INTERNATIONAL CIVIL AVIATION ORGANIZATION
ASIA and PACIFIC OFFICE

Aeronautical Telecommunication Network
Implementation Coordination Group
(ATNICG)

ASIA/PAC
RECOMMENDED SECURITY CHECKLIST

September 2009

Prepared by
ATN ICG Security Sub-Group and

Adopted by APANPIRG/20

Document Revision History

Release	Date	Comment
Draft 1	21 April 2008	Controls from NIST SP 800-53 Identified
Draft 2	25 September 2008	Controls in checklist format
Version 1	4 May 2009	Checklist reduced to policy and essential check item(s) in each control family

Table of Contents

1 Introduction

1.1 Motivation

The Asia/Pacific Region is implementing the Aeronautical Telecommunication Network (ATN) infrastructure in support of the ATN Message Handling Service (AMHS). In order to ensure that security measures are implemented throughout the Asia/Pac ATN, a comprehensive checklist is needed. The ATNICG Security Sub-Group decided at the first sub-group meeting in April 2008 to base the checklist on the list of security controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (SP800-53) [1].

This paper aims to provide a set of security controls in the form of a checklist. The goal is to describe each security control in a fashion suitable for an organization to verify that a set of controls sufficient for their operating environment has been implemented in accordance with the Asia/Pacific System Security Policy [2]. This checklist may be used as the basis of an organization's *verification* that their system is implemented with appropriate security measures. With this checklist filled in the organization's Designated Approving Authority (DAA) can provide *authorization* that the system may be placed into operation.

1.2 References

The following documents were used in the preparation of this paper.

[1] National Institute of Standards and Technology. Special Publication 800-53. Recommended Security Controls for Federal Systems. February 2005. Currently available from: http://csrc.nist.gov/publications/nistpubs/index.html.

[2] Asia/Pacific ATN System Security Policy, 2nd Edition, May 2008

2 Security Control Overview

Table 2-1 is a summary list of the control classes and families. Each control family is classified as a Management, Operational, or Technical Control.

Table 2-1. Security Control Classes and Families

Class	Family	Identifier
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Each family comprises one or more security controls. Each security control is sequentially numbered within the family. The following subsections describe the structure of the security controls and the organization of the security controls into baselines.

3 Catalogue of Security Control Requirements

Table 3-1 identifies the developed security checklist.

The ID column provides the security checklist identifier. It can be used to trace the security checklist item back to its control family. To enable traceability to the security controls, each security checklist item is assigned an identifier based on the identifier of the security control family.

The Security Checklist Text column contains the language for each checklist item.

The Implemented column is where an organization may indicate compliance with the checklist item.

The Comment column provides any additional information noted during the assessment of the particular item.

Table 3-1. Security Checklist

ID	Security Checklist Text	Implemented (Yes/No)	Comment
	ACCESS CONTROL (AC)		CLASS: TECHNICAL
	ACCESS CONTROL POLICY		
AC.1	Does the organization have a formal, documented, access control policy?		
	ACCOUNT MANAGEMENT		
AC.2	Does the organization manage system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts?		
	ACCESS ENFORCEMENT		
AC.3	Does the system enforce assigned authorizations for controlling access to the system in accordance with applicable policy?		
	SUPERVISION AND REVIEW — ACCESS CONTROL		
AC.4	Does the organization review the activities of users with respect to the enforcement and usage of system access controls?		
	REMOTE ACCESS		
AC.5	Does the organization document, monitor, and control all methods of remote access (e.g., dial-up, Internet) to the system?		
	AWARENESS AND TRAINING (AT)		CLASS: OPERATIONAL
	SECURITY AWARENESS AND TRAINING POLICY		
AT.1	Does the organization have a formal, documented, security awareness and training policy?		
	SECURITY TRAINING		
AT.2	Does the organization provide basic security awareness training to all users?		
	AUDIT AND ACCOUNTABILITY (AU)		CLASS: TECHNICAL
	AUDIT AND ACCOUNTABILITY POLICY		
AU.1	Does the organization have a formal, documented, audit and accountability policy?		
	AUDITABLE EVENTS		
AU.2	Does the system generate audit records for the significant security events?		
	AUDIT MONITORING, ANALYSIS, AND REPORTING		
AU.3	Does the organization regularly review/analyze audit records for indications of inappropriate or unusual activity?		

ID	Security Checklist Text	Implemented (Yes/No)	Comment
	CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS (CA)		CLASS: MANAGEMENT
	CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICY		
CA.1	Does the organization have a formal, documented, security assessment and verification and accreditation policy?		
	SECURITY CERTIFICATION		
CA.2	Does the organization conduct an assessment of the security controls in the system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system?		
	SECURITY ACCREDITATION		
CA.3	Does the organization authorize (i.e., accredit) the system for processing before operations?		
	CONFIGURATION MANAGEMENT (CM)		CLASS: OPERATIONAL
	CONFIGURATION MANAGEMENT POLICY		
CM.1	Does the organization have a formal, documented configuration management policy?		
	CONFIGURATION CHANGE CONTROL		
CM.2	Does the organization control changes to the system?		
	CONTINGENCY PLANNING (CP)		CLASS: OPERATIONAL
	CONTINGENCY PLANNING POLICY		
CP.1	Does the organization have a formal, documented contingency planning policy?		
	CONTINGENCY PLAN		
CP.2	Does the organization develop a contingency plan?		
	SYSTEM BACKUP		
CP.3	Does the organization conduct backups of user-level and system-level information?		

ID	Security Checklist Text	Implemented (Yes/No)	Comment
	IDENTIFICATION AND AUTHENTICATION (IA)		CLASS: TECHNICAL
	IDENTIFICATION AND AUTHENTICATION POLICY		
IA.1	Does the organization have a formal, documented identification and authentication policy?		
	USER IDENTIFICATION AND AUTHENTICATION		
IA.2	Does the system uniquely identify users (or processes acting on behalf of users)?		
IA.3	Does the system authenticate users (or processes acting on behalf of users)?		
	DEVICE IDENTIFICATION AND AUTHENTICATION		
IA.4	Does the system identify specific devices before establishing a connection?		
IA.5	Does the system authenticate specific devices before establishing a connection?		
	INCIDENT RESPONSE (IR)		CLASS: OPERATIONAL
	INCIDENT RESPONSE POLICY		
IR.1	Does the organization have a formal, documented incident response policy?		
	INCIDENT HANDLING		
IR.2	Does the organization implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery?		
	MAINTENANCE (MA)		CLASS: OPERATIONAL
	SYSTEM MAINTENANCE POLICY		
MA.1	Does the organization have a formal, documented system maintenance policy?		
	CONTROLLED MAINTENANCE		
MA.2	Does the organization perform routine preventative and regular maintenance on the components of the system?		
	MEDIA PROTECTION (MP)		CLASS: OPERATIONAL
	MEDIA PROTECTION POLICY		
MP.1	Does the organization have a formal, documented media protection policy?		

ID	Security Checklist Text	Implemented (Yes/No)	Comment
	MEDIA ACCESS		
MP.2	Does the organization restrict access to system media to authorized individuals?		
	MEDIA STORAGE		
MP.3	Does the organization physically control system media within controlled areas?		
	PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)		CLASS: OPERATIONAL
	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY		
PE.1	Does the organization have a formal, documented physical and environmental protection policy?		
	PHYSICAL ACCESS CONTROL		
PE.2	Does the organization control all physical access points to facilities containing systems?		
	EMERGENCY POWER		
PE.3	Does the organization provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the system in the event of a primary power source loss?		
	FIRE PROTECTION		
PE.4	Does the organization employ and maintain fire suppression and detection devices/systems that can be activated in the event of a fire?		
	PLANNING (PL)		CLASS: MANAGEMENT
	SECURITY PLANNING POLICY		
PL.1	Does the organization have a formal, documented security planning policy?		
	SYSTEM SECURITY PLAN		
PL.2	Does the organization develop and implement a security plan for the system?		
	PERSONNEL SECURITY (PS)		CLASS: OPERATIONAL
	PERSONNEL SECURITY POLICY		
PS.1	Does the organization have a formal, documented personnel security policy?		
	PERSONNEL SCREENING		

ID	Security Checklist Text	Implemented (Yes/No)	Comment
PS.2	Does the organization screen individuals requiring access to organizational information and systems?		
	RISK ASSESSMENT (RA)		CLASS: MANAGEMENT
	RISK ASSESSMENT POLICY		
RA.1	Does the organization have a formal, documented risk assessment policy?		
	RISK ASSESSMENT		
RA.2	Does the organization conduct assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and systems that support the operations and assets of the organization?		
	VULNERABILITY SCANNING		
RA.3	Does the organization scan for vulnerabilities in the system?		
	SYSTEM AND SERVICES ACQUISITION (SA)		CLASS: MANAGEMENT
	SYSTEM AND SERVICES ACQUISITION POLICY		
SA.1	Does the organization have a formal, documented system and services acquisition policy?		
	ALLOCATION OF RESOURCES		
SA.2	Does the organization determine, document, and allocate as part of its capital planning and investment control process the resources required to adequately protect the system?		
	SYSTEM AND COMMUNICATIONS PROTECTION (SC)		CLASS: TECHNICAL
	SYSTEM AND COMMUNICATIONS PROTECTION POLICY		
SC.1	Does the organization have a formal, documented system and communications protection policy?		
	DENIAL OF SERVICE PROTECTION		
SC.2	Does the system protect against or limit the effects of denial of service attacks?		
	BOUNDARY PROTECTION		
SC.3	Does the system monitor and control communications at the external boundary of the system and at key internal boundaries within the system?		
	TRANSMISSION INTEGRITY		

ID	Security Checklist Text	Implemented (Yes/No)	Comment
SC.4	Does the system protect the integrity of transmitted information?		
	TRANSMISSION CONFIDENTIALITY		
SC.5	Does the system protect the confidentiality of transmitted information?		
	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT		
SC.6	Does the system employ automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management?		
	PUBLIC KEY INFRASTRUCTURE CERTIFICATES		
SC.7	Does the organization develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the system?		
	SESSION AUTENTICITY		
SC.8	Does the system provide mechanisms to protect the authenticity of communications sessions?		
	SYSTEM AND INFORMATION INTEGRITY (SI)		CLASS: OPERATIONAL
	SYSTEM AND INFORMATION INTEGRITY POLICY		
SI.1	Does the organization have a formal, documented system and information integrity policy?		
	FLAW REMEDIATION		
SI.2	Does the organization identify, report, and correct system flaws?		
	MALICIOUS CODE PROTECTION		
SI.3	Does the system implement malicious code protection that includes a capability for automatic updates?		
	SYSTEM MONITORING TOOLS AND TECHNIQUES		
SI.4	Does the organization employ tools and techniques to monitor events on the system, detect attacks, and provide identification of unauthorized use of the system?		
	SECURITY ALERTS AND ADVISORIES		
SI.5	Does the organization receive system security alerts/advisories on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response?		
	SOFTWARE AND INFORMATION INTEGRITY		

ID	Security Checklist Text	Implemented (Yes/No)	Comment
SI.6	Does the system detect and protect against unauthorized changes to software and information?		
	SPAM AND SPYWARE PROTECTION		
SI.7	Does the system implement spam and spyware protection?		