EBU

OPERATING EUROVISION AND EURORADIO

R 143

CYBERSECURITY RECOMMENDATION FOR MEDIA VENDORS' SYSTEMS, SOFTWARE & SERVICES

RECOMMENDATION

Version 2.0

Geneva
November 2020

This page and others in the document are intentionally left blank to maintain pagination for two sided printing

Cybersecurity Recommendation for media vendors' systems, software & services

EBU Committee	*First Issued*	*Revised*	*Re-issued*
TC	March 2016	Nov. 2020	

Keywords: Security, Services, Infrastructure, Broadcasting, IP, Software, Application, Cyber, Security Controls Assertation, Vendor, Vulnerabilities, Authentication, Password, Encryption, Certificate, PKI, Keys, Log, Incident.

Recommendation

The EBU, considering that

1. Media companies increasingly employ third parties to provision their systems, software and services.
2. Production workflows and infrastructures are rapidly migrating to generic IT technologies.
3. Cyberthreats (e.g. malware and ransomware) are increasingly easy to perform and are continuously evolving.
4. Connected media devices still tend to have a low security threshold inherited from the era of non-connected broadcast media.

Recommends that media companies:

1. Apply the safety security safeguards set out in R 143 Security Controls Assertation[1] and associated guidance when planning and designing their systems, software and services.
2. Require potential vendors of systems, software and services to declare their ability to comply with R 143 Security Controls Assertation (by completing columns A & B) and associated guidance, when responding to tenders or requests for technology.
3. Define their minimal vendor system acceptance level on the basis of this Recommendation with full awareness of the potential risks.

[Annex A, B & C & the Security Controls Assertion spreadsheet complete this Recommendation]

[1] The Security Controls Assertation is a companion document to this publication. It is an Excel spreadsheet that may be downloaded from the publication page of this Recommendation.

Spreadsheet completion guidelines

Definitions

Product:	The product, service, system or software being provided by the organisation to the customer.
Organisation/vendor:	The potential vendor (including appointed sub-contractors) providing the product, service, system or software.
Customer:	The entity that uses (purchases) a Product from your organisation

The sections in **Annex A** and **Annex B** correspond to the elements that must be completed in the Security Controls Assertation spreadsheet. Please read these Annexes carefully as they will assist you in correctly filling in the spreadsheet.

Annex C reproduces the Security Controls Assertation spreadsheet for convenience of referencing. Entries in the Security Controls Assertation should be made in the Excel spreadsheet that may be downloaded from the publication page of this Recommendation on the EBU technical website.

Annex A: Vendor Information Security Management System

IS. Vendor ISMS

IS-01 Cyber security policy

There is a documented Cyber Security Policy (or set of policies) in place that are aligned to or certified against recognised security standards and frameworks and approved by senior management.

Information security policy is the foundation of an organisation's security programme. It should set out how the organisation protects information assets taking into account:

Confidentiality: the protection of information from unauthorised access;

Integrity: ensuring that information is complete and accurate and hasn't been tampered with, altered or damaged in an unauthorised way;

Availability: information is available to the right people when it is needed.

The policy should be approved and signed off by senior management to demonstrate their commitment to the organisation's security programme.

There are a number of recognised cyber security frameworks and standards (including but not limited to): ISO27001, National Institute of Standards & Technology (NIST), Cloud Security Alliance (CSA), European Union Agency for Cybersecurity (ENISA), Content Delivery & Security Association (CDSA), Motion Picture Association (MPA)

If your organisation is certified, you should provide evidence of the certification as part of the completion of the R 143 Security Controls Assertation.

Cyber security policies are kept up to date and effectively communicated to all relevant personnel.

Policies should be reviewed regularly to make sure that they are suitable, adequate and effective for the organisation.

They should be communicated regularly to everyone that needs to see them. This should be in a way that is relevant and understandable by the intended reader, and they should be easy to access.

IS-02 Effective cyber security organisation

All cyber security roles and responsibilities are assigned and communicated to relevant personnel.

Cyber security roles and responsibilities should be assigned in line with the cyber security policy.

There is a named Chief Information Security Officer (CISO) or appointed person who has overall responsibility for cyber security within the organisation.

The CISO or appointed person should be of sufficient seniority within the organisation and have relevant experience to be able to carry out the role effectively.

Cyber security awareness training and education is provided to all employees (including contractors) as is relevant to their role.

Training should include at a minimum: information protection and security, password and user account security, legal and regulatory (e.g. GDPR).

IS-03 Audit plan

The organisation has audit procedures in place that ensure periodic review of the suitability and effective operation of its security controls framework.

Regular reviews should be carried out to ensure that the organisation's approach to cyber security is continually being assessed for its effectiveness and suitability and that any areas identified for improvement or change are addressed.

OS. Operational Security

OS-01 Technical security analysis

Regular technical security analysis such as penetration or vulnerability testing of the product or service is performed.

Vulnerability scans are automated tests that identify vulnerabilities in a system or application. Penetration testing is more in depth than a vulnerability scan and can be used to identify weaknesses as well as exploit them.

System components, processes and software must be tested frequently to ensure that security of customer information is maintained. This is especially important when significant changes are made to infrastructure or internet-facing services.

Results of such penetration or vulnerability testing are provided to the customer.

Assurance should be provided to the customer that any identified vulnerabilities or weaknesses have been fixed and any residual risk has been mitigated.

OS-02 Vulnerability management

A vulnerability management process is in place to keep track of identified vulnerabilities and patches that may fix them.

A vulnerability management process should be in place that demonstrates to customers how frequently vulnerability testing is carried out and how patching is managed and implemented to fix any identified weaknesses.

The process should ensure that potential vulnerabilities within the product stack are identified (e.g. if running an Oracle DB then Oracle security bulletins should be subscribed to) and there should be a release process to patch security issues for customers in line with this.

Reporting of vulnerabilities is covered in section IM. Incident Management.

OS-03 Product lifecycle

The product lifecycle is clearly defined, and patches and updates are made available throughout that lifecycle.

The product or service lifecycle should be clearly defined so that the customer is aware of key dates. Patches and updates should be made available to ensure that security can be maintained throughout the lifecycle of the product or service, from implementation to decommission.

To limit the damage that could be caused by attackers, critical patches should be implemented as soon as possible. Non-critical patches should be implemented within a month but no later than 90 days of release.

The vendor should also support the upgrade of the software components of the system (OS, DBMS, Application Server etc.) if any of these components becomes unsupported.

OS-04 Product/software delivery

There is a secure process in place for the delivery of products, software or services.

The vendor should provide physical and digital security controls for the delivery process of products, software or services. These security controls may include:

- encrypted USB keys;
- delivery through secure protocols;
- encrypted software packages; and
- hash value checking.

OS-05 Customer Maintenance

Secure methods are in place to provide remote support and maintenance for customers.

Customer support for the product or service should be provided securely, including, but not limited to:

- Virtual Private Network (VPN) using Multi-factor authentication (MFA).
- Remote support accounts should only be enabled for the duration of the troubleshooting activity.
- All troubleshooting activity should be logged and reviewed.

OS-06 Separation of production and non-production

Production and non-production environments are kept separate.

Development, test and production facilities should be separated to reduce the risk of unauthorised access or changes to the operational environment.

SD. Secure Development

SD-01 Development lifecycle

Security is designed into and implemented through the whole lifecycle of product development.

There should be a policy or equivalent documentation in place which outlines the secure process for the development of software or systems.

The development lifecycle should include as a minimum:

- a risk assessment/threat modelling process;
- secure design/architecture review;
- documented secure coding guidelines and industry good practice (e.g. OWASP) that are applied and kept up to date;
- mandatory test stages/security gates;
- secure code analysis where the source code and/or compiled versions of code are analysed to help find security flaws; and
- code cleaning to ensure that there is no test code remaining from the development process in the final version.

SD-02 Training

Development staff are trained in the latest secure coding principles and industry good practice.

Development staff should receive regular training and continuous development to ensure they keep up to date with the latest secure coding principles and industry good practice.

SD-03 Source-Code

Access to program source-code is restricted and is strictly controlled.

Program source-code should be protected and access strictly controlled to prevent introducing unauthorised functionality, unintentional changes and to maintain confidentiality where there are intellectual property implications.

IM. Incident Management

IM-01 Incident response

A documented incident response and crisis management process/procedure is in place, that is regularly reviewed and kept up to date.

Security incident response responsibilities and procedures must be established to ensure a quick, effective and orderly response to information security incidents. This includes having a clear outline of responses to different attack scenarios and clear escalation routes.

The process should also include a post-incident review so that appropriate action can be taken to prevent the same or a similar security incident from reoccurring.

IM-02 Contact points

There are clearly appointed points of contact (internal, external, and at customers) in place to ensure a quick and effective response to security incidents.

The list of contacts should consider the risk of people being unavailable (e.g. to have more than one person and contact method for each escalation point).

The organisation should have a 24/7 contact number available to respond to critical or significant information security incidents such as zero-day attacks, for example.

IM-03 Forensic readiness

A documented policy or process is in place to manage the preservation of evidence relating to security incidents.

Documentation should be in place to preserve evidence for when disciplinary or legal proceedings are required. This includes the collection, retention and presentation of such evidence.

IM-04 Responsible vulnerability disclosure

There is a vulnerability disclosure policy or process in place for the responsible reporting of vulnerabilities.

Having a vulnerability disclosure policy/process helps to reduce the risk of an incident occurring. It allows a reasonable time for a vendor to provide a vulnerability patch before it is publicly disclosed.

It is expected that a vendor will comply with EBU R 160.

PS. Physical security

PS-01 Access control

Physical access controls are in place to restrict the entry and exit of personnel, equipment and media from areas such as office buildings, data centres or rooms where communication servers are located.

The organisation must ensure that any equipment and facilities are secured to prevent loss, damage, theft or compromise of customer information. This includes:

- access control for entrances into the organisation's data centre (e.g. security guard, badge reader, electronic lock, court admissible CCTV) with logs recorded, reviewed and retained as necessary;
- physical access restricted to those with a business need and the minimum access necessary to do their job;
- control of delivery and loading areas and other points of access where unauthorised persons could enter the premises;
- emergency exit doors should be alarmed, monitored and tested in line with appropriate regional, national and international standards;
- power supplies and fire safety mechanisms undergo regular maintenance checks and comply with Health and Safety regulations; and
- intruder detection systems should be installed, monitored and tested in line with appropriate regional, national and international standards.

PS-02 Service outages

Security measures are in place to protect equipment from utility service outages (e.g. power failures and network disruptions).

Security measures should be in place to protect customer information and could include (but is not limited to):

- backup power generation;
- dual/multiple routing;
- load balancing and redundancy;
- bandwidth capacity monitoring and alerting; and
- regular testing.

PS-03 Environmental threats

Physical protection is in place to reduce the risk from environmental threats and hazards as well as deliberate attack.

Environmental threats should be considered and the risk assessed. This includes threats such as flood, fire, earthquake, civil unrest and other forms of natural or man-made disaster. Specialist advice may be needed to ensure that there is adequate protection in place.

CS. Cloud Security

CS-01 Cloud-based service adoption procedure

Vendor can provide all information needed by customer to follow the cloud adoption procedure defined in EBU R 146.

Recommendation R 146 provides a procedure for the acceptance of cloud-based services by media companies. The Vendor shall cooperate and provide all information needed by the media company to follow the procedure, including service functionalities, processes, systems and data, data classification, possible usage limitations according to local or European laws, technical and organizational requirements to operate the service etc.

CS-02 Segregation of customer data

Appropriate segregation of customer data is in place where it is being stored or processed in a multi-tenanted environment.

If customer data is hosted on cloud platforms where there are multiple tenants, there should be segregation between customers so that each customer's data are kept confidential and are not disclosed to the other customers and that an incident affecting one customer does not have an adverse impact on other customers or their information.

CS-03 Segregation of customer platforms/infrastructure

Adequate segregation exists between customer platforms and infrastructure to allow updates or changes to be applied independently, where required.

As in section CS-02, there should be segregation between customers to ensure that if an update or change needs to be applied independently to one customer, there is no adverse impact to other customers.

BC. Business Continuity

BC-01 Business continuity planning

A business continuity and/or disaster recovery plan is in place that is tested and reviewed at regular intervals.

The organisation should have a business continuity or disaster recovery plan in place that includes the continuation of security of customer information in the event of an adverse situation.

As a minimum, the plan should:

- set out how business operations will be restored following an interruption to or failure of business processes within an agreed time period (agreed with the customer);
- set out how information security will be maintained;
- include arrangements to inform and engage the appropriate customer personnel in its execution;
- be tested at regular intervals;
- be regularly reviewed and updated where necessary.

There should be sufficient redundancy to meet the availability requirements for providing the services to the customer.

SC. Supply Chain Management

SC-01 Supply chain security control assessment

The Vendor applies the same level of security control assessment procedure to its own suppliers.

The Vendor requires its own potential suppliers and vendors of main subsystems, software and services that are embedded in their products to declare their ability to comply with security controls assertation and guidance with the same level of detail provided in this Recommendation. Vendors can communicate the results to their customers.

Annex B: Product Security Requirements

DO. Documentation

DO-01 Password change

There are explicit instructions to change default passwords, especially in internet facing systems.

Default passwords are a well-known vulnerability. The documentation issued with the product should have explicit instructions to change default passwords.

DO-02 Security functionality

Product documentation includes a complete description of security functionality.

Documentation provided should include details of all the security functionality provided with the product. This should cover all the requirements in Annex B of this Recommendation as a minimum.

DO-03 Networking

Product documentation includes a complete description of interfaces, access points, network communication and features.

In detail, the vendor should provide:

- which Layer 3 capabilities are used;
- which IP ports are used by the application/system;
- which IP ports are open (not used, but could potentially be used for application attack); and
- which IP ports are disabled as part of the standard application configuration.

DO-04 Integration

Product documentation includes information on how to integrate the product in a security framework (e.g. different network zones, central authentication service, workflows, interfaces, only necessary TCP/UDP ports are open).

Clear documentation should be provided that includes detail on how to integrate the product in various security scenarios.

DO-05 Hardening

The product includes recommendations on hardening or best practice configuration, including the default state of the product. Only the minimum required services should be active.

Where available, industry best practice should be followed for system hardening e.g. CIS Benchmarks or SANS Institute.

Only the minimum required services should be running.

DO-06 Patch management process

Product documentation includes a description of the patch and release management process (especially regarding security updates).

The patch management and release management documents for the product should be produced in line with section OS-O3 Product lifecycle.

AA. Authentication & Authorisation

AA-01 Central authentication

The product supports central authentication services that are most used in the industry.

The product should support central authentication services. The following is a list of those that are most used in the industry:

- Active Directory: Kerberos based authentication
- LDAP over SSL: LDAPS
- Identity Provider:
  - SAML IdP: Simple Authentication Mark-up Language
  - OpenID IdP: Identity layer on top of the OAuth protocol
- RADIUS
- TACACS+

AA-02 Session timeout

The product supports the timeout of sessions.

Session timeouts should be set with a balance of security and usability. The window of opportunity for an attacker needs to be limited, but a user should be able to comfortably complete operations within the product without the session timing out too often.

AA-03 Role based access control (RBAC)

The product should support RBAC.

Role based access restricts access based on a user's role within an organisation.

AA-04 Personalised accounts

The product supports the authentication of individual users.

Every user should log into the system with a unique personal account to ensure that the individual activity of each person using the account can be identified and audited, and that individual accountability is maintained.

AA-05 Default passwords

The product allows default passwords to be changed for built-in accounts.

It must be possible to change default passwords. As factory or default passwords are often well know and publicly documented, they could be a source of unauthorised access, especially for equipment that is exposed to the internet.

The product does not have global hidden accounts with the same password for all product units and customers.

Products often embed "hidden" accounts, used by vendors to perform maintenance tasks (which means that these accounts have high privileges.

Such "hidden accounts", if present, must have different passwords at least on a per-customer basis.

AA-06 Password policy

The product supports strong password policy implementation.

To implement strong passwords, the password policy should include as a minimum:

- Minimum password length of 8 characters (longer for administrative accounts).
- Upper/lowercase characters.
- Numbers.
- Special characters and extended special characters.

AA-07 Authentication

The product supports multi-factor authentication (MFA) mechanisms.

Strong authentication mechanisms provide additional layers of security to the traditional authentication scheme. The strong authentication method relies on implementing more than one of the following authentication factors (Multi-Factor Authentication – MFA):

1. Something you know
2. Something you have
3. Something you are

For example, using an authenticator App on a trusted device, a physical security token or a one-time password/code that is regularly refreshed or with a short expiry.

The product supports enhanced authentication mechanisms in internet-facing interfaces.

The product must support enhanced authentication mechanisms (second factor of authentication (2FA) using Security Assertion Mark-up Language V2 (SAML2)) in internet-facing interfaces. This method can be combined with SSO, allowing users to authenticate only once, and not for each application they access.

AA-08 Authentication, Authorisation and Accounting (AAA) logging

The product generates logs for authentication events, authorisation events and user activities as they occur.

The product generates security event logs that record details of:

- **Authentication**: details of any logins to the system and whether they were successes or failures.
- **Authorisation**: details of user attempts to access specific system functions (especially sensitive administrative functions) and whether these were permitted or denied.
- **Accounting**: details of activities / actions undertaken by users on the system.

See also: BA-01 for recommendations on how to manage logs generated.

EN. Encryption

EN-01 Password storage and transfer

Passwords are neither stored in the product nor transferred in plain text or in any reversible format.

The product must also implement onscreen password masking (i.e. when typing in a password, the system displays a row of asterisks rather than an actual password). This ensures that the entry of user passwords cannot be observed by another user.

EN-02 Data at rest

The product supports state-of-the-art encryption technologies following industry best practice recommendations and latest standards.

Data at rest shall be encrypted using state-of-the-art encryption, at least stronger than AES 256.

The following ciphering operating modes shall also be considered:

- GCM: Galois/Counter Mode
- CTR: Counter Mode
- CBC: Cipher Block Chaining Mode

It is also important to bear in mind:

- for the same encryption algorithm, a longer encryption key generally provides stronger protection;
- longer complex phrases are stronger than shorter passphrases.

EN-03 Data in transit

The product supports encrypted network protocols.

Communications must be encrypted when transmitted across networks so as to protect against eavesdropping of network traffic by unauthorized users.

- The following protocols should be used:
  - HTTPS
  - SFTP
  - FTPS
  - SCP
  - SSHv2
  - SNMPv3

- The following protocols should be avoided:
  - HTTP
  - FTP
  - TELNET
  - SNMPv1 - SNMPv2
  - SSHv1
  - VNC

EN-04 Certificates and PKI support

The product should support the use of certificates and Public Key Infrastructure (PKI).

PKI and certificates are necessary to authenticate people, devices and services and to secure the transfer of information.

EN-05 Master keys Management

Master keys are securely managed.

Every encryption-based system has a default master key that encrypts all the private keys and passwords in the configuration to secure them. It is recommended to:

- Configure a new master key instead of using the default.
- Change it periodically (the time-period depends on factors such as the criticality/sensitivity of the data being protected).
- Store it in a safe location.

Information on how to configure and potentially reset the master key might also need to be provided by the vendor.

BA. Base configuration

BA-01 Log management

The product generates security event and error logs.

The product should, as a minimum, generate the following types of log:

- **Security events**: the system should log AAA data in accordance with AA-08.
- **Errors**: the system should generate error logs when something has gone wrong.

The product provides capabilities for securely delivering logs in real-time to a centralised log management platform.

The product should support regular time synchronisation (e.g. using NTP) with the agreed common reference time-source used by the organisation deploying it. The investigation of issues is challenging if systems on a network do not use the same time-source.

The product should support logging through mechanisms that provide assurance that the centralised logging system unequivocally received the data (e.g. TCP preferred over UDP).

The product should support encryption in transit of log data between the product and the centralised log management platform.

BA-02 Portable media control

The product supports disabling or controlling the interfaces and access rights to portable media.

Portable media (e.g. USB devices) are a frequent route for the introduction of malware, both accidental and deliberate. The product should support disabling or controlling the interfaces and access rights to this kind of device. The provider should explicitly state:

- what interfaces are available;
- the default access rights of the interfaces, and the default operating state (e.g. interfaces activated by default or disabled by default);
- the method needed to enable these interfaces if required.

BA-03 Unnecessary protocol deactivation and OS hardening

Unnecessary protocols are disabled.

Following OS hardening best practices, any protocol/feature that is not used by the product, should be disabled by default.

BA-04 Effective antivirus/malware protection

The product supports effective protection against virus/malware and server-side and client-side exploits.

The product should support effective protection against Virus/Malware and server-side and client-side exploits. The vendor should provide the following detailed information regarding installation and use:

- List of AV solutions that have been tested on the system.
- Installation/update/roll-back methods.

BA-05 Monitoring support

The product provides access to data that supports real-time monitoring processes.

The product should support a real-time-audit trail and log-monitoring process. Product administrators can access event logs that include an audit trail of system activity, any system/application errors and security relevant events.

Products should support making system status/health data and performance metrics available by means of an appropriate mechanism (e.g. via SNMP) so that they can be monitored using third party monitoring platforms.

BA-06 Backup/restore support

The product supports backup and restore.

The product supports backup and restore, including as a minimum:

- User Data.
- System Data.
- Firmware.
- Configuration.

BA-07 Software/OS decoupling

The product supports OS and software decoupling, allowing OS and runtime environments patching.

The product should support OS and software decoupling, allowing OS and runtime environment patching. The vendor should communicate when an operating system patch has been validated and can be installed.

NE. Network configuration

NE-01 Network segmentation

The product supports granular segmentation of networks (MPLS, multi-VLAN, routing).

The product should support granular segmentation of networks (MPLS, Multi VLAN, routing). It should also include isolation between management and data network interfaces, as is done in common network management and monitoring tools.

NE-02 Security of call-home Internet connectivity

If the device requires a default call-home connection, it should be secured by appropriate means. In particular:

The product should work without needing a constant and direct connection to the internet.

The product should support content inspection when connected to the internet.

This kind of inspection can be implemented through forward and reverse proxies, including authentication mechanisms.

The product should support jumphost.

The product supports maintenance access points in a demilitarized zone (DMZ) so that vendors or administrators first connect to a DMZ instead of to the appliance itself.

The product should provide traffic monitoring (inbound/outbound).

Monitoring or filtering the traffic can be useful to detect abnormal behaviour related to unauthorized activities.

AP. Application security

Detail on the controls for application security can be found on the OWASP website https://cheatsheetseries.owasp.org/

AP-01 Input validation

The product implements proper input validation inside the application.

AP-02 XSS and SQL Validation

The product implements controls against cross site scripting and SQL injection for web frontends.

AP-O3 Non-admin context running

Every program and user system operates using the least set of privileges necessary to complete the job.

AP-04 Account enumeration

The product implements mechanisms to protect against account enumeration.

AP-05 Session management

The product implements mechanisms to protect user sessions against session hijacking attacks.

AP-06 Fail secure

The application is designed to fail securely, with every failure following the same execution path as disallowing the operation.

CM. Change management

CM-01 Change management

Changes that affect the security of the product or service are controlled and authorised through a formal, documented process.

Changes that affect the security of the product or service must be controlled, documented, and authorised through a formal process. Any such change must be reviewed and tested to ensure that there is no adverse impact on the product and services provided to the customer or to the security of customer information.

Annex C: Security Controls Assertation (for information only – use the spreadsheet)

Vendor Security Requirement			A	B	C
			Do you meet this requirement?	Please provide details to support your response in column A	Reviewer comments
IS. Vendor ISMS - This section sets out your organisation's approach to information security					
IS-01	Cyber security policy	There is a documented Cyber Security Policy (or set of policies) in place that are aligned to or certified against recognised security standards and frameworks and approved by senior management.			
		Cyber security policies are kept up to date and effectively communicated to all relevant personnel.			
IS-02	Effective cyber security organisation	All cyber security roles and responsibilities are assigned and communicated to relevant personnel.			
		There is a named Chief Information Security Officer (CISO) or appointed person who has overall responsibility for cyber security within the organisation.			
		Cyber security awareness training and education is provided to all employees (contractors) as relevant to their role.			
IS-03	Audit plan	The organisation has audit procedures in place that ensure periodic review of the suitability and effective operation of its security controls framework.			
OS. Operational Security					
OS-01	Technical security analysis	Regular technical security analysis such as penetration or vulnerability testing of the product or service is performed.			
		Results of penetration or vulnerability testing are provided to the customer.			
OS-02	Vulnerability management	A vulnerability management process is in place to keep track of identified vulnerabilities and patches that may fix them.			
OS-03	Product lifecycle	The product lifecycle is clearly defined and patches and updates are made available throughout that lifecycle.			
OS-04	Product/software delivery	There is a secure process in place for the delivery of products, software or services.			

OS-05	Customer maintenance	Secure methods are in place to provide remote support and maintenance for customers.			
OS-06	Separation of production and non-production	Production and non-production environments are kept separate.			
SD. Secure Development					
SD-01	Development lifecycle	Security is designed into and implemented through the whole lifecycle of product development.			
SD-02	Training	Development staff are trained in the latest secure coding principles and industry good practice.			
SD-03	Source-code	Access to program source-code is restricted and strictly controlled.			
IM. Incident Management					
IM-01	Incident response	A documented incident response and crisis management process/procedure is in place, that is regularly reviewed and kept up to date.			
IM-02	Contact points	There are clearly appointed points of contact (internal, external, and customers) in place to ensure a quick and effective response to security incidents.			
		A documented process is in place to notify customers when a security incident occurs.			
IM-03	Forensic readiness	A documented policy or process is in place to manage the preservation of evidence relating to security incidents.			
IM-04	Responsible vulnerability disclosure	There is a vulnerability disclosure policy or process in place for the responsible reporting of vulnerabilities.			
PS. Physical Security					
PS-01	Access control	Physical access controls are in place to restrict the entry and exit of personnel, equipment and media from areas such as office buildings, data centres or rooms where communication servers are located.			
PS-02	Service outages	Security measures are in place to protect equipment from utility service outages (e.g. power failures and network disruptions).			
PS-03	Environmental threats	Physical protection is in place to reduce the risk from environmental threats and hazards as well as deliberate attack.			

CS. Cloud Security					
CS-01	Cloud based service adoption procedure	Vendor can provide all information needed by customer to follow the cloud adoption procedure defined in EBU R 146			
CS-02	Segregation of customer data	Appropriate segregation of customer data is in place where it is being stored or processed in a multi-tenanted environment.			
CS-03	Segregation of customer platforms/infrastructure	Adequate segregation exists between customer platforms and infrastructure to allow updates or changes to be applied independently where required.			
BC. Business Continuity					
BC-01	Business continuity planning	A business continuity or disaster recovery plan is in place that is tested and reviewed at regular intervals.			
SM. Supplier Management					
SC-01	supply chain security control assessment	Vendor applies same level of security control assessment procedure to its own suppliers.			

Vendor Security Requirement			A	B	C
			Do you meet this requirement?	Please provide details to support your response in column A	Reviewer comments
DO. Documentation					
DO-01	Password change	There are explicit instructions to change default passwords, especially in internet facing systems.			
DO-02	Security functionality	The product documentation includes a complete description of security functionality.			
DO-03	Networking	Product documentation includes a complete description of interfaces, access points, network communication and features.			
DO-04	Integration	Product documentation includes information on how to integrate the product in a security framework (e.g. different network zones, central authentication service, workflows, interfaces, only necessary TCP/UDP ports are open).			
DO-05	Hardening	The product includes recommendations on hardening or best practice configuration, including the default state of the product. Only the minimum services required should be active.			
DO-06	Patch management process	Product documentation includes a description of the patch and release management process (especially regarding security updates).			
AA. Authentication & Authorisation					
AA-01	Central authentication	The product supports central authentication services that are most used in the industry.			
AA-02	Session timeout	The product supports the timeout of sessions.			
AA-03	Role based access control (RBAC)	The product should support RBAC.			
AA-04	Personalised accounts	The product supports the authentication of individual users.			
AA-05	Default passwords	The product allows default passwords to be changed for built-in accounts.			
		The product does not have global hidden accounts (such as maintenance accounts) with the same password for all product units and customers.			

AA-06	Password policy	The product supports strong password policy implementation.			
AA-07	Authentication	The product supports enhanced authentication mechanisms in internet-facing interfaces, such as Multi-Factor Authentication (MFA).			
AA-08	Authentication, Authorisation and Accounting (AAA) logging	The product generates logs for authentication events, authorisation events and user activities as they occur.			
EN. Encryption					
EN-01	Password storage and transfer	The product stores and transfers every password in a secure way, avoiding plain text. Any password stored in the product must use non-reversible encryption/hashing.			
EN-02	Data at rest	The product supports state-of-the-art encryption technologies following industry best practice recommendations and latest standards.			
EN-03	Data in transit	The product supports encrypted network protocols			
EN-04	Certificates and Public Key Infrastructure (PKI) support	The product supports the use of certificates and PKI.			
EN-05	Master keys management	Master keys are securely managed.			
BA. Base configuration					
BA-01	Log management	The product generates security event and error logs.			
		The product provides capabilities for securely delivering logs in real-time to a centralised log management platform.			
BA-02	Portable media control	The product supports disabling or controlling the interfaces and access rights to portable media.			
BA-03	Unnecessary protocol deactivation and OS hardening	Unnecessary protocols are disabled.			
BA-04	Effective antivirus/malware protection	The product supports effective protection against virus/malware and server-side & client-side exploits.			

BA-05	Monitoring support	The product provides access to data that supports real time monitoring processes.			
BA-06	Backup/restore support	The product supports backup and restore			
BA-07	Software/OS decoupling	The product supports OS and software decoupling, allowing OS and runtime environments patching			
NE. Network configuration					
NE-01	Network segmentation	The product supports granular segmentation of networks (MPLS, multi-VLAN, routing)			
NE-02	Security of call home Internet connectivity	The product should work without needing a constant and direct connection to the internet			
		The product should support content inspection when connected to the internet			
		The product should support jumphost			
		The product should provide traffic monitoring (inbound/outbound)			
AP. Application security					
AP-01	Input validation	The product implements proper input validation inside the application.			
AP-02	XSS and SQL validation	The product implements controls against cross site scripting and SQL injection for web frontends.			
AP-03	Non-admin context running	Every program and user system operates using the least set of privileges necessary to complete the job.			
AP-04	Account enumeration	The product implements mechanisms to protect against account enumeration.			
AP-05	Session management	The product implements mechanisms to protect user sessions against session hijacking attacks.			
AP-06	Fail secure	The application is designed to fail securely, with every failure following the same execution path as disallowing the operation.			
CM. Change Management					
CM-01	Change management	Changes that affect the security of the product or service are controlled and authorised through a formal, documented process.			