



Deposited via The University of York.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/id/eprint/109818/>

Version: Accepted Version

Article:

Chivers, Howard Robert (2016) Control Consistency as a Management Tool: The Identification of Systematic Security Control Weaknesses in Air Traffic Management. International Journal of Critical Computer-Based Systems. ISSN: 1757-8787

<https://doi.org/10.1504/IJCCBS.2016.079079>

Reuse

Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

Control Consistency as a Management Tool: The Identification of Systematic Security Control Weaknesses in Air Traffic Management.

Howard Chivers

Department of Computer Science, University of York, Deramore Lane,
York, YO10 5GH. Email: hrchivers@iee.org

Abstract: In 2008 EUROCONTROL published Information and Communications Technology (ICT) Security Guidance to Air Navigation Service Providers (ANSPs), to assist them in complying with regulatory security requirements. This included a visualisation tool which allowed the consistency of control sets to be reviewed and communicated: consistency being the degree to which more sophisticated controls were supported by core controls. The validation of that guidance included surveys which were conducted to contrast current practice in European ANSPs with a baseline control set based on ISO/IEC 27001:2005. The consistency test revealed significant gaps in the control strategies of these organisations: despite relatively sophisticated control regimes there were areas which lacked core controls. Key missing elements identified in the ANSPs surveyed include security management and senior management engagement, system accreditation, the validation and authentication of data used by ATM systems, incident management, and business continuity preparedness. Since anonymity requires that little can be said about the original surveys these results are necessarily indicative, so the paper contrasts these findings with contemporaneous literature, including audit reports on security in US ATM systems. The two sources prove to be in close agreement, confirming the value of the control consistency view in providing an overview of an organisation's security control regime.

This paper is a revised and expanded version of the paper entitled "Security Blind Spots in the ATM Safety Culture" presented at the SecATM workshop at ARES 2013, Regensburg, Germany. September 2-6th 2013. This paper introduces the consistency perspective and its methodological use, the previous paper was limited to results as they applied to ATM.

Keywords: Security Management, Security Control, Authentication, Business Continuity, Incident Management, Air Traffic Management, Air Navigation Service

Biographical Notes: Howard Chivers is a Senior Lecturer in Cyber Security at the University of York, and Director of Oddenhill, a company which provides services in information security and computer forensics. His research interests are in forensic analysis, intrusion detection, system security and risk management. His previous career includes the development of cryptographic products in Industry, managing the UK national computer security research program at CESG, and acting as the Director of the Centre for Forensic Computing at Cranfield University.

1. Introduction

In order to assist Air Navigation Service Providers (ANSPs) in Europe with the implementation of EC Regulation 2096/2005(2005a), EUROCONTROL developed a range of security guidance material which included Information and Communications Technology (ICT) Security Guidance published in 2008.

The guidance material was designed to assist ANSPs with the selection of baseline controls to meet the requirements of ISO/IEC 27001:2005 (International Organisation for Standards (ISO), 2005), and includes a questionnaire which can be used to assess an organization's current level of compliance. The questionnaire was tested by a small (less than 10) sample of ATM organizations in Europe, chosen to represent a range of different size organizations and degree of security maturity. The responses were a mixture of comments on the proposed questions and completed questionnaires.

The ICT guidance presented controls in 6 incremental levels, allowing a control baseline (a specific level) to be set using a coarse risk assessment for a specific organization. A modified form of 'spider' presentation was developed as a management tool to allow the examination of control maturity and, importantly, visualize if the pattern of controls is accumulative (more complex controls built on the basis of core controls) or if it is inconsistent, meaning that some sophisticated controls are present but more basic controls are missing. Reviewing the survey findings in this way demonstrates a high degree of inconsistency in the control sets.

This paper respects the anonymity of the survey responders, and is therefore limited in the details that can be provided. However, the structure of the guidance material and the results taken as a whole provide important lessons for the assessment of control systems and specific conclusions relating to deficiencies in Air Navigation Service Providers' security management.

These putative findings are tested by reviewing other literature sources that identify security defects in Air Traffic Management, including contemporaneous audit reports on US organizations. The results closely parallel the findings derived from the European survey data.

The contribution of this work is that it introduces the concept of consistency in control regimes, and provides a mechanism that allows it to be readily assessed and visualized. The value of this concept is demonstrated by quantifying key problems in security in existing ATM organizations, based on actual survey and audit information.

ATM organizations have a long-established safety culture supported by organizational practices and standards. There is certainly an overlap between controls used in support of safety and those needed to mitigate security threats; however, this work demonstrates that organizations with a strong safety focus may have serious deficiencies in their ability to defend and respond to security incidents.

This paper is organized as follows. Section 2 provides an introduction to the ICT Guidance; in particular it explains how baseline controls were structured and the purpose of the questionnaire. Section 3 introduces Control Consistency and the diagrams used to visualize and review consistency. Section 4 describes the method used to process survey results, the validation of those results and their review using a control consistency spider. Section 5 reviews ISO/IEC 27001 controls that were found to be absent in the corpus, and Section 6 describes contemporaneous evidence from alternative sources that suggest security problems in ATM systems: audit reports on US ATM organizations and known ATM ICT security vulnerabilities. The discussion in section 7 contrasts the two sets of results and also identifies current security standards in which this technique could be employed. The paper is concluded in section 8.

2. ICT Guidance

The brief for the ICT Guidance was to provide assistance for ANSPs who wished to establish appropriate baseline security controls in compliance with established international standards. The primary source was ISO/IEC 27001:2005, which is also the focus of this paper; other standards (COBIT and ISO 13335-4) were also referenced.

The controls specified in ISO/IEC 27001 are necessarily generic requirements that apply to a wide range of different circumstances. Even supplemented by the guidance in ISO/IEC 27002 they are difficult to interpret for those new to security management. One problem is the selection of appropriate concrete controls; another is ensuring that the type of each control is proportionate to the risk.

The approach taken in the guidance was first to define six levels which correspond to coarse graduations of risk. Controls in the guidance were then arranged to allow a baseline set of controls to be selected appropriate to the level of risk to which the organization is exposed. The choice of which risk level applied to an organization used a high-level risk assessment process which is not described in detail here; however, the next section summarizes the criteria used in the assessment in order to clarify how risk levels were motivated and structured.

2.1. ICT Risk Levels

Information security is often a balance between protecting the whole organization, and dealing with risks to specific Service or Business Critical (SBC) assets. This balance is influenced by the degree to which critical assets are isolated from the rest of the organization; relatively isolated systems maintain a focus on managing SBC-specific risks, whereas if SBC assets are fully integrated the need is to focus more on overall protection.

This split was recognized in the choice of the 6 risk levels, with the principal difference between levels 1 and 2, 3 and 4, 5 and 6 being the scope of many of the controls. At the odd numbered levels, the most stringent controls are confined to those parts of the ANSP that support SBC functions, whereas at the even numbered levels most of the controls apply throughout the organization. Odd numbered levels are appropriate where sensitive functions are isolated from the rest of the organization and it is possible to protect them separately.

The second differentiator between levels is the nature of the threat from potential adversaries. The basic level (1, 2) is concerned with low-capability threats, such as those from hackers and criminals with limited expertise and resources. The risks arising from these threats can be mitigated by procedural and management controls and readily available technical products. As the threat agents become more capable, and their targets more attractive, the strength of the controls needs to be increased. Levels 3 and 4 anticipate the need to protect more valuable assets (strictly speaking, more severe impacts) against threats from more sophisticated and better-resourced adversaries, such as those engaged in serious or organized crime, including certain terrorist organizations. The highest levels (5 and 6) are concerned with risks arising from the most capable adversaries, with the resource and expertise normally associated with a nation state.

On this scale we anticipate that many ANSPs, including national Air Traffic Management services, require a level 3 baseline, corresponding to systems whose compromise could result in serious impacts, but where the critical assets are well isolated.

Howard Chivers

2.2. *Example of Assignment of Controls to Risk Levels*

Consider ISO/IEC 27001 A8.1.2 as an example of how risk levels are used to suggest baseline controls. The ISO control requirement is:

“Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.”

The ICT Guidelines specify three levels of rigor in background checking: taking up normal employment references, basic verification checks, and extensive background checks. The last two will usually be specified by national security authorities; for example a basic verification may be a check on criminal records, and an extensive check may be a full background investigation.

The resulting guidance for this control is summarized in **Table 1**, in which these requirements are placed on SBC-specific staff for isolated systems, or all staff where SBC systems are not isolated.

In practice not all controls are amenable to this treatment; however, this example provides an illustration of the general approach used to specify ranked controls.

Table 1 Control Guidance in Proportion to Risk

<i>Risk Level</i>	<i>Summary of guidance for ISO 27001 A8.1.2</i>
1	Employment References, SBC staff
2	Employment References, all staff
3	Basic verification Checks, SBC staff
4	Basic verification Checks, all staff
5	Extensive background verification, SBC staff
6	Extensive background verification, all staff

3. Control Consistency

3.1. *Definition of Consistency*

As a mathematical construct the idea of consistency is concerned with avoiding contradictions between formulae. (For a seminal account see (Church, 1996) section 17). This strict logical consistency is sometimes used to ensure that security policies, such as firewall or access control rules, do not contain contradictions that may suggest a mistaken configuration or lead to unpredictable results. The notion of consistency used here is less formal, being concerned with detecting omissions rather than contradictions, and more in keeping with the informal English definition:

Agreement or harmony of parts or features to one another. (Merriam-Webster)

This idea is important in security because of the holistic nature of the problem. A security auditor tasked with reviewing the quality of a web application will certainly be concerned with access control, but will also care about other factors such as software quality, change control, service continuity, audit facilities, the management of physical

Control Consistency as a Management Tool: The Identification of Systematic Security Control Weaknesses in Air Traffic Management.

access, human factors and compliance to regulatory standards. A significant omission in any of the control areas identified in standards such as ISO/IEC 27002 is likely to provide an easy route into the system regardless of the quality of other controls.

We therefore model the fundamental idea that the security of a system is a function of its weakest component, and that the components belong to diverse categories that are not directly comparable.

Specifically we define:

- A control **Category** to be one of a number of classes of controls (e.g. the 'clauses' in ISO/IEC 27002).
- A control **Level** to be a group of controls within a Category.
- Levels are **ordered** within a category but are not necessarily directly comparable with levels in other categories..
- A control **Baseline** to be a set of Levels, one from each category.

Using these terms our definition of consistency is that:

A control regime is consistent if within every category all controls at the baseline level are present and that there are no missing controls at levels below the baseline.

This paper is concerned with detecting and highlighting consistency problems in control regimes and providing an accessible gap analysis, rather than attempting to provide numerical metrics. However, it should be evident that if controls are ordered in levels, then omissions at the lowest levels are potentially the most serious.

There are several current examples of security control systems in which the controls are ordered in levels, these will be discussed further in section 7.2, below.

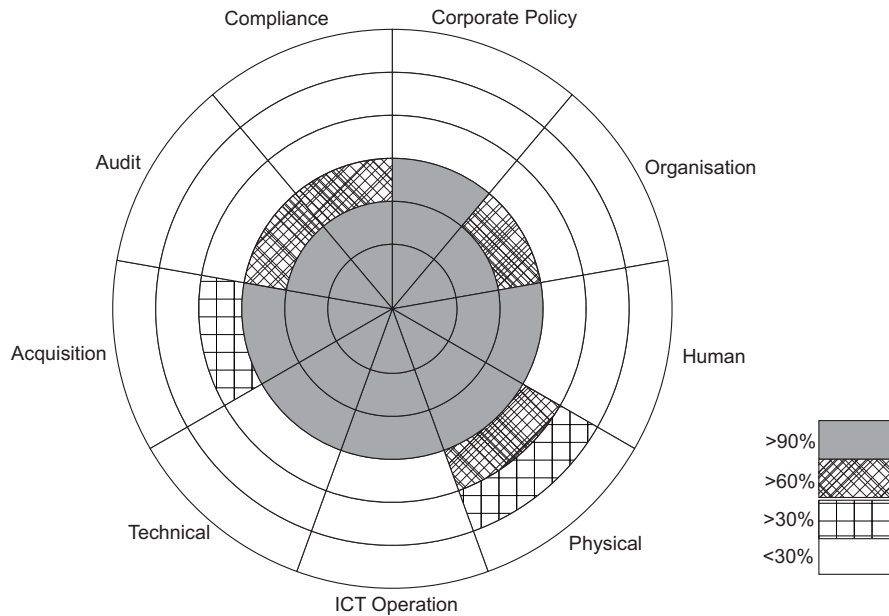
3.2. Visualisation

Spider diagrams are effective in showing the 'high water mark' of various categories of control (e.g. management v operational, v physical) and identifying categories which are generally under or over controlled by comparing the number or percentage of implemented controls in each category. However, we argue that in their usual form they are unable to capture the important concern identified above: missing low-level components.

To meet this need a diagram was developed which showed control coverage in a spider-form, but where the area inside the spider was coloured to show the percentage of controls actually implemented. This provided the same effective visual summary as a normal spider, with the added benefit of showing consistency of control coverage within the overall boundary.

The resulting consistency spider diagram, which also illustrates the expected result for ATM organisations, is shown in Figure 1.

Figure 1. Expected Consistency Spider



Note that categories used in this diagram are similar, but not exactly identical to those in ISO 27001, because the ICT Guidance was required to consolidate requirements from several security standards.

Organisations with an overall risk level of 3 (as expected for Air Traffic Management Services) would be expected to implement all the core controls at this level, although it would be reasonable to expect that in some areas the control treatment would not be complete - not all controls would be applicable to every organisation. For the sake of illustration the figure shows a lower proportion of controls implemented at level 3 for Audit, Compliance and Organisation. This type of incompleteness would merit review. It would also be normal to expect some additional controls; for illustration Figure 1 shows extra controls implemented in the physical and acquisition categories. Controls of this sort may be motivated by security risk analysis, or by other concerns, such as safety. In the case of Air Traffic Management physical controls are often a significant safety consideration and so advanced controls, such as the physical protection of communications cables, may be present for this reason.

This type of presentation provides a more informative summary of the control regime than a standard spider, which would show only the outer boundary, or the overall proportion, of controls implemented.

4. Results

In addition to the ICT guidance which specified control levels a self-assessment questionnaire was developed which allowed organisations to measure their current control profile. The questionnaire and the results of the survey carried out to validate the guidance are described below.

Control Consistency as a Management Tool: The Identification of Systematic Security Control Weaknesses in Air Traffic Management.

4.1. Questionnaire

The purpose of the questionnaire was to allow ANSPs to self-assess their compliance with the ICT Guidance, allowing an organization to develop a two-dimensional model which indicated the degree (in risk level terms) to which ISO/IEC 27001 controls are applied.

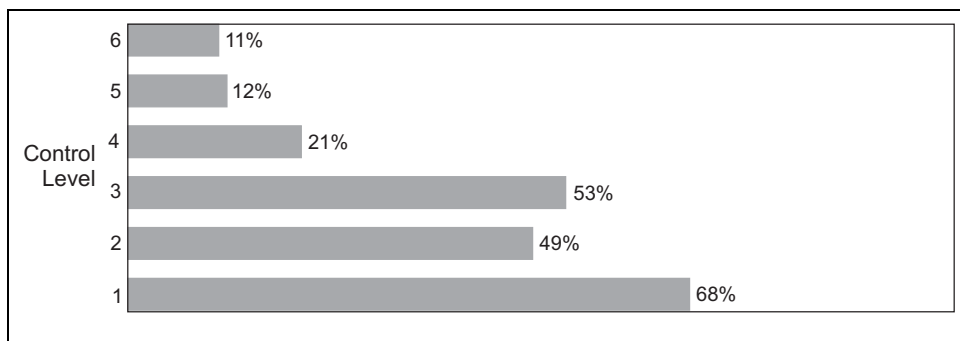
The ICT Guidance and Questionnaire was peer-reviewed by experts at EUROCONTROL and within the broader ATM Security Team. Of more relevance here is the process used in the development of the questionnaire.

The questionnaire was provided to a small volunteer sample of ANSPs in Europe, chosen to represent a range of different size organizations and degree of security maturity. They were asked to attempt to complete the questionnaire; some did so while others provided comments on the questions. Invariably some questions were difficult to interpret and needed to be updated; overall the exercise produced valuable feedback.

4.2. Validation of Risk-Level Approach

Using the survey results it was also possible to numerically test the assessment that a typical ANSP would correspond to a risk level of 3 by measuring the proportion of reported controls at each risk level. The results are presented in Figure 2.

Figure 2 Proportion of Controls Reported at each Risk Level

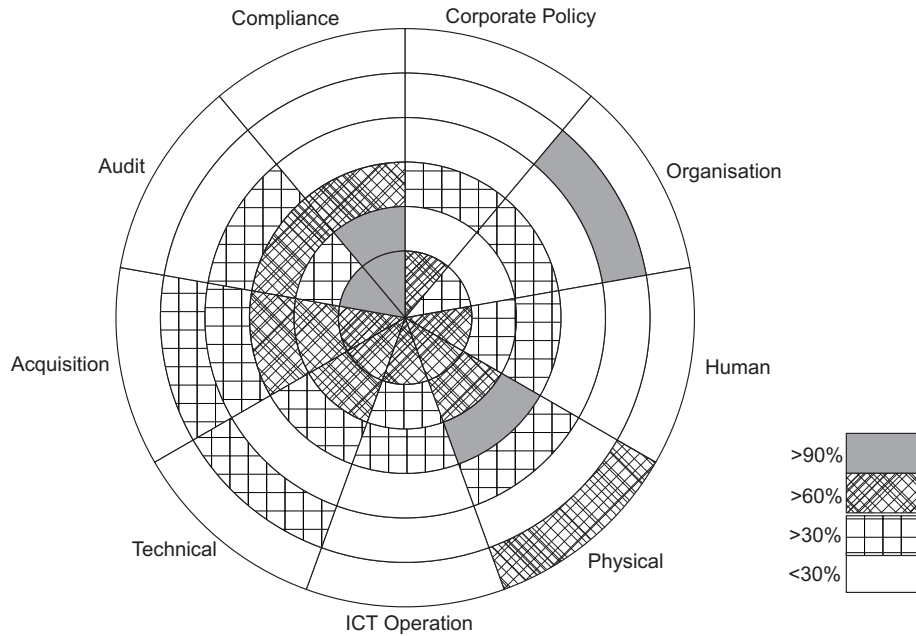


The overall pattern of reported controls in Figure 2 supports this assessment, with a strong proportion of controls appropriate to risk levels 3 and below: systems where the impact of a security incident may be significant, but which are relatively isolated within their organizations.

The reader should bear in mind that baseline controls are supplemented by specific controls derived from an analysis of the actual risks in the environment. As noted above, the presence of a proportion of higher-level controls should therefore be expected. In practice many of these derive from established safety concerns and practices, such as the protection of physical sites and infrastructure.

Plotting these results using the consistency spider resulted in a much more revealing analysis, as shown in Figure 3

Figure 3. Consistency Spider for Combined Survey Results



4.3. Consistency results

The consistency spider in Figure 3 is the sum of all the survey responses, essentially an average control disposition for the Air Navigation Service Providers surveyed. It highlights a wide range of issues associated with the controls actually deployed.

The presence of controls above the level three baseline is expected in organisations where such controls are justified by safety issues, or where additional controls have been selected in response to a risk analysis.

However, Figure 3 suggests that the controls deployed at risk level 3 and below are extremely inconsistent: there are major gaps in the control regime, and these gaps appear in many of the control categories. There are significant gaps in Organisation, Corporate Policy, Human control and ICT Operation categories, and to a lesser degree in other areas.

The anonymous basis of this survey prevents an organisation-by-organisation analysis, but the joint consistency spider shown above provides a strong indication of the power of this approach to identify inconsistencies in control regimes.

The next section will provide more information about exactly what this consistency test suggests in terms of missing controls, while remaining within the bounds of anonymity.

5. Control Review

The questionnaires were completed with no agreement or intention of publication, so the results presented in this paper are limited to identifying common trends in order avoid identifying respondents, or providing statistics from which any respondents may be identified.

Trends are quantified by identifying controls that are missing from all the questionnaire responses. We recognize that this is not as sensitive a test as a more detailed analysis of individual responses; however, the very sparse entries in some of the core control areas in the consistency spider suggests that this approach may be productive. In more detail:

The responses were merged, and controls which were omitted from all of the inputs were identified; these were further filtered to include only controls identified as requirements for risk levels 1-3 in the ICT Guidance. Finally any controls where a respondent queried the interpretation or specificity of a question were removed.

The resulting controls are those appropriate to a wide range of ANSPs (control levels 1-3) but which were missing from the survey responses.

We acknowledge that even if a respondent failed to identify a control it does not necessarily mean that the control was not present; the question may not have been correctly interpreted, or that aspect of the organization may have been outside the knowledge of the individual concerned. This is a further motivation for anonymity; however, identifying controls omitted from all the responses should provide valid candidates for systematic omissions, even if there are occasional errors in the responses.

The results listed in the next section are mapped to associated ISO/IEC 27001:2005 control requirements. The questionnaire used numbered questions which were traceable to paragraphs in the ICT Guidance which were in turn cross-referenced to controls in the standard.

5.1. Results

Controls absent in all the questionnaire responses are presented in three tables below:

- **Table 2** Consistently Missing Management and Organization Controls
- **Table 3** Consistently Missing Technical Controls
- **Table 4** Consistently Missing Incident Management and Business Continuity Controls

Table 2 Consistently Missing Management and Organization Controls

<i>ISO 27001 Annex A/ISO 27002 Control Requirement</i>	<i>Finding</i>
5.1.1 An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.	Policy was not communicated consistently to employees and others. In some organisations a policy was 'available', for example on a security website.
5.1.2 The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	No planned policy reviews were identified.
6.1.1 Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.	No director-level manager was identified with explicit responsibility for security.
6.1.8 The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.	No external/independent reviews were identified.
6.2.1 The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.	No process for assessing the risk of connection to external parties was identified.

The meaning of 'independent' in control 6.1.8 (Table 2) was interpreted as broadly as possible to include any form of fully independent review of the security management system. In particular, it was not judged on the basis of ISO/IEC 27001 certification. There is a potential difficulty in judging independence if no director-level manager is assigned security responsibility, but in the event this problem did not arise.

In Table 2, answers to 6.2.1 were generally blank. Other controls associated with the commissioning of systems or software elicited a range of answers. It is clear that there are well-established processes for testing and commissioning safety-related systems, and some security testing is also conducted. However, there is no evidence of a security accreditation processes: specific decision gates based on the security risk of deployment, enhancement or connection.

Control Consistency as a Management Tool: The Identification of Systematic Security Control Weaknesses in Air Traffic Management.

Table 3 Consistently Missing Technical Controls

<i>ISO 27001 Annex A/ISO 27002 Control Requirement</i>	<i>Finding</i>
12.2.1 Data input to applications should be validated to ensure that this data is correct and appropriate.	These three controls were presented as separate questions, and no evidence was found for systematic validation of input/output data or processing. Virus checking and source authentication of software were quoted as controls that may mitigate malicious corruption of software.
12.2.2 Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	
12.2.4 Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.	
12.3.1 A policy on the use of cryptographic controls for protection of information should be developed and implemented.	No policies were identified, nor key management to support technical controls.
12.3.2 Key management should be in place to support the organization's use of cryptographic techniques.	

In Table 3, it may be a surprise that a cryptographic policy is included at risk level 3. Note that this does not imply that there is any confidential information in a system; for example, key management is necessary to support the authentication of servers to validate data transfer.

Table 4 Consistently Missing Incident Management and Business Continuity Controls

<i>ISO 27001 Annex A/ISO 27002 Control Requirement</i>	<i>Finding</i>
13.2.1 Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.	No evidence was offered for an organised approach to information security incidents.
14.1.1 A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.	No 'explicit and practiced' processes were identified for business continuity

Table 4 reflects the responses accurately; however, some clarification may be helpful. Most ATM organizations have response processes and reserve capacity for some types of incident; for example, loss of mains power, or some types of communication or equipment failure. There are also security-related processes, such as the detection and resolution of the misuse of IT by employees. The missing elements highlighted here are a planned response to information security incidents (13.2.1), or major continuity events such as the loss of a whole centre or major sub-system (14.1.1).

6. Literature Evidence

The survey results suggest weaknesses in several areas of management, in data validation and in incident response. This section reviews other sources to determine if

Howard Chivers

these indicators are supported by external evidence. The most comprehensive primary sources available are US Audit reports which are contemporaneous with the surveys described above, a summary of their evidence is followed by a brief review of known ATM system vulnerabilities.

6.1. US Audit Reports

The US Department of Transportation carries out independent audits on transport services, including Air Traffic Management. A series of reports reviewing major failings in ATM security were published contemporaneously with the survey described above; these failings are summarized in a progress review (2009a); they were:

- “(1) the status of [business continuity] implementation and
- (2) the enhanced methodology used in the certification and accreditation of air traffic control systems security at operational sites.”

The business continuity issue concerned planned contingencies in the event of the failure of a major en-route centre. The reference reports unresolved problems including technical, communications, staffing and funding aspects; the most significant issue, however, is the lack of impact analysis. The capability plan is estimated to achieve: “restoration of 80 percent of any affected en route center’s capabilities within 3 weeks ...” The report notes that the impact on the national service of a three week outage of a major center is unexplored.

A formal accreditation process had been introduced in response to previous audits; however, configuration management of the systems was not sufficient to ensure that accredited systems were deployed in the same configuration as that which had been tested, nor prevent subsequent unauthorized changes. An actual attack is quoted which exploited an unauthorized system configuration to prevent the transfer of flight data in FAA Alaska Region, “forcing FAA to manually provide flight information to pilots flying in that region.”

A major focus of this report is the inadequacy of independent site reviews, which should have detected configuration problems.

The precursor to this report was a general overview of the US Department of Transport security program (2007) which identified the two failings described above. A number of detailed issues were identified, which may be transient (e.g. aviation systems not correctly classified as high-impact), together with a major deficiency in incident reporting:

“During FY 2007, FAA did not report 40 cyber security incidents ... Most of these incidents involved viruses in FAA computers.

... During FY 2006, FAA had to shut down a portion of air traffic control systems because of security events. While FAA did a commendable job in cleaning up the infected computers and enhancing the underlying configuration management controls, it nonetheless reported that ‘no successful cyber events that significantly disabled or degraded our service’ had taken place.”

An earlier report by the US Government Accountability Office (2005b) identifies a wide range of security problems, and ascribes the core problem to security management:

“A key reason for the information security weaknesses that we identified in FAA’s air traffic control systems was that the agency had not yet fully implemented an information security program ...”

Control Consistency as a Management Tool: The Identification of Systematic Security Control Weaknesses in Air Traffic Management.

Finally, a report on FAA web security (2009b) highlights the vulnerability of ATM systems to attacks on webservers, including documenting actual attacks. It concludes that the core deficiency is the need for intrusion detection and incident response.

In summary, these audit reports highlight serious failures in:

- Security Management.
- Business Continuity.
- Incident Management (detection and reporting).
- System accreditation and subsequent configuration control.

Current audits (e.g. (2011a)) focus on a wide range of specific controls. They report progress against some of the previously identified problems, but continue to highlight the difficulty of achieving a fully effective security management system within ATM.

6.2. ATM System Vulnerabilities

The audit reports referenced above describe virus infections that disabled ATM services, and other events where intrusive hacking resulted in the deep access to ATM infrastructure by malicious hackers. Penetration testing also demonstrated the vulnerability of ATM systems to targeted attacks (2009b) and challenges the assumption that ATM operational systems are effectively isolated within their organizations and from Internet-facing servers.

The vulnerability of radio signals, including GPS, to jamming is well known. However, the types of attack that can be achieved as a result of interfering with radio signals are poorly understood. Recent evidence presented in the US (2012) includes an account of a GPS spoofing demonstration carried out by the University of Texas at the White Sands Missile range. A locally generated spoof GPS signal overpowered genuine satellite broadcasts and allowed the manipulation of the flight path of an unmanned helicopter, despite the fact that it remained in communication with its flight controller. Despite known vulnerabilities and a future dependence on high-accuracy timing and position information in civil transport systems, 'limited progress' has been made on backup capabilities to mitigate possible disruption (2013a).

Other ATM protocols are known to be vulnerable to spoofing attacks; for example, researchers have demonstrated the ability to inject false surveillance tracks using spoof ADS-B transmissions (Costin, and Francillon, 2012). Unlike GPS spoofing this attack can be achieved with relatively low-cost and widely accessible components; the authors also reference similar results presented within the hacking community. The scope for the confusion of pilots or controllers by the injection of false tracks is considerable.

In all these cases, the underlying defect is a lack of data validation, whether by poor system configuration in the case of virus and hacking incidents, or by design oversight in the case of ADS-B. Costin and Francillon note:

“The first and simplest thing ... is to add integrity verification to ADS-B messages. If any certified ADS-B device can securely verify validity of other aircrafts' broadcasts ... message injection is suddenly not possible or at least not as easy to accomplish.”

The lack of authentication in aviation data protocols has also been exploited in a demonstration attack which subverted the navigation systems of a standard aircraft simulator (Teso, 2013). In this case spoof messages were injected via the Aircraft Communications Addressing and Reporting System (ACARS). Even if the same

vulnerabilities are not present in operational systems, the method of access - via an unauthenticated protocol - has been demonstrated.

There are two common objections to the need for security controls that are not present in an existing system, such as authentication in new protocols: the need to demonstrate that malicious attacks will actually occur, and the belief that since the system is currently 'secure' then no new controls are needed to ensure its future security. From the security perspective both are based on false premises. Real incidents already occur where unauthenticated voice traffic is used in an attempt to control aircraft. Recordings of real incidents where attackers spoof voice commands leave no doubt about the potential danger of confusing the person who is the last line of defence (2011b), or about the reality of such spoofing attacks. The deliberate use of GPS jammers, resulting in the accidental jamming of nearby GPS avionics systems is also often reported, and has resulted in at least one documented judgment against a perpetrator (2013b).

7. Discussion

7.1. *Contrasting the Consistency approach with Literature Evidence*

Summaries of the core security issues suggested by the survey and those identified in the literature are contrasted in **Table 5**.

Table 5 Comparison of Survey and Literature Issues

<i>Survey Indicators</i>	<i>Literature Evidence</i>
	<i>Management</i>
Senior management responsibility	Lack of Information security program
Policy review	Independent review
Policy communication	Accreditation process and subsequent configuration control.
Independent review	
Accreditation process	
	<i>Technical</i>
Systematic validation of data	Baseline security configuration
Supporting cryptography	Data authentication
	<i>Incident</i>
Incident response	Incident reporting
Business continuity planning	Business continuity planning

It is clear from both sources that deficiencies in essential elements of a security management system are present, although the survey controls (responsibility, review, communication) are more detailed than the non-specific 'lack of program' described in published audits. In both cases it is safe to conclude that security management requires explicit responsibilities and new processes, and cannot be assumed to exist in a mature safety organization.

The other management security issues align exactly between the two sources: lack of independent review, and lack of an accreditation process.

Control Consistency as a Management Tool: The Identification of Systematic Security Control Weaknesses in Air Traffic Management.

In the case of independent review, there is clearly management-level audit in the US – evidenced by the audit reports – but not of the controls in individual organizations. The most recent reports are concerned with detailed control deficiencies, so it is reasonable to assume that more effective control-level review in the US has now been established.

A similar pattern is evident in the lack of an accreditation process: making an explicit security decision about the acceptability of a new system, upgrade or connection. The literature records that this process was initially absent, but when introduced it failed to defend actual attacks because of a lack of other controls, in this case system configuration management.

Lack of data validation is a common theme in vulnerability analysis; in the examples quoted a critical factor is the authentication of the source of data used in ATM. The design of protocols without authentication, particularly when they are used over public or broadcast networks, is a blatant disregard of the likely safety impact of types of attack that are already known to take place.

Finally, both sources identify business continuity management and incident management as issues. The business continuity management problem is a lack of resilience and understanding in the face of major events such as loss of a complete centre. The sources do not provide enough information to be sure that the incident management issues are identical; however, both indicate the absence of a working incident management process.

With reference to Figure 3, it is obvious that this analysis has not identified all of the control weaknesses in the organizations surveyed. The combined survey results in Figure 3 suggest further problems in organization, human factors, and ICT operations. However, the approach taken above has identified the common deficiencies, other weaknesses are therefore related to individual organizations, and although important, are outside the scope of this report.

In conclusion, there is a clear alignment between the major issues suggested by the survey, and those that are found in the literature. The issues summarized in Table 5 should be regarded as probable core security deficiencies in ATM organizations, until an explicit management focus on security is achieved.

7.2. Applicability to other Control Standards

While risk assessment is still the primary mechanism for deciding the value of controls and evaluating the overall need for security, baseline-oriented systems which specify minimum security requirements and rank controls into levels are becoming increasingly important. Security standards that embody this approach include FIPS 200 (FIPS PUB, 2006) which uses a high-level impact assessment to specify a control baseline from one of three layers defined in NIST 800-53 (NIST SP, 2007), and a range of standards that define organizational maturity in layered terms.

The best established maturity approaches are related to software development where the levels range from ad-hoc development to predictable process-oriented management. A security-related maturity model for software is maintained by the Building in Security Maturity Model (McGraw et al., 2010) community. In this model activities are reported which support 12 different categories in three maturity layers.

A recent development is the CyberSecurity Capability Maturity Model based on work in the U.S. energy sector (U.S. Department of Energy, 2014). From the perspective of this paper it is another example of a system of categories with defined levels in which consistency, as defined here, is a required property.

The trend toward security control systems which are layered with defined baselines suggests that the approach described here is directly applicable in a wide range of current security applications.

8. Conclusions

This paper has introduced control consistency as a means of reviewing and communicating information about the set of controls in a management system. Its use in the analysis of a survey of European Air Navigation Service Providers prompted a review of common deficiencies in their control regimes. Since confidentiality restricts what can be said about the original surveys these results can only be regarded as indicative, so the paper contrasts these findings with a review of other evidence from the literature, in particular contemporaneous audit reports on security in US ATM systems. The two different sources are in close agreement, suggesting that the consistency approach is effective in identifying systematic security defects.

The key issues are listed in Table 5; they include security management and senior management engagement, system accreditation, the validation and authentication of data used by ATM systems, incident management, and business continuity preparedness. The evidence suggests that these may be systematic deficiencies in Air Traffic Management security.

Acknowledgment

We are grateful to EUROCONTROL for permission and encouragement to publish the limited account of the survey information contained in this paper.

References

- European Commission. (2005a) *Common Requirements for the Provision of Air Navigation Services*, (Regulation No 2096/2005).
- International Organisation for Standards (ISO) (2005) *ISO/IEC 27001:2005: Information Technology - Security Techniques - Information Security Management Systems - Requirements*
- A. Church (1996) *Introduction to Mathematical Logic*, Princeton University Press.
- Federal Aviation Administration. (2009a) *Review of FAA's Progress in Enhancing Air Traffic Control System's Security*, (FI-2010-006), https://www.oig.dot.gov/sites/default/files/ATC_BCP-_Final_Report_11-03-2009.pdf. (Accessed October 2015)
- United States Department of Transportation. (2007) *Information Security Program*, (FI-2008-001), https://www.oig.dot.gov/sites/default/files/FISMA__508_Compliant.pdf. (Accessed October 2015)
- United States Government Accountability Office. (2005b) *Information Security*, (GAO-05-712), <http://www.gao.gov/products/GAO-05-712>. (Accessed October 2015)
- Federal Aviation Administration. (2009b) *Review of Web Applications Security and Intrusion Detection in Air Traffic Control systems*, (FI-2009-049), https://www.oig.dot.gov/sites/default/files/ATC_Web_Report.pdf. (Accessed October 2015)
- United States Department of Transportation. (2011a) *FISMA 2011: Persistent Weaknesses in DOT's Controls Challenge the Protection and Security of its Information Systems*, (FI-2012-007), <https://www.oig.dot.gov/sites/default/files/FISMA%2011-14-2011.pdf>. (Accessed October 2015)
- (2012) 'Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing', *Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security*.

Control Consistency as a Management Tool: The Identification of Systematic Security Control Weaknesses in Air Traffic Management.

- U.S. Government Accountability Office. (2013a) *GPS Disruptions: Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced*,(GAO-14-15), <http://www.gao.gov/assets/660/658792.pdf>. (Accessed October 2015)
- A. Costin and A. Francillon, (2012), 'Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices'.Paper Presented at *Black Hat USA 2012*.
- H. Teso, (2013), 'Aircraft Hacking'.Paper Presented at *Hack in the Box Security Conference*,
<http://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf>. (Accessed October 2015)
- '25-May-2011 Fake ATC in Action (LTBA-ISTANBUL)' [online]
<http://www.liveatc.net/forums/atcaviation-audio-clips/25-may-2011-fake-atc-in-action-%28ltba-istanbul%29> (Accessed October 2015).
- (2013b) 'NOTICE OF APPARENT LIABILITY FOR FORFEITURE', in Federal Communications Commission (Ed.), *FCC 13-106*, Whitehouse Station, New Jersey.
- FIPS PUB (2006): *200, Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP (2007): *800-53, Recommended Security Controls for Federal Information Systems*
- G. McGraw, et al. (2010) 'Building Security In Maturity Model BSIMM v2. 0', <http://www.bsimm.com/>.
- U.S. Department of Energy (2014) 'CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)', http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.