OCCAR Management Procedure

Title:	**CIS Security Requirements for OCCAR Restricted Information**
Number:	Annex OMP 11-F Date: 13/06/17
Computer Ref:	Annex OMP 11-F_CIS Security Requirements RESTRICTED_Issue1_20170613
Current status:	Issue 1
:	
Contact address:	Central Office, OCCAR-EA Bonn Email: questions@occar.int

Approved for issue:	OCCAR File Ref: CO/PMSD/2017/00182

This document replaces: N/A

Record of changes

Date	Issue	Changes
13/06/17	Issue 1	Initial issue

Table of Contents

0. Introduction

The protection of Classified Information within OCCAR Communication and Information Systems (CIS) relies upon the balanced and proportionate application of measures designed to control and reduce the likelihood of information compromise.

This Annex draws upon the variation and diversity of CIS Security measures already established within the National CIS Security Policies of OCCAR Member States to define a set of personnel, physical, procedural and technical security controls that establishes a common minimum standard for the protection of OCCAR RESTRICTED information within CIS across all OCCAR stakeholders.

The defined security controls fall under the following general themes:

1. Identification and Authentication;
2. Access Control;
3. Security Audit;
4. Protection against Malicious Software;
5. Mobile Code;
6. Configuration Management;
7. Security Management;
8. Handling of Information and Removable Media;
9. Assurance of Security Enforcing Functions;
10. Electronic Transmission of OCCAR RESTRICTED information;
11. Physical Security;
12. Security Testing;
13. Vulnerability Assessment;
14. Security Awareness and Training;
15. Wireless LAN;
16. Virtualisation;
17. Maintenance;
18. Incident Management;
19. Sanitisation and Destruction;
20. Testing Tools;
21. Interconnection Requirements.

CIS Security Baseline Control Set

In the context of these Security Regulations, the term "baseline" is used to accommodate an element of inferred flexibility regarding the application of a minimum standard of controls; while the intention is for all controls to be applied to all CIS, there may be cases

where some controls are either not applicable or not appropriate. Where such conflicts arise, individual controls may be waivered for specific CIS upon documented agreement of the Security Accreditation Authority (SAA).

To aid in this activity, a number of requirements have already been identified as being potentially inappropriate for some CIS; these are highlighted with a grey background, and their relevance should be ascertained through discussion with the SAA of each CIS as early as possible in the planning phase of the CIS project.

An extra column is provided to the right-hand side of each control which can be used as a checklist by SAAs or Planning and Implementation Authorities (PIAs) to define or acknowledge what controls have been implemented within a CIS.

A set of example requirements is shown in the table below:

ID	Requirement	✓
0.1	These requirements are the baseline for all CIS handling OCCAR RESTRICTED information.	
0.2	These requirements apply for CIS handling OCCAR RESTRICTED, if required by an SAA. These optional requirements have a split tick box allowing the SAA to indicate whether compliance is necessary.	

1. Identification and Authentication

ID	Requirement	✓
1.1	An up-to-date list of authorised users shall be maintained by security administrators.	
1.2	User accounts with privileges (for System or Security Administrators, for example) shall be distinguished from normal user accounts and strictly controlled.	
1.3	All users shall be uniquely identified through the issue of personal account credentials prior to use of the CIS.	
1.4	All users shall be authenticated by the CIS before any access to it is granted.	
1.5	User accounts and passwords shall be generated in accordance with a scheme developed for the system, as stated in the security documentation.	
1.6	The use of previously-used passwords shall be prevented.	
1.7	All passwords shall have a minimum time-period of validity in order to deter deliberate changes, thus negating the effect of requirement 1.6.	
1.8	Passwords shall be changed whenever they have, or are suspected to have been compromised or disclosed.	
1.9	Administrator passwords shall be stored in a protected manner for emergency access (e.g. sealed in envelopes, locked in appropriate security containers), as defined in the security documentation.	

ID	Requirement	✓
1.10	When the authentication of a user is not established when entering the area in which a CIS will be operated, two-factor authentication shall be used (when using Mobile Devices in unsecured environments, for example).	
1.11	Passwords for system access shall be protected as OCCAR RESTRICTED documents in accordance with the security documentation.	
1.12	The CIS shall provide only limited feedback to the user during the authentication process so as not to inform which aspect of authentication was incorrect.	
1.13	Accounts that are no longer required shall be locked or deleted.	
1.14	Clear-text user passwords shall not be included in any automated log-in procedure. I.e. the CIS username and password shall not be stored on the CIS device itself, even for the purpose of auto-login: only the HASH of the password should be stored on a CIS. For auto-login, legitimate user-authenticated tokens should be used (such as Single Sign On).	
1.15	Security and system administrators shall define a list of events for which a user shall require re-authentication. For example, after a given time.	
1.16	When not in use, two-factor authentication tokens shall be kept separate from any CIS they relate to.*	
1.17	CIS shall be able to terminate the authentication process for a particular user after an inappropriate number of failed login attempts. The system shall be able, after such termination, to lock the user account or the point of entry from which the attempts were made until an administrator-defined condition occurs. The security management staff shall implement a process to unlock the user account.	
1.18	All passwords shall have a minimum length of 9 characters, with a maximum time-period validity of 180 days (where there is a single authentication mechanism in place)**.	
1.19	System Operating Authorities shall have an approved process in place to control physical access to their respective CIS environments.	

* Determined by a valid security risk assessment in consultation with the SAA.
** The maximum validity may be less, where determined by a valid security risk assessment, and may be longer if additional authentication mechanisms are implemented.

2. Access Control

ID	Requirement	✓
2.1	Privilege-based mechanisms shall be implemented to restrict user access to only the information required to support a given programme or other OCCAR-related activity based on business requirements, taking into account the need-to-know principle.	

ID	Requirement	✓
2.2	Identification and Authentication data shall be used by the system to determine user privileges, in accordance with the access control requirements set out in the security documentation.	
2.3	Each user account shall be accessible by only one individual, such that it shall be possible for the security management staff to identify the actions of specific users and/or roles.	
2.4	Access to security and system information shall be restricted to only authorised security and/or system administrators.	
2.5	The CIS Security Functions shall lock interactive sessions after a specified period of user inactivity, by clearing the screen or overwriting display devices, making the current contents unreadable and by disabling any of the user's data access / display devices other than unlocking the session.	
2.6	The CIS Security Functions shall allow user-initiated locking of the user's own session, as defined by 2.5.	
2.7	Security mechanisms and/or procedures to regulate the introduction or connection of removable storage media to CIS assets shall be implemented.	
2.8	Before establishing a user session, a notice shall be displayed indicating that only authorised users are permitted to access the CIS and that activity will be monitored.	
2.9	CIS and storage media used to store, forward, or process OCCAR RESTRICTED Information, shall be physically protected against unauthorised access in accordance with requirements in para. 8 and 11.	
2.10	Wherever possible, Full-device FIPS-140 approved encryption systems shall be used to protect data-at-rest within Mobile Devices and removable storage media. Where Member Nation-approved certification or evaluation exists, equipment may be downgraded in classification as specified in the associated evaluation/certification documentation of the encryption system in use.	
2.11	CIS shall only be connected to printers within a controlled environment, as defined in the security documentation	

3. Security Audit

ID	Requirement	✓
3.1	An audit log of security events shall be generated and maintained. System Level, Application Level and User Level events shall be included in the log, as detailed in the Security Documentation. For each of the auditable events, it shall record: ▪ Individual user identities; ▪ Date and time of the event; ▪ Type of event; ▪ The outcome (success or failure) of the event.	

ID	Requirement	✓
3.2	The security events to be addressed in the accounting and audit shall be as set out in the security documentation. This shall include, at the very least: ▪ All log on and log off attempts; ▪ Initial creation, changes and withdrawal of access rights/privileges; ▪ Initial creation and changes to passwords; The delay before destruction of the audit record shall be stated in the security documentation.	
3.3	The audit trail and associated archive shall be protected from unauthorised deletion and/or modification; it shall be presented in human-readable format directly (e.g., storing the audit trail in human-readable format), indirectly (e.g., using audit reduction tools) or both.	
3.4	The audit trail and associated archive shall be protected from accidental deletion or modification in the event of system failure.	
3.5	Access to audit information shall be controlled; access permissions shall be established to permit access only by the appropriate management staffs.	
3.6	A means shall be available to analyse and review system activity and audit data, looking for possible or real security violations (analysis may work in support of intrusion detection/ automatic response to an imminent security violation).	
3.7	The use of security tools to analyse and review audit data shall be in accordance with the requirements set out in para. 20 "Testing Tools".	
3.8	The audit data shall be retained for a specified period of time agreed by SAA.	
3.9	The Security Functions shall be able to provide reliable time stamps in order to support the required accounting and audit processes. Alteration of the system time reference shall be an administration function.	
3.10	Response mechanisms and/or associated actions, based upon security alarms, shall be initiated in case a potential security violation is detected. These may include the generation of real-time alarms, termination of offending processes, disabling of a service, or disconnection or invalidation of a user account.	
3.11	New connections, or connections discovered during routine testing, shall be reported to the appropriate SAA.	

4. Protection against Malicious Software

ID	Requirement	✓
4.1	Virus/malicious code detection software shall be installed on all servers, portable computing devices and workstations dependent upon the vulnerability of the underlying operating system environment. It shall be configured to automatically check on the introduction of removable media (e.g., CDs, USB mass storage devices, flash memory).	

ID	Requirement	✓
4.2	The virus/malicious code detection software shall be regularly updated as defined in the security documentation.	
4.3	Use or installation by users of unauthorised software not part of an agreed configuration baseline defined in the security documentation shall be prohibited.	
4.4	Downloading of system software shall only be permitted by a system administrator, from trusted sources as defined in the security documentation.	
4.5	New or modified versions of software (for example: operating systems, subsystems, software packages and applications) shall be checked for the presence of any malicious software before being introduced into the system. Such checks shall, wherever possible, be conducted in a stand-alone environment. When software is developed by a trusted source in a secure environment and delivered via a trusted method, this check may not be necessary.	
4.6	Incoming e-mail, files, media and other exchanged data types shall be checked for the presence of malicious code. This check shall be carried out using appropriate software either on an isolated system or on each appropriate server and/or workstation as defined in the security documentation. Encrypted data that cannot be inspected at the boundary of an interconnection shall be checked for malicious code at the point of decryption.	

5. Mobile Code

ID	Requirement	✓
5.1	The use of mobile code – executable content that runs within or above a framework that allows it to easily move across platforms or execution mechanisms (for example, embedded macros, Javascript, Java Applets, or Microsoft.NET applications) which may run natively, within a browser, or as part of other applications – shall be subject to approval by the security approval or accreditation authority.	
5.2	The source of the mobile code shall be appropriately verified.	
5.3	The integrity of the mobile code shall be appropriately verified.	
5.4	All mobile code shall be verified as being free from malicious software.	
5.5		

ID	Requirement	✓
	Available technical measures shall be enabled to ensure the use of mobile code is appropriately managed. For example, Microsoft Office applications and Internet Browser applications shall be configured to control; 1. Import/acceptance of mobile code; 2. Use and creation of mobile code.	

6. Configuration Management

ID	Requirement	✓
6.1	A detailed hardware and software configuration control system (including system and network diagrams) shall be available and regularly maintained.	
6.2	Configuration baselines (including available services) shall be established for servers, LAN Components, Portable Computer Devices (PCDs) and workstations.	
6.3	Configuration checks shall be made by appropriate Security Management staff on hardware and software to ensure that unauthorised hardware and software has not been introduced.	
6.4	An inventory of hardware and software shall be maintained, with equipment and cabling labelled as part of the inventory.	
6.5	The configuration of the security enforcing and security relevant functions of the operating system shall only be subject to change by a limited number of authorised and appropriately cleared system and security administrators.	
6.6	The security configuration of the operating system shall be maintained with the implementation of the appropriate security patches and updates. Regression aspects i.e. any potential adverse affects of the modification on existing security measures shall be considered and appropriate action taken.	
6.7	The installation and configuration of application software with security-relevant or security-enforcing functions shall be subject to a limited number of authorised system and security administrators.	
6.8	The configuration of the operating system shall be subject to periodic checks to ensure its security compliance.	
6.9	Changes to the system or network configuration shall be assessed for their security implications / impacts.	
6.10	The Basic Input / Output System (BIOS) or similar firmware shall be password protected in order to protect access to the system. The strength of the password selected shall be commensurate with the information it is protecting.	

7. Security Management

ID	Requirement	✓
7.1	The System's Security Documentation shall be validated by the SAA as part of CIS Security Accreditation before being authorised to store, forward, or process OCCAR RESTRICTED Information.	
7.2	Mechanisms shall be implemented which manage security functions and security-relevant data, which may only be performed or accessed by defined and authorised users (or roles).	
7.3	CIS Security incidents shall be reported for inspection and investigation purposes in accordance with the security documentation.	
7.4	PCDs shall indicate discreetly to the user the highest classification of information that may be handled.	
7.5	Backup, recovery and business continuity requirements for CIS shall be defined within the security documentation, along with their implementation procedures.	
7.6	CIS users do not require a minimum national security clearance to access OCCAR RESTRICTED information; however they must sign a declaration of understanding and compliance with any user-specific Security Operating Procedures.	

8. Handling of Information & Removable Media

Removable Media is a term that describes any computer storage device designed to be removed from a computer without powering it down or affecting its operating state. It is a term that includes CDs, DVDs, Blu-Ray Disks, Camera memory cards (SD Card, Memory Stick etc), and the various types of storage device (Pen Drives, Hard Drives, Mobile Phones, Tablets etc) compatible with the Universal Serial Bus (USB), FireWire (IEEE 1394) and Intel/Apple Thunderbolt interfaces.

ID	Requirement	✓
8.1	Electronic versions of Documents or other forms of electronic records containing OCCAR RESTRICTED information shall be classified and marked with the words "OCCAR RESTRICTED" in accordance with the Programme Security Instructions or Security Classification Guides.	
8.2	Removable media used to store OCCAR RESTRICTED shall be marked with the words "OCCAR RESTRICTED" in black writing, in such a manner that any recipient shall know it contains OCCAR RESTRICTED information (on the Material itself or on the container holding the Material).	
8.3	Reusable removable media that has been used to store or transport OCCAR RESTRICTED information shall retain the marking "OCCAR RESTRICTED" and shall continue to be treated as OCCAR RESTRICTED material until it is securely disposed of – even if all Classified Information is removed from it.	

9. Assurance

The purpose of assurance is to obtain confidence that the security functions of a system meet or adhere to applicable standards. This is achieved through independent evaluation and certification of products through schemes such as Common Criteria (CC) or equivalent Member State evaluation processes.

Use of CC evaluated security products in accordance with the requirements below ensures OCCAR CIS meet minimum security functionality and assurance requirements.

ID	Requirement	✓
9.1	The minimum assurance level associated with the Identification and Authentication, Access Control and Security Audit functions of Operating Systems, based upon the Evaluation Assurance Levels (EALs) of the Common Criteria (or national/international equivalent) shall be EAL2. The relevant Security Target and/or Protection Profile shall be consulted for compliance of individual products. This may be increased in consultation with the SAA.	
9.2	Service Level Agreement (SLA) information (e.g. availability, performance, quality of service, data priority etc) shall be defined within the security documentation.	
9.3	Backup, recovery and business continuity requirements for CIS and their associated procedures shall be defined in the security documentation.	

10. Electronic Transmission of OCCAR RESTRICTED Information

ID	Requirement	✓
10.1	OCCAR RESTRICTED Information shall not be transmitted via public network (e.g. by telephone, fax, Video Tele-Conferencing, E-mail, or via online services such as FTP, HTTP, telnet or their secured variants SFTP, HTTPS and SSH) unless an encryption system is used whose operational configuration has been approved in accordance with requirements 10.2 – 10.4. Where exceptional urgent circumstances apply, Telephone conversations, video conferences, and facsimile transmissions containing OCCAR RESTRICTED Information may be conducted in clear text, subject to the following conditions: ▪ an encryption system satisfying requirements 10.2 – 10.4 is not available, and; ▪ time is of paramount importance, and; ▪ Unencrypted transmission of OCCAR RESTRICTED Information is not explicitly prohibited for the given OCCAR Programme or activity.	
10.2	For the transmission of Classified Information within the territory of a Member State, encryption products shall be used whose configuration has been approved by the Member State's NSA/DSA.	

ID	Requirement	✓
10.3	The international transmission of OCCAR RESTRICTED Information to non-Member States shall comply with the relevant Security Agreements.	
10.4	For the international transmission of OCCAR RESTRICTED Information between Member States, encryption products shall be used whose configuration has been evaluated and added to the list of products approved for the encryption of OCCAR RESTRICTED Information by an OCCAR Member State's NSA or DSA.	

11. Physical Security

ID	Requirement	✓
11.1	Where persistent storage (such as hard disks and removable media) holding Classified Information relating to a programme cannot be physically protected in accordance with OMP 11 para. 13, an encryption product shall be used that has been approved by at least one, and accepted by all other Programme Participating States participating in the Programme.	
11.2	Any encryption products shall be handled in accordance with the security operating procedures issued by the approving OCCAR Member State NSA/DSA.	
11.3	Server rooms and ICT administration areas of CIS processing or storing OCCAR RESTRICTED information shall be protected by appropriate physical security precautions and access controls to prevent unauthorised persons from having access to the Systems or supporting components in accordance with OMP11 para. 13.	
11.4	Workstations, Mobile Devices, and removable media used to handle OCCAR RESTRICTED information, and any hard-copy output shall be protected in accordance with the provisions outlined in OMP11 para. 13.	

12. Security Testing

ID	Requirement	✓
12.1	The system shall be subject to security testing and periodic re-testing in accordance with a security test plan outlined within the security documentation.	
12.2	The security test plan shall cover, where appropriate: Identification and Authentication, Access Control, Accountability, Audit, Integrity, Availability, Data Exchange and Security Management functions.	
12.3	Security test findings shall be categorised in terms of severity.	

13. Vulnerability Assessment

ID	Requirement	✓
13.1	The system shall be subject to periodic vulnerability assessments in accordance with the requirements of the security approval or accreditation authority. The frequency of the assessment as stated in the security documentation.	

14. Security Awareness and Training

ID	Requirement	✓
14.1	A security education and awareness programme as agreed by the SAA shall be defined in the security documentation in conjunction with requirement 7.6. It should emphasise the importance of information marking, labelling, and the balance between "responsibility-to-share" and "need-to-know".	
14.2	Users (including system and security administrators) shall be made aware of the security issues with respect to the CIS and shall acknowledge their security responsibilities.	
14.3	Users shall be trained in the appropriate security actions they should be expected to perform, such as dealing with a malicious software infection.	

15. Wireless LAN

ID	Requirement	✓
15.1	The range of Access Points shall be set to minimise exposure to external attacks, special attention shall be given to the selection of antennae, their location, power and signal propagation.	
15.2	The encryption of information in transmission shall be in accordance with requirements in para. 10.	

16. Virtualisation

ID	Requirement	✓
16.1	The use of virtualisation shall be subject to approval by the SAA.	
16.2	A deployed virtualisation product itself shall be treated as at least the highest classification of any of its Virtual Machines (VMs).	
16.3	VMs shall be appropriately configured and managed. System patching, administration of accounts, and maintenance of anti-virus software, shall all be performed as if the machine were a physical machine. The host-operating machine shall also be correctly configured and maintained.	

ID	Requirement	✓
16.4	Network routing provided internally by the virtualisation product to connect VMs shall not be considered as a security measure. For example, a firewall shall not be virtualised with the systems it is protecting.	
16.5	When existing systems are combined using a virtualisation product, the accreditation of each of the systems shall be reviewed to ensure that any mitigations and assumptions previously made are still appropriate.	
16.6	The administrative interface for the hypervisor shall only be used for administration of the hypervisor. It shall not be used for the normal administration of services provided by the VMs.	
16.7	Access to the hypervisor functions shall be appropriately controlled.	
16.8	The automatic mounting of removal media in VMs shall be appropriately controlled.	
16.9	The ability to "cut-and-paste" between VMs shall be appropriately configured and controlled.	
16.10	Data transfers between VMs in different security domains shall be controlled and managed in the same way as data transfers between physical machines in different security domains.	
16.11	The potential impact on overall system availability as a result of Denial-of-Service attacks against one VM shall be considered.	
16.12	The potential impact on overall system resilience to faults due to VMs running on a single host platform shall be considered.	
16.13	The ability to create VMs shall be appropriately configured and controlled.	
16.14	VMs shall be suitably decommissioned after use.	
16.15	Software-based virtual networks created between VMs shall be appropriately configured, controlled and monitored.	
16.16	Separation of roles and permissions between administrators and users shall be maintained in all virtual environments.	
16.17	Virtual Servers and Virtual Workstations shall not be located on the same physical host except for testing purposes in sandboxed, non-production environments.	
16.18	VMs operating in different areas of the system architecture shall not be located on the same physical host. For example, VMs operating in a DMZ shall not be located on the same physical host as those operating within the secured LAN.	
16.19	The management of the virtualisation infrastructure shall be appropriately controlled. Only virtual Management, patch management, anti-malware and Active Directory communication mode shall be allowed.	
16.20	Management of the Virtualisation Infrastructure shall be performed locally, i.e. not via Wide Area Network (WAN) or the Internet.	
16.21	Management of the Virtualisation infrastructure shall be performed via a dedicated administrative account.	

ID	Requirement	✓
16.22	The Storage Area Network (SAN) used for virtualisation shall be isolated and only accessible by the physical host.	
16.23	The SAN used to host VMs operating at different security classifications shall be isolated onto separate Logical Unit Numbers (LUNs).	
16.24	Modifications to the 'Master Copy/Version' of a VM shall be appropriately controlled.	
16.25	Network cards shall not be shared across VMs that are operating in different security domains.	

17. Maintenance

ID	Requirement	✓
17.1	Only appropriately cleared personnel shall conduct hardware maintenance on site, unless authorised by the SAA.	
17.2	Software maintenance shall not be conducted on the operational system unless specifically authorised by the SAA.	
17.3	All procedures for the maintenance of CIS equipment shall be defined in the security documentation.	
17.4	Where it is necessary to deviate from maintenance procedures as defined in the security documentation, prior approval shall be obtained from the SAA.	
17.5	External facilities involved in maintenance or repair work shall be obliged, on a contractual basis, to comply with the applicable provisions for handling of OCCAR RESTRICTED Information (Annex OMP 11-C).	
17.6	Equipment returning from external maintenance shall be subject to security checks and/or isolated testing prior to re-installation in the operational system.	
17.7	Maintenance requiring remote access diagnostic procedures shall be permitted only in exceptional circumstances, under strict control, as fully detailed in the security documentation. Doing so for isolated systems shall mean they're interconnected.	

18. Incident Management

ID	Requirement	✓
18.1	Technically oriented security management staff shall be designated and available to address security incidents.	

ID	Requirement	✓
18.2	All CIS Security incidents shall be reported for inspection and investigation purposes in accordance with the security documentation, which shall include notification to NSA/DSAs.	
18.3	Reports of CIS Security incident affecting CIS handling OCCAR RESTRICTED information shall be classified as OCCAR RESTRICTED documents, with a strict need-to-know distribution.	
18.4	Collection and retention of digital forensics data shall be undertaken in accordance with procedures clearly defined in the security documentation, and by personnel trained in forensic procedures. NSAs/DSAs shall advise on further steps to be taken where required.	

19. Sanitisation and Destruction

ID	Requirement	✓
19.1	All equipment that stores, forwards or processes OCCAR RESTRICTED information shall have its persistent storage overwritten by Member State approved sanitisation tools.	

20. Testing Tools

ID	Requirement	✓
20.1	The CIS shall provide tools for on-demand (not real-time) configuration scanning, in order to collect snap-shot information about the CIS' operational configuration. Tools shall include for instance ping sweep, TCP/UDP port scanning, OS identification, SMTP/DNS/HTTP/SNMP information collection.	
20.2	The CIS shall provide tools for on-demand (not real-time) vulnerability scanning, in order to evaluate and assess potential vulnerabilities within the system. The tools shall allow targeted testing against specific assets, producing results that can be annotated with CIS-specific information.	
20.3	The CIS shall provide tools for real-time intrusion detection, analysing events occurring within a CIS for signs of intrusion or other unauthorised activities. The tool shall include a set of exploitation signatures that are recognised and kept up-to-date by the supplier, which can be modified so as to be adapted to CIS-specific elements. The tool shall also collect data to facilitate post-incident investigation.	
20.4	The CIS shall provide tools to check files and (where appropriate) data streams for malicious software such as viruses, worms and Trojans. The tool shall include centralised management that can provide updates to malicious signatures on all assets within the CIS.	

ID	Requirement	✓
20.5	The CIS shall provide audit tools that monitor and record security relevant events and the status of CIS resources. The tools shall be centrally managed, allowing collection of audit information from all assets within the CIS. Administrators shall be able to identify which security events are relevant for audit. The output audit data shall be protected from the time of generation. Measures shall be implemented to enforce data integrity and non-repudiation.	
20.6	The CIS shall provide tools for network security management, collecting, displaying and analysing network traffic in near real time. The tool shall be able to break down the protocols and payloads into their component parts for appropriate analysis, allowing an administrator to create and apply filters to set up which types of network traffic to be collected and displayed.	
20.7	The CIS shall provide other utility tools as required, for instance OS utilities, password checkers, media processing etc. The use of these tools shall be subject to agreement of the SAA.	

21. Interconnections

ID	Requirement	✓
21.1	CIS assets shall mutually authenticate with each other when establishing trusted connections in order to avoid communication with rogue devices masquerading as legitimate service providers.	
21.2	Logical access control mechanisms shall be used to control local and remote access to data on CIS.	
21.3	All users, devices and systems/security administrators shall be subject to an approved identification, authentication and authorisation process when establishing connection to the CIS from external or public networks.	
21.4	Each administrator of an interconnection boundary protection system shall be uniquely and reliably identified and authenticated and have access rights limited to those required for duties.	
21.5	Network management and security management information shall be subject to strong authentication mechanisms to ensure only authorised traffic is processed by the CIS.	
21.6	Mechanisms shall be established in order to monitor and control the security of interconnections between CIS. This shall include, for example: ▪ User authentication information; ▪ User authorisation information;	

ID	Requirement	✓
	▪ Network communication information; ▪ Application layer information; White lists and black lists of authorised and hostile/dangerous devices and services.	
21.7	Processes to control the import and export of executable content (including mobile code) between interconnected CIS shall be defined in the security documentation of each interconnected CIS.	
21.8	Mechanisms to validate the format of data exchanged between interconnected CIS (e.g. checking that web traffic is in fact HTTP or HTTPS) shall be defined in the security documentation of any interconnected CIS in order to minimize the risk of exploits.	
21.9	Interconnected CIS shall implement techniques to authenticate exchanged data using certificates and digital signatures wherever possible (e.g. SSL/TLS, S/MIME, SOAP).	
21.10	Where encrypted information must be decrypted and re-encrypted as part of the protection mechanisms for an interconnection between CIS (for example, a Man-in-the-middle checkpoint used to analyse and block illegitimate content), the confidentiality of the decrypted data shall be maintained until it is re-encrypted.	
21.11	Wherever encryption is used to protect information during transit, malicious code detection and filtering technologies shall be employed prior to encryption, and immediately after decryption.	
21.12	Boundary Protection mechanisms shall be configured and managed such that modification of configuration settings can only be performed by authorised system and/or security administrators.	
21.13	All information outgoing from a CIS handling OCCAR RESTRICTED to public networks shall be content-checked at the boundary to ensure no unencrypted classified information is unintentionally released to the public network.	
21.14	Where possible, information incoming to a CIS handling OCCAR RESTRICTED information shall be content-checked at the boundary to monitor and isolate unencrypted or inappropriately classified information so that it may be properly labelled. A procedure shall be defined to address logging of incidents and determination of follow-up actions.	
21.15	Additional security events shall be identified in the security documentation for interconnected CIS, in particular regarding the need to continuously monitor boundary devices for intrusions and attacks. Where possible, monitoring shall occur at both "outer" and "inner" points in order to identify and respond to attempted and successful intrusions.	

ID	Requirement	✓
21.16	Security devices deployed to protect interconnection boundaries shall allow the execution of self-tests during start-up, at the request of the security administrator(s), and during automated recovery, to verify the integrity of their code and data structure. In the event of system failure, there shall be no loss of audit and logging data, and the device shall recover to a secure state.	
21.17	Mobile Devices shall be checked for "endpoint security compliance" prior to connection to any network handling OCCAR RESTRICTED information.	
21.18	Any intent to interconnect a CIS handling OCCAR RESTRICTED information shall be initiated through the development of an operational requirement statement, detailing the business justification for the interconnection as agreed by all IDAs, SOAs and SAAs involved.	
21.19	Any CIS intending to connect with any other CIS handling information equivalent to OCCAR RESTRICTED shall have a valid Statement of Compliance describing the security posture of the system and the standards against which it was approved, issued by its SAA.	
21.20	Appropriate security arrangements shall exist to ensure that SAAs and SOAs of any interconnected CIS are bound by the requirement to protect OCCAR Classified Information.	
21.21	The conditions and required actions for emergency disconnection/limitation of service(s) in the event of security incidents shall be detailed within the security documentation. This shall include the provision for protection against DDoS attacks, defining a list of priority and non-priority clients to be maintained.	
21.22	Bidirectional end-to-end communication (such as voice over IP, collaboration, web conferencing and chat) over public networks shall be limited to UNCLASSIFIED conversations only, unless entirely contained within an appropriately secured VPN.	
21.23	CIS that are interconnected with public networks such as the internet shall make use of Boundary Protection mechanisms whose Security Enforcing Functions meet EAL4 as a minimum. This may be increased or lowered in consultation with the SAA.	
21.24	Boundary protection mechanisms embedded within Mobile Devices may not meet requirement 21.23. Where this is the case, Mobile Devices shall not directly mediate information exchange with public networks, unless operating in an UNCLASSIFIED environment. Mobile Devices operating with OCCAR RESTRICTED information shall establish Member State approved encrypted tunnels into equivalently-classified CIS so as to make use of boundary protection mechanisms that meet requirement 21.23, which can securely mediate information exchange with public networks.	

ID	Requirement	✓
21.25	Procedures for the exchange of security incident-related information (e.g. relevant intrusion and audit information) for the resolution of cross-boundary security incidents of interconnected CIS shall be defined in the security documentation.	