

The Office of the Adjudicator - BTS

Audit of the Arqiva Information Security Strategy

Jon Butler
4th May 2011 v1.0

Contents

Introduction..... 3

Executive Summary 3

Audit Scope..... 3

Audit Steps 4

The Audit Schedule..... 4

The review and testing of the measures and protocols..... 5

 ISS Part 2: Principles for Access and Use of Confidential Information..... 5

 ISS Part 3: Protocol for the Identification and Treatment of Different Categories of Confidential Information..... 6

 ISS Part 4: Measures to Ensure the Security of Confidential Information 6

 Security of Information Storage and Systems 6

 Physical Security of Confidential Information 6

 Employee Disclosure 7

 In the event that Arqiva is a bidder in a Competitive Spectrum Action..... 7

 Staff Training and Awareness..... 7

 ISS Part 5: Next Steps 7

ISS Protocols and Measures - The Undertakings..... 9

ANNEX A - Information and documents supporting the ISS audit. 10

Introduction

Section 16 of the Undertakings require that Arqiva publish an Information Security Strategy to meet the Confidentiality of Information requirements of the Undertakings. The Undertakings also set requirements related to this strategy.

The Office of the Adjudicator- BTS undertook an audit of the Arqiva Information Security Strategy (ISS) during March 2011. This document represents a summary of the findings.

Executive Summary

The evidence presented by Arqiva and the tests and interviews undertaken by the representative of the Adjudicator demonstrated that Arqiva are compliant with the protocols and measures stated within the published Information Security Strategy document and that no material deviation was evident. The evidence produced by Arqiva also demonstrates that the protocols and measures stated in the Undertakings have been satisfactorily implemented by Arqiva. The audit tests have established that these measures are operating satisfactorily.

The representative of the Adjudicator makes two observations for consideration:

- 1) Since the ISS document was published the protocols and measures referenced in the ISS document have been put into practise and in some cases further developed. It is recommended that either the ISS document is updated to reflect current practises or a separate document is produced which describes these practises.
- 2) That tests related to the protocols and measures are documented and that the results of these tests are recorded.

Audit Scope

The Audit scope was agreed between the Adjudicator and Arqiva with the aim of the audit to answer the key question: 'Do Arqiva meet the requirements of the Undertakings?'

In order to answer this question the audit scope was set as follows:

- 1 Do the protocols and measures described in the Arqiva ISS document meet the requirements of the Undertakings?
- 2 Can Arqiva demonstrate that these protocols and measures are appropriately applied and successfully practised within their business?

Audit Steps

In order to answer the questions within the Audit Scope it was agreed between the Adjudicator and Arqiva that the audit would follow the following steps.

- 1) To review the ISS document with Arqiva.
- 2) Establish how the protocols and measures within the ISS document are practically undertaken within Arqiva.
- 3) To agree tests and checks related to these protocols and measures as applied to real business activities within Arqiva.
- 4) Undertake these tests and checks, and to obtain evidence as appropriate
- 5) Establish if the protocols and measures, as evidenced, meet the requirements of the Undertakings

The Audit Schedule

The Audit steps were delivered through face to face meetings, document reviews, Q&A exchanges, the provision of information packs and supporting documents, interviews with Arqiva staff and through physical checks at Arqiva offices in Warwick.

The representative of the Adjudicator (J Butler) met with Arqiva at UK house on 10th Feb 2011 to review the ISS strategy. Following this meeting Arqiva produced a comprehensive information pack to demonstrate the measures and protocols related to the matters discussed.

This information was reviewed by the representative of the Adjudicator and discussed with Arqiva at UK House on 11th March 2011. Further supporting information was provided by Arqiva following this meeting and a set of interviews and physical tests were agreed.

The interviews and tests were undertaken at Arqiva Warwick on 24th March. This also provided an opportunity for final Q&A's and Arqiva followed up with additional supporting information. Arqiva made available a selection of locations and departments for interviews and tests and the Adjudicator selected Warwick and Arqiva staff from Spectrum Planning and Arqiva MuxCo for interview.

The documentation and information supplied by Arqiva has not been copied into this report but 'Annex A' provides a comprehensive list of the information and documents used in support of this audit.

The review and testing of the measures and protocols

The ISS document contents are listed below, the measures and protocols are contained within sections 2-5.

1. Introduction
2. Principles for Access and Use of Confidential Information
3. Protocol for the Identification and Treatment of Different Categories of Confidential Information
4. Measures to Ensure the Security of Confidential Information
 - 4.1. Security of Information Storage and Systems
 - 4.2. Physical Security of Confidential Information
 - 4.3. Employee Disclosure
 - 4.4. In the event that Arqiva is a bidder in a Competitive Spectrum Action
 - 4.5. Staff Training and Awareness
5. Next Steps

Within each of these sections the measures and protocols were extracted for comment and, where appropriate, evidence and/or test was provided or undertaken to demonstrate compliance. The following sections provide a summary of the evidence which was reviewed and the tests which were undertaken.

ISS Part 2: Principles for Access and Use of Confidential Information

a) Managers personal objectives regarding ISS

Evidence and Test: Screen prints of electronic HR personal objective records were provided as evidence and in addition these were discussed and evidenced in interviews. This was deemed compliant by the representative of the Adjudicator.

b) Distinction between business activities and for the purposes of audit evidenced regarding Arqiva MuxCo and Spectrum Planning.

Evidence and Test: Organisation charts were produced as well as screen prints of HR records showing line management structures. Also tested by physical observation of the working areas and by demonstration of the restrictions imposed by security tags. This was deemed compliant by the representative of the Adjudicator.

c) Bid team management regarding spectrum auction

Evidence and Test: Arqiva are in the process of setting up a spectrum auction bid team but this has not been finalised. Evidence was produced regarding the current dialogue between Arqiva, Ofcom and the Office of the Adjudicator as evidence that implementation of appropriate management separation will exist to the satisfaction of Ofcom and the Adjudicator. This was deemed compliant by the representative of the Adjudicator.

d) Separation of MTS and NA account teams and confidential information.

Evidence and Test: Arqiva demonstrated the storage of confidential information and the electronic access restrictions. This is also discussed later. In addition, Arqiva demonstrated the management separation between relevant teams through organisational diagrams and screen

prints from their HR database. This was deemed compliant by the representative of the Adjudicator.

ISS Part 3: Protocol for the Identification and Treatment of Different Categories of Confidential Information

- a) For Very High Risk Confidential Information the Arqiva protocol specifies additional measures.

Evidence and Test: The Arqiva Spectrum Planning team are under contract from Ofcom to provide spectrum planning services related to spectrum auctions. This is classified as Very High Risk Confidential Information. Through interviews and physical checking, evidence of correct categorisation and the application of appropriate physical and electronic security measures was provided. This was deemed compliant by the representative of the Adjudicator.

ISS Part 4: Measures to Ensure the Security of Confidential Information

Security of Information Storage and Systems

- a) Measures relate to the restricted access and maintenance of records specific to electronic information and storage systems.

Evidence and test: Arqiva use the Livelink system to store and retrieve electronic information. The maintenance of the access restrictions was evidenced through a documented procedure for the control and permissions rights for staff accessing Livelink. Arqiva have further enhanced Livelink access control through the complete separation of Arqiva MuxCo with a standalone intranet based Livelink system. This has been undertaken as a preventative enhancement rather than corrective measure. This separation was evidenced through observation of the MuxCo Livelink system by the representative of the Adjudicator.

Storage on Arqiva laptops and memory sticks is encrypted for those staff working on activities covered by the Undertakings. A programme is also underway to roll-out this approach to the rest of the organisation. This was evidenced through IT policy and project documents.

This was deemed compliant by the representative of the Adjudicator.

Physical Security of Confidential Information

- a) Measures: Physical security of information is achieved through door access control, physical separation of departments and locked cabinets.

Evidence and Test: The door access control at Warwick was tested, by sample, using staff passes from permitted and non-permitted departments and in addition the temporary passes at reception were also sample checked. The physical separation was evidenced through observation and locked cabinets were inspected within the Spectrum Planning department. This was deemed compliant by the representative of the Adjudicator.

Employee Disclosure

- a) Measures: The Arqiva code of conduct outlines the confidentiality policy and the individual staff requirement to adhere to this policy.

Evidence and Test: This is available to all staff on the Arqiva intranet and evidence of this was provided in screen shots. Staff undergo training to ensure that they understand the policy and this was evidenced through interviews and by Arqiva providing training records. Specific objectives exist in staff records and these were evidenced through screen shots of electronic objective records. This was deemed compliant by the representative of the Adjudicator.

In the event that Arqiva is a bidder in a Competitive Spectrum Action

- a) Staff responsible for a bid related to a spectrum Auction will be distinct from those required to access and use confidential information related to a customer or prospective customer where they may be in competition.

Evidence and Test: Arqiva are in the process of setting up a spectrum auction bid team but this has not been finalised. Evidence was produced regarding the current dialogue between Arqiva, Ofcom and the Office of the Adjudicator as evidence that implementation of appropriate management separation will exist to the satisfaction of Ofcom and the Adjudicator. This was deemed compliant by the representative of the Adjudicator.

Arqiva are not currently bidding on any spectrum auctions and so no related Very High Risk Confidential information exists for test within this audit.

Staff Training and Awareness

- a) Arqiva state three steps regarding protocols and measures which relate to initial and on-going staff awareness and training and annual performance reviews.

Evidence and test: Through interviews and the production of screen dumps related to staff objectives the performance review requirement was evidenced. Training was evidenced through schedules of staff training completed and the presentations used to deliver this training. Arqiva provided a standard employee Welcome Pack which contained a Code of Conduct (ref BOP920.4) which includes appropriate Confidentiality statements. This was deemed compliant by the representative of the Adjudicator.

ISS Part 5: Next Steps

- a) The ISS notes that Arqiva will further develop and test the measures set out in the ISS and that the ISS will be subject to regular review and may be updated from time to time.

Evidence and Test: Throughout the Audit, evidence of the development of the ISS was demonstrated by the practical steps which have been put in place by Arqiva to deliver the protocols and measures within the Information Security Strategy. The Information Security Strategy document has not been updated to reflect these developments.

Tests related to the protocols and measures were evident through interviews and evidenced by the measures adopted. As examples, the Spectrum Planning team undertake testing related to the access of restricted technical information held electronically and the tracking and management of staff training provided a test of compliance. However, a documented programme of test was not evident nor was the requirement for testing documented in the adopted measures.

In reference to these observations two recommendations are made:

- 1) That either the ISS document is updated to reflect current practises or a separate document is produced which demonstrates how the strategy has been put into practise.
- 2) That tests related to the protocols and measures are documented and that the results of these tests are recorded.

ISS Protocols and Measures - The Undertakings

Section 16.2 of the Undertakings states that Information Strategy shall require Arqiva to implement appropriate measures described as:

- 16.2.1 to ensure the security of Arqiva's information storage systems and data systems (including data collection, storage and archiving), particularly where confidential information referred to in paragraph 16.1 is stored in systems shared between business units;
- 16.2.2 to ensure the physical security of confidential information referred to in paragraph 16.1;
- 16.2.3 to ensure that an employee of one business unit does not disclose or use the confidential information referred to in paragraph 16.1 of which the employee had become aware whilst working for another business unit;
- 16.2.4 to ensure the security of the confidential information referred to in paragraph 16.1 in the event that Arqiva is a bidder in a spectrum auction in competition with a Customer or prospective customer; and
- 16.2.5 to ensure that staff receive adequate training in relation to the Information Security

The evidence produced by Arqiva demonstrates that the protocols and measures stated in the Undertakings have been satisfactorily implemented by Arqiva. The audit tests have established that these measures are operating satisfactorily.

ANNEX A - Information and documents supporting the ISS audit.

1. The Arqiva Information Security Strategy v1.0 1st October 2008.
2. Undertakings Compliance report for the period 1st September 2008 to 30th June 2009, dated 30th November 2009.
3. Undertakings Compliance report for the period 1st July 2009 to 30th June 2010, dated 30th November 2010.
4. High level Arqiva organisational chart & Spectrum Planning Organisation Chart
5. Digital Platforms team organisational chart
6. Screen print from Arqiva Intranet: Commercial section regarding Compliance and Undertakings, ISS Strategy, Code of Conduct and training packs.
7. Organisation Charts from HR Systems:
 - a. Drew Hose: BBC Client Director
 - b. Kevin Moroney: Regulatory and Compliance Director
 - c. Peter Mensforth: Head of Network Access
 - d. Denis Moloney: Head of Change Management
 - e. Mark Jordan: Business Operations
 - f. Tony Mattera: TV Network Design Director
 - g. Brent Vaughan: Director of Sales, Commercial Broadcast
 - h. Brian Tait: Spectrum Planning Manager
 - i. Adrian Briggs: Spectrum Planning Manager, Warwick
 - j. Glenn Doel: Principal Spectrum Engineer
8. Screen dumps from Arqiva PeopleSoft HR database showing Personal Objectives
9. Terms of Reference for the ISS Audit
10. Extract from the Undertakings: Section 16 Confidentiality of Information
11. ISS document: marked up version show responses to Audit questions
12. Arqiva Code of Conduct
13. ISS & Code of Conduct: Training Pack (2008/9)
14. ISS & Code of Conduct: Training Pack (Refresher 2010/11)
15. ISS & Code of Conduct: Training pack – Board Update (Refresher 2010/11)
16. ISS & Code of Conduct: Training Status Update (Refresher 2010/11)
17. Spectrum Planning Correspondence, Overview & Compliance statements
18. ISS Security Project – Scoping document
19. Physical Security Explanatory Note
20. Compliance strategy presented to Arqiva board
21. Arqiva Staff lists
22. Arqiva Staff lists showing those who have undertaken ISS training
23. Reference Offer interface points – Overview
24. Monthly SDO Status report examples – Copy stamped company confidential
25. Example MuxCo daily report examples – Copies stamped company confidential
26. Document containing responses to questions raised by J Butler on 9th March 2011-04-21
27. Follow up questions and responses to above
28. Interview questions: J Butler interviews of Arqiva Spectrum Planning and Arqiva MuxCo staff.
29. Arqiva MuxCo to Arqiva TransCo interaction- flip chart presentation
30. Live Link Permissions configuration and supporting screen shots
31. Monthly Compliance Pack pro-forma: Inclusion of confidentiality and ISS compliance sign off.

32. Physical Check of security measures at Arqiva Warwick – Audit Tick Sheet by J Butler
33. Arqiva Staff Welcome pack