list) – see *section 4.1* above for details ASKED BILL
- A risk tool (STREAM) has been adopted for the purpose at creating and maintaining the risk assessment. This was adopted following the customers dissatisfaction with the preferred Risk Pro approach.
- Risk steps are not necessarily addressed in the conventional order but there is clear evidence that the risk assessment approach ensures that: -
    - Assets have been categorised and owned,
    - threats & vulnerabilities identified,
    - Confidentiality, Integrity and availability incorporated.
- The above has been evaluated as a score and controls selected based on the risk score rating, which was against, a predetermined scoring scheme. Residual risks are retained and risks have been treated by the selection and application of appropriate controls.
- The ISO 27001 controls have been supplemented by additional controls to meet the contractual and regulatory requirements. An SOA (statement of applicability) records the applied controls.
- "**Opportunity for Improvement**" - Review of the values set to each vulnerability selected in the development of the risk assessment are not readily recoverable in the toolset. LATER This could represent an obstacle to understanding the decisions taken in the early stages of the risk assessment. This being said the method is repeatable and vulnerabilities for each category are well defined.
- The SOA (Statement of Applicability) is not version controlled and is a dynamic document produced by the toolset. The controls include more than the references to the standard and it is difficult to navigate. After discussion with the registrar it is agreed that the SOA should be produced as a direct mapping to the Appendix A controls of the standard. The SOA needs to be version controlled and directly traceable to any issued certificate or assessment report. PLACED IN A DOCUMENT AND iIS VERSION CONTROLLED Additionally it is a requirement that exceptions are documented with a reason for their non-selection. (ALL CONTROL GROUPS SEEM PERTINENT AT THIS TIME) *Please see Non-conformance Ref 2.*

FUJ00080528

- Measurement is in place that demonstrates the trend in the risk measures. These are tracked with the objective of reducing risk.

1.1 4.3 Documentation requirements

Assessment Criteria: *Documentation Control & Records, Q&BE/08.*

ISO 27001 sections 4.3.

- Documents & Records are generally available and version controlled in Dimensions. Documentation is controlled in accordance with Q&BE/08.
- Delays in versions updates can occur due to the bottleneck of the document controller.
- Some quality records such as monthly security review are not yet held on a network repository. **(Don't understand this, the monthly security report is held on Dimensions)**
- Audit plans and records are not consistently recorded – please see *section 4.4* below for details.
- Records & Repositories need to be retained on a FS UK&I corporate drive. There were a few examples of meeting notes that had been retained on laptops. **These meeting notes are now on our security web site** This was resolved at the assessment however awareness of this needs to be flowed down the team.

4.4 Key ISMS processes & activities

Assessment Criteria: Assess & review the BMS, process management, Manage the BMS.,

ISO 9001 sections5- 8,

Management Review & Responsibility

- Management Review is partly addressed in the quarterly system reviews (ISMR). It is suggested that the input requirements of the standard are checked to the agenda to ensure that all aspects are covered. It may also be appropriate to summarise the proposed security measures as an input. See measures of Effectiveness below:

Measures of Effectiveness

- It is a requirement of the international standard that measures of effectiveness of the system controls are made (4.2.2 (d)).
- The measures defined in the ISMS manual in respect of the system (see also *section 4.1* above for details) are not fully aligned to the objectives and targets. **Now aligned and measures upgraded** There is a need to understand what control measures will demonstrate effectiveness. Then to develop an appropriate reporting mechanism such as a scorecard…**Scorecard will be developed** Please see Non-Conformance *Ref 3*.

Training Awareness, Education and Competence

- The corporate CBT used for security awareness training has been mandated on the account and current completion rate stands at 87%
- A RMGA communications strategy is in place and this includes:

FUJ00080528

- Regular cascades of security information.
- CafeVik articles
- Communication is provided by the PMO (Programme office) function.

- It was stated that security competence is recorded within Performance plus and that records of training are available.
- Key security roles have defined competences.

Internal Audits

- The RMGA account including the Core services aspect is some 300 people. The key site for the operation of the service is Bracknell. Internal security audits have been conducted throughout the development of the ISMS, however, records are held in various locations and plans are not consistent. This means that coverage and recoverability of records is impacted.
  - A local internal audit strategy plan exists.
  - A local internal audit plan for 2010-11 has been produced.
  - One audit has been completed this year
  - By the time of the assessment only 3 will have been completed.
  - Last years audit records (2009-10) are not controlled by a formal plan and to demonstrate coverage suitable for an assessment this will need to be addressed. Please see Non-Conformance *Ref 4*.
  - Internal Security Audits are not shown on the RMG account integrated assessment plan. Please see *section 4.5 below.*

Corrective and Preventive Actions

- Corrective Actions from previous internal assessments are outstanding. It is essential that this is resolved prior to an external assessment. Please see Observation *Ref 5*.
  - There are 48 aged issues and the new quality manager has currently evidenced closure of 14.
  - The Quality Manager has a plan in place to review and close theses issues.
- **"Opportunity for Improvement" -** The location of the records of defects and the actions taken to resolve them is inconsistent and it has been agreed that all will now be recorded into the assessment Db.

4.5 BMS & Quality Management

Assessment Criteria: Assess & review the BMS, process management, Manage the BMS.,

ISO 9001 sections 4,

- As part of the interview process for the readiness to ISO 27001 it was noted that a number BMS management issues arose. Although these are not show stoppers in respect of ISO 27001 there needs to be action taken to ensure future compliance with the BMS. These are raised collectively under one Non-Conformance against the Quality Policy rather than at the individual process level. Please see Non-conformance *Ref 6*.

FUJ00080528

- Integrated audit schedule is in place but for year 2009-10. It does not contain information about Security Audits conducted in that period.
- Most of the internal audit reports and internal security audit reports are recorded in the assessment database. However, 2010 audits have not been recorded in the assessment database and findings are therefore not consistently located. 1.1
- Process lets were not readily available for the sampled processes at this assessment. It is thought that some exist but due to staff changes the traceability seems to have been lost. It has been suggested that in future lets or equivalent evidence are hot linked to the IAD.
- The Implementation approach document (IAD) is in place however it is considered that it may be out of date and due review.

4.6 Sampled Controls & associated processes

Assessment Criteria: *Sampled controls see below for details*

ISO 27001 sections A5 – A15

Change Management

- All New Services and changes are introduced via Change Control. This has recently transferred to the MSC toolset.
    - Criteria has been set to involve Security in CAB and risk assessment where appropriate (typically Sophos firewalls etc..).
    - Mechanisms to include change impacts into Security risk assessment are in place but still need to be documented in the ISMS risk method.
    - Although at this time no change has impacted the overall security risk register it should be remembered that this can occur and that a significant change could increase or decrease the applied controls.

Security Incident Management

- A local process supports this activity and a register of incidents is retained. All incidents are discussed and acted upon in conjunction with the customer. Security meetings are formally in place. Incidents and trends are discussed with senior management of the account at the interim (currently 2 weekly) and quarterly reviews.
    - It is unclear if the local Security Incident management process has been approved by the process owner / champion and a let granted.
    - Security Incidents are not reported outside the account. It is a requirement of the Security Policy that all incidents (possibly anonymous) be recorded into the corporate incident management system. This allows the SMF to analyse issues occurring within Fujitsu UK & I so that they can further advise the SMB as to whether or not additional controls may be necessary. Please see Non-Conformance *Ref 7*.

Third Party Management

- Although the account has numerous suppliers only one is deemed to impact the security system. This supplier is based in India (Infinite). The supplier is ISO 27001 registered and

FUJ00080528

is also subject to supplier audit by the RMG account security team. The supplier audit process is laid out in SVM/SEC/PRO/0036.

- Audits of the supplier have been conducted.
- Security requirements are expressed in the contract.

1.1

- A scoring mechanism is in place against the International Standard (ISO 27001) clauses.
- Longer term it may be possible to reduce the frequency of visits based on the performance achieved.

Risk in S/W Design & Development

- The processes operated for the software design & development are based on the Waterfall model. The processes are unique to the RMG account. It is thought that the ADBM process owner was consulted during the process development. Security issues are considered in the overall architectural approach and security risks and requirements are reviewed and accepted during design approval.
  - The process design let was not available. A collective issue is raised in *section 4.5* above.
  - Code review is conducted at an independent level as is system testing.
  - There is an **"Opportunity for Improvement"** to add a single sheet to the development overview showing the interactions of security with the software development method.

Business Continuity Management

- Business Continuity plans exist for the account activities and are covered by 3 separate document:- HnGx Services, Support and Engineering Services. All plans have been approved and up to date.
  - Test plans are scheduled annually and all tests have currently been achieved.
  - Results of tests are reviewed with the customer.
  - Activities are reported in the Service report
  - There would appear to be an **"Opportunity for Improvement"** to ensure that any threats in this area flow through to all impacted activities.

Secure Areas (Physical Security and Access Control)

- A walk round was conducted of the secure rooms on Floor 4. Access is controlled by key card and the rooms are also within a secure area. The rooms deal with confidential transaction and fraud activities and can involve copying data to CD's to support customer investigations. Access is limited to around 10 people. At the time of the visit there was activity in progress.
  - The activity is being condensed to one room and the removal of obsolete kit, Dat tapes and storage of some test items will discontinue.
  - All machines in use were found to be locked down and password protected.
  - All data extractions are encrypted and delivered by courier.

FUJ00080528

- Access is controlled via site services and it is recommended that an audit is conducted to ensure that access to the card updating facilities is secure and that the staff are trained and aware of the latest authorised signatories for granting access to secure areas.

1.1

FUJ00080528

5. NON-CONFORMITIES AND OBSERVATIONS

The following Observations and Non-conformities were raised during the course of this assessment

1.1

FUJ00080528

5.1 Observation Ref.1

Reference / Sequence	1	**Date of Observation**	14/06/10	
Category	Observation	**Standards / Section**	ISO 27001	4.2.1
Corporate Process	Manage Security	**Local Process**		
Unit	RMGA Account	**Country**	UK	
Location	GRO	**Division**	PSD	
Interviewee	Tom Lillywhite	**Interviewee's Role**	CISO	
Area Contact	David Parker	**Assessor's Name**	John E Wright	

Observation

- The ISMS manual has no indication of the documentation structure.
- Improvement in the navigating the system could be achieved and it is recommended that the following be considered:-
  - Add a documentation map or diagram
  - Improve linkage to the CCD documents and local procedures.
  - Boundaries & Interface diagram be added to the manual

A document map has been added
There is link to the major Fujitsu processes (CM20 etc)
Boundaries and Interface diagram has been produced

Notes

[1]

[1] A Corrective Action Plan that 1), clearly addresses Observation detailed above 2), identifies why any recommendations detailed within the Notes section are not included and 3), identifies a realistic planned completion date for the corrective action, must be reviewed and agreed by the Lead Assessor.

FUJ00080528

5.2 Non-conformance Ref.2

Reference / Sequence	2	**Date of Observation**	14/06/10	
Category	Non-conformance	**Standards / Section**	ISO 27001	4.2.1 (j)
Corporate Process	Manage Security	**Local Process**		
Unit	PSD-RMG / Royal Mail Account	**Country**	UK	
Location	GRO	**Division**	PSD	
Interviewee	Bill Membery	**Interviewee's Role**	Technical Security Specialist	
Area Contact	David Parker	**Assessor's Name**	John E Wright	

Non-conformance

The SOA (Statement of Applicability) is not version controlled and is a dynamic document produced by the toolset.
The controls include more than the references to the standard and it is difficult to navigate.

Additionally, it is a requirement that exceptions are documented including the reason for their none selection

The document has now been produced; follows the RMGA template standard and is version controlled (Version 8). There are, currently, no exceptions

Notes

After discussion with the registrar it is agreed that the SOA should be produced as a direct mapping to the Appendix A controls of the standard. The SOA needs to be version controlled and directly traceable to any issued certificate or assessment report**....and so it is**

[2]

[2] A Corrective Action Plan that 1), clearly addresses the Non-conformance detailed above 2), identifies why any recommendations detailed within the Notes section are not included and 3), identifies a realistic planned completion date for the corrective action, must be reviewed and agreed by the Lead Assessor.

FUJ00080528

5.3 Non-conformance Ref. 3

Reference / Sequence	3	**Date of Observation**	14/06/10	
Category	Non-conformance	**Standards / Section**	ISO 27001	4.2.2 (d)
Corporate Process	Manage Security	**Local Process**		
Unit	PSD-RMG / Royal Mail Account	**Country**	UK	
Location	GRO	**Division**	PSD	
Interviewee	Tom Lillywhite / Bill Membery	**Interviewee's Role**	CISO / Technical Security Specialist	
Area Contact	David Parker	**Assessor's Name**	John E Wright	

Non-conformance

The measures defined in the ISMS manual (Section 3) in respect of the system are not fully aligned to the objectives and targets.

Defined measures are not SMART.

Notes

There is a need to understand what control measures will demonstrate effectiveness and to develop an appropriate reporting mechanism such as a scorecard.

Aligned and the measures have been altered

[3]

[3] A Corrective Action Plan that 1), clearly addresses the Non-conformance detailed above 2), identifies why any recommendations detailed within the Notes section are not included and 3), identifies a realistic planned completion date for the corrective action, must be reviewed and agreed by the Lead Assessor.

FUJ00080528

5.4 Non-conformance Ref. 4

Reference / Sequence	4	**Date of Observation**	14/06/10	
Category	Non-conformance	**Standards / Section**	ISO 27001	6
Corporate Process		**Local Process**		
Unit	PSD-RMG / Royal Mail Account	**Country**	UK	
Location	GRO	**Division**	PSD	
Interviewee	Tom Lillywhite / Bill Membery	**Interviewee's Role**	CISO / Technical Security Specialist	
Area Contact	David Parker	**Assessor's Name**	John E Wright	

Non-conformance

Records and planning of Security audits are not readily available.

Last years audit records (2009-10) are not controlled by a formal plan and to demonstrate coverage suitable for an assessment this will need to be addressed.

Notes

I think I have forwarded the present schedule to David, who is looking into the matter

[4]

[4] A Corrective Action Plan that 1), clearly addresses the Non-conformance detailed above 2), identifies why any recommendations detailed within the Notes section are not included and 3), identifies a realistic planned completion date for the corrective action, must be reviewed and agreed by the Lead Assessor.

FUJ00080528

5.5 Observation Ref. 5

Reference / Sequence	5	**Date of Observation**	14/06/10	
Category	Observation	**Standards / Section**	ISO 9001	8.2
Corporate Process		**Local Process**		
Unit	PSD-RMG / Royal Mail Account	**Country**	UK	
Location	GRO	**Division**	PSD	
Interviewee	Tom Lillywhite / Bill Membery	**Interviewee's Role**	CISO / Technical Security Specialist	
Area Contact	David Parker	**Assessor's Name**	John E Wright	

Observation

Corrective & Preventive Actions from previous internal assessments are outstanding.

Notes

It is essential that this issue is resolved prior to an external assessment

There are 48 aged issues and the new quality manager has currently evidenced closure of 14.

The Quality Manager has a plan in place to review and close theses issues.
Have noted the work on these!

[5]

[5] A Corrective Action Plan that 1), clearly addresses the Observation detailed above 2), identifies why any recommendations detailed within the Notes section are not included and 3), identifies a realistic planned completion date for the corrective action, must be reviewed and agreed by the Lead Assessor.

FUJ00080528

5.6 Non-conformance Ref. 6

Reference / Sequence	6	**Date of Observation**	14/06/10	
Category	Non-conformance	**Standards / Section**	ISO 9001	4.2.1 (e)
Corporate Process	Document & Record Management	**Local Process**	Document & Record Management	
Unit	PSD-RMG / Royal Mail Account	**Country**	UK	
Location	GRO	**Division**	PSD	
Interviewee	David Parker	**Interviewee's Role**	Quality Manager	
Area Contact	David Parker	**Assessor's Name**	John E Wright	

Non-conformance

- Integrated audit schedule is in place but for year 2009-10. It does not contain information about Security Audits conducted in that period.
- An amount of internal audit reports and internal security audit reports are recorded in the assessment database. However, 2010 audits have not been recorded in the assessment database and findings are therefore not consistently located.
- Process lets were not readily available for the sampled processes at this assessment. It is thought that some exist but due to staff changes the traceability seems to have been lost. It has been suggested that in future lets or equivalent evidence are hot linked to the IAD.
- The Implementation approach document (IAD) is in place however it is considered that it may be out of date and due review.

Notes

David and Bill/Tom

6

A Corrective Action Plan that 1), clearly addresses the Non-conformance detailed above 2), identifies why any recommendations detailed within the Notes section are not included and 3), identifies a realistic planned completion date for the corrective action, must be reviewed and agreed by the Lead Assessor.

FUJ00080528

5.7 Non-conformance Ref. 7

Reference / Sequence	7	**Date of Observation**	14/05/10	
Category	Non-conformance	**Standards / Section**	ISO 27001	A 13.1.1
Corporate Process	Security Policy	**Local Process**		
Unit	PSD-RMG / Royal Mail Account	**Country**	UK	
Location	GRO	**Division**	PSD	
Interviewee	Tom Lillywhite / Bill Membery	**Interviewee's Role**	CISO / Technical Security Specialist	
Area Contact	David Parker	**Assessor's Name**	John E Wright	

Non-conformance

It is a requirement of the Security Policy that all incidents (possibly anonymous) be recorded into the corporate incident management system.

This allows the SMF to analyse issues occurring within Fujitsu UK & I so that they can further advise the SMB as to whether or not additional controls may be necessary.

Notes

Security Incidents are not currently reported outside the account.

Putting process in place to do this…latest, sale of a router on ebay has been copied across

[7]

[7] A Corrective Action Plan that 1), clearly addresses the Non-conformance detailed above 2), identifies why any recommendations detailed within the Notes section are not included and 3), identifies a realistic planned completion date for the corrective action, must be reviewed and agreed by the Lead Assessor.