BS EN 16495:2014

BSI Standards Publication

Air Traffic Management — Information security for organisations supporting civil aviation operations

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 16495:2014.

This standard was voted against by the UK committee as the model of security controls specified in this standard are direct references from ISO 27002:2005, which has been superseded by ISO 27002:2013.

ISO 27002:2013 uses different controls and numbering to ISO 27002:2005, which may lead to increased complexity in organisations transitioning their business IT systems to ISO 27002:2013, alongside introducing BS EN 16495 in their operational systems.

The UK participation in its preparation was entrusted to Technical Committee ACE/58, Environmental and operating conditions for aircraft equipment.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2014

ISBN 978 0 580 80325 3

ICS 03.220.50; 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2014.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16495

January 2014

ICS 03.220.50; 35.040

English Version

Air Traffic Management - Information security for organisations supporting civil aviation operations

Gestion du trafic aérien - Sécurité de l'information pour les organismes assurant le soutien des opérations de l'aviation civile

Flugverkehrsmanagement - Informationssicherheit für Organisationen im Bereich der Zivilluftfahrt

This European Standard was approved by CEN on 9 November 2013.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword

This document (EN 16495:2014) has been prepared by Technical Committee CEN/TC 377 “Air Traffic Management”, the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by July 2014, and conflicting national standards shall be withdrawn at the latest by July 2014.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

1 Scope

This European Standard defines guidelines and general principles for the implementation of an information security management system in organisations supporting civil aviation operations.

Not included are activities of the organisations that do not have any impact on the security of civil aviation operations like for example airport retail and service business and corporate real estate management.

For the purpose of this European Standard, Air Traffic management is seen as functional expression covering responsibilities of all partners of the air traffic value chain. This includes but is not limited to airspace users, airports and air navigation service providers.

The basis of all requirements in this European Standard is trust and cooperation between the parties involved in Air Traffic Management.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000:2012, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security controls*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000:2012 and the following apply.

3.1
Air Traffic Management
aggregation of the airborne and ground-based functions (air traffic services, airspace management and air traffic flow management) required to ensure the safe and efficient movement of aircraft during all phases of operations

3.2
trust
situation where one party is willing to rely on the actions of another party

Note 1 to entry: Trust is more than what can be achieved by assurance. However, assurance represents a supporting instrument to trust building.

4 Information security management in aviation

4.1 Structure of this European Standard

This European Standard is structured in line with ISO/IEC 27002. ISO/IEC 27002 is merely referenced in all cases in which its measures can be applied without being amended or supplemented.

In all cases in which the implementation of ISO/IEC 27002 measures requires supplementation specific to aviation, this has been integrated directly in the respective section.

Implementation examples for specific application areas are described in Annex A (informative). This relates to the following areas:

— Security of information in web applications and web services;

— Connections between multiple organisations /external connections;

— Certificates / Public Key Infrastructure;

— Identity Management.

4.2 Information security management systems in aviation

This European Standard is a guideline for implementing and controlling an information security management system in aviation organisations. It is based on the international standard ISO/IEC 27002 (Code of practice for information security management). Aviation organisations have also to consider the security measures listed in this European Standard in addition to the objectives and measures of ISO/IEC 27002.

Information security management has a high priority in aviation regardless of the respective position of the organisation within the service chain. Without an effective information security management system, the risks in connection with the confidentiality, availability and integrity of the information/data required for service delivery increase critically.

Service delivery in aviation is greatly defined by the cooperation of the individual participants. An organisation's information security management is therefore dependent on the information security management of the organisations with which it cooperates to deliver service. This European Standard therefore focusses on aspects of cooperation.

This cooperation requires

— sharing the results of risk assessments along the business process chain,

— agreement on the required level of trust,

— agreement on the required security controls and their implementation.

4.3 Assessment of information security risks

4.3.1 Internal information security risk management

To understand its own security position, an organisation will need to have an understanding of the security position of its partners.

Making network connections and exchanging data are based on a trust assessment between the parties involved. The extent to which the network traffic and data needs to be controlled and checked is determined by the degree of trust. This is further explored in 4.5.

To enable a secure external connection and data exchange the organisation shall assess the trust it can place in the connection and in the data being received, and ensure itself that the trust assessment is validated.

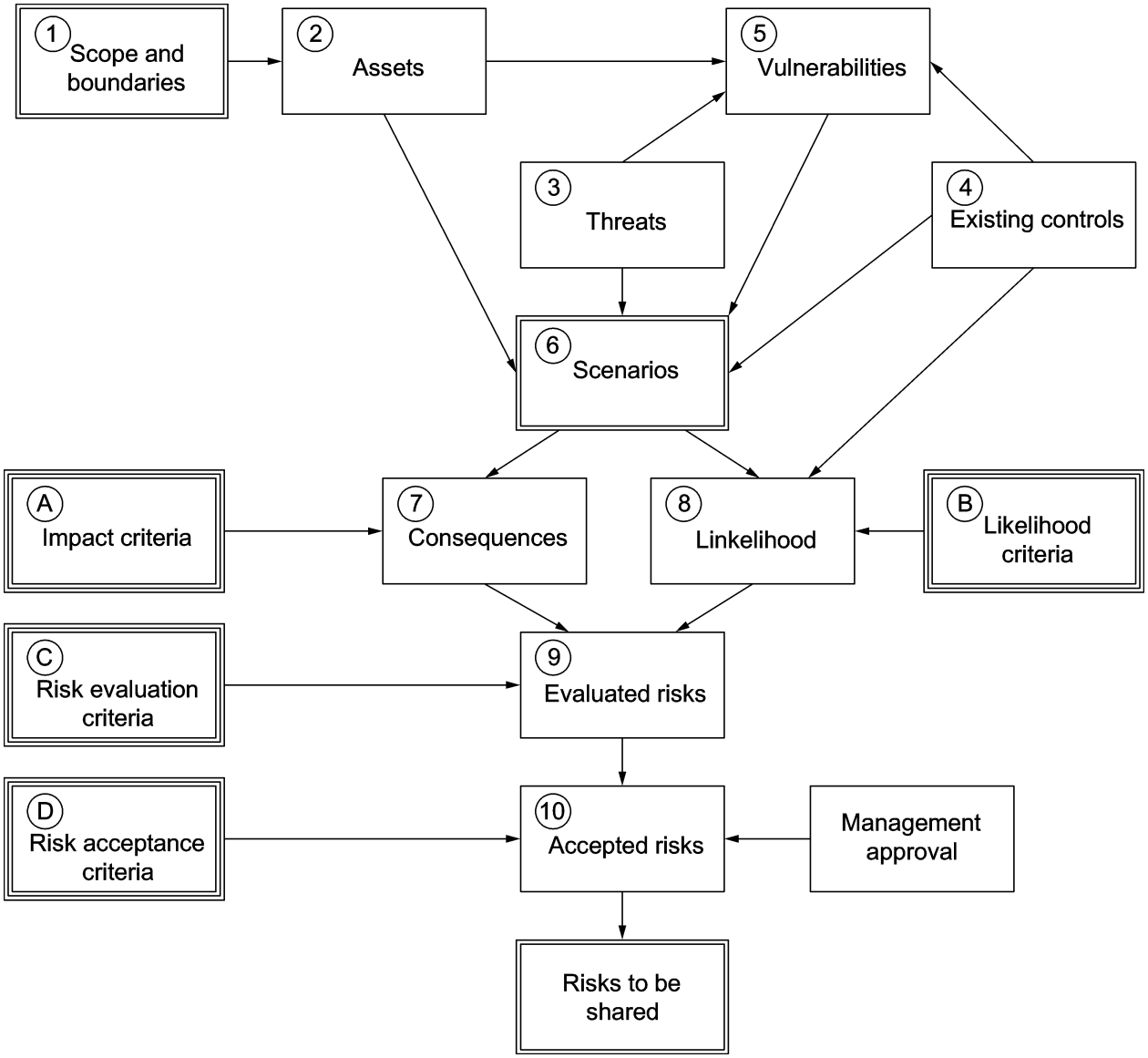
It is important to stress that this does not mean the organisation needs to know everything about its partners' security. What is needed is enough information to provide the required level of assurance, based on risk assessments.

Generic Interconnectivity cases may be constructed and assessed based on a common set of parameters and processes. When these cases apply to concrete interconnectivity cases, additional risk assessments are not necessary. An example of a generic interconnectivity case can be found in Annex A.

Organisations shall share this information to the required level with their partners in civil aviation. This European Standard specifies what information needs to be shared.

The underlying risk assessment process is compatible with ISO/IEC 27005:2011. This applies especially to the terminology used below.

Activities described in subsequent clauses may be conducted in a different order depending on the methodology used.



Key

Boxes with a double line indicate information to be shared as discussed in 4.3.3

Boxes with triple line indicate criteria that have to be established as part of the organisations risk management process. They are then used as fixed inputs to the individual risk assessments

Figure 1

A. Impact criteria

Impact criteria should be developed and specified in terms of the degree of damage or costs to the organisation caused by an information security event.

B. Likelihood evaluation criteria

Likelihood evaluation criteria should be developed that are understood in a similar way by all organisations involved and affected.

C. Risk evaluation criteria

Risk evaluation criteria should be developed for evaluating the organisation's information security risk considering the following:

— the strategic value of the business information process;

— the criticality of the information assets involved;

— legal and regulatory requirements, and contractual obligations;

— operational and business importance of availability, confidentiality and integrity;

— stakeholders' expectations and perceptions, and negative consequences for goodwill and reputation.

D. Risk acceptance criteria

Risk acceptance criteria should be developed and specified.

The **risk assessment process** should include the following steps.

Step 1. Scope and boundaries:

Function: To ensure that all relevant assets are taken into account and to assess risks that might arise through the organisation's boundaries. Additionally, the organisation should provide justification for any exclusion from the scope.

Results: The specification of the assessment scope and boundaries.

Step 2. Assets:

Function: To identify anything that has value to the organisation and which therefore requires protection. An asset shall have a single set of attributes that can be related to threats and vulnerabilities, to allow for analysis in the following steps.

Results: A list of assets to be risk-managed and a list of business processes related to assets and their relevance together with the relevant owners.

Step 3. Threats:

Function: To identify threats which have the potential to harm assets such as information, processes and systems. A threat may arise from within or from outside the organisation.

Results: A list of threats with the identification of threat type and source.

Step 4. Existing controls:

Function: To identify the existing or planned controls to see how they would reduce threat likelihoods and the ease of exploiting vulnerabilities, or the impact of an incident.

Results: A list of all existing and planned controls, their implementation and usage status.

Step 5. Vulnerabilities:

Function: To identify the features inherent to the assets and business processes can be exploited to deliver an attack. Not all vulnerabilities will be known at the time of the assessment (particularly the technical so-called zero-day vulnerabilities). This possibility needs to be addressed in security controls that allow for rapid reassessment of risk when they are discovered.

Results: A list of vulnerabilities in relation to assets, threats and controls.

Step 6. Scenarios:

Function: To identify the effects to the organisation that could be caused by a threat scenario. A threat scenario is the description of a threat exploiting a certain vulnerability or set of vulnerabilities to attack assets, despite existing controls.

Results: A list of threat scenarios with their effects related to the organisation's assets and business processes as well as those of other affected organisations.

Step 7. Consequences (assessment):

Function: To assess the consequences of each scenario, related to asset valuation and based on the business impact criteria.

Results: A list of assessed consequences of an incident scenario expressed with respect to assets and impact criteria.

Step 8. Likelihood:

Function: To assess the likelihood of each scenario occurring.

Results: Likelihood of threat scenarios (quantitative or qualitative).

Step 9. Evaluated Risk:

Function: To turn scenarios into evaluated risks based on the consequences and likelihood and the risk evaluation criteria defined during the context establishment. Aggregation of multiple low or medium risks may result in much higher overall risks and need to be addressed accordingly.

Results: A list of risks ranked according to risk evaluation criteria in relation to the threat scenarios that lead to those risks.

Step 10. Assessed Risk:

Function: To assess the list of ranked risks for acceptability based on the risk acceptance criteria previously defined.

Results: A list of assessed risks with related threat scenarios prioritised according to risk acceptance criteria. This will include information on consequences and likelihood for each risk.

4.3.2 Interoperability issues of risk assessments

Interoperability of risk assessments is an important issue within an environment that can be characterised as “system of systems”. In such an environment, risk assessments covering (sub-parts of) these systems will exist and it is important to identify the correspondences amongst risks identified and mitigation controls proposed in these assessments. This will allow for a coherent security policy for the entire complex system.

In order to achieve interoperability of risk assessments if different risk assessment methodologies are used,

— an understanding about the correspondence between the issues/notions/terms introduced in each of the underlying risk assessment methodologies needs to be established and

— the depth and width of each assessment needs to be compared and assessed in order to understand the assumed environment and the decisions regarding the security level of the system at hand.

Terminology issues might also be relevant, as even if the underlying methods are the same, it might happen that issues/notions/terms are being assigned different semantics.

To ensure comparability across multiple organisations, the organisation shall share at least information on scope and boundaries, threat scenarios and the assessed risks.

Information sharing should be based on the need to know principle to the extent necessary to deal with shared risks. Due to the sensitive nature of the catalogues of assessed risks, these results are usually developed by each organisation internally and are kept internally confidential.

The exchange of the information needs to be backed by appropriately binding confidentiality agreements between the organisations affected.

4.4 Selecting controls

Controls should be selected and implemented in line with the results of the information security risk assessments:

— controls from ISO/IEC 27002;

— controls supplementing those stated in ISO/IEC 27002. These are described in this European Standard as implementation specifications specific to aviation.

4.5 Levels of trust

4.5.1 Introduction

As stated above in 4.2, service delivery in aviation is defined by a high level of cooperation between the organisations involved. Guaranteeing the security of information and the systems that process that information within an individual organisation in a shared business process and the underlying proprietary business processes entails a high level of individual agreements and reviews.

Aviation organisations working in partnership should agree that levels of trust backed by reasonable evidence (from 1:1 relationships between two parties or through third-party verification) be recognised in further shared business processes (including with third parties).

The “Level of Trust of the organisation” (LoT-O) relates to the respective organisation. Classification always relates to the aspect of the shared process handled by the respective organisation. In particular, this takes into account potential information security risks that can arise for the respective party through linking business processes.

In addition to the organisation's overall assessment, a level of trust can also be classified for a specific subarea application area as described in the examples in Annex A.

4.5.2 Scale of trust levels

A six-point scale is used to classify the “Level of Trust”:

— Trusted;

— Limited Trust 0;

— Limited Trust 1;

— Limited Trust 2;

— Limited Trust 3;

— Untrusted.

The general definitions for the different levels should be as follows:

a) Trusted
The “trusted” category is only applied to an organisation's own departments, subsidiaries or business processes that are fully subject to their own security requirements. Third-party organisations cannot be categorised as “trusted”.

b) Limited Trust 0
The “Limited Trust 0” (LT0) category describes third-party organisations or organisations within the company that are not subject to proprietary security specifications but that meet the following requirements:

All the controls of this European Standard have been bindingly implemented. Compliance with the standard has been confirmed by a qualified information security auditor.

NOTE This can be for example a CISA, an ISO/IEC 27001 Lead Auditor or an equivalent professional.

c) Limited Trust 1
The “Limited Trust 1” (LT1) category describes third-party organisations or organisations within the company that are not subject to proprietary security specifications but that have a very high level of information security. This also applies to areas in which there are only indirect risks to partners.

EXAMPLE 1 linking networks

Under specific circumstances, organisations will grant access to their own applications to LT1 partners on a need-to-have basis without implementing application-specific protection measures (e.g. web application firewalls) and without further authentication at edge-of-network (e.g. on the firewall).

This procedure is only appropriate if the partner has a very high security level (LT1) and has implemented all relevant information security management system measures in this context.

d) Limited Trust 2
The “Limited Trust 2” (LT2) category describes third-party organisations or organisations within the company that are not subject to proprietary security specifications but that have a high level of information security.

EXAMPLE 2 linking networks

Under specific circumstances, organisations will grant access to their own applications to LT2 partners on a need-to-have basis, but require explicit authentication at edge-of-network (e.g. on the firewall) before establishing a connection.

This procedure is only appropriate if the partner has a high security level (LT2) and has implemented all key information security management system measures in this context (e.g. security incident management).

e) Limited Trust 3
The “limited trust 3” (LT3) category describes third-party organisations or organisations within the company that are not subject to proprietary security specifications but that have a basic level of information security.

EXAMPLE 3 linking networks

Under specific circumstances, organisations will grant access to their own applications to LT3 partners on a need-to-have basis, but require explicit authentication at edge-of-network (e.g. on the firewall) and other protection measures (e.g.

content filtering, input control, rights management, etc.) before establishing a connection. This procedure is only appropriate if the partner has implemented basic security measures (e.g. virus protection, back-up/restore, etc.) and a security management system.

f) Untrusted
This category describes all organisations that do not meet the requirements of the “Limited Trust 3” category.

4.5.3 Classification criteria

The details of the specific controls to be implemented for the different levels of trust should be worked out by the partners. An example of the Implementation of levels of Trust for an organisation can be found in Annex B.

4.6 Statement of applicability

The organisation should establish a “statement of applicability” in line with ISO/IEC 27001:2013, 4.2.1. j). The “statement of applicability”, should be made known to a partner if necessary.

4.7 Measurement and auditing of security

Measurement of effectiveness of the implemented controls should be carried out considering the guidelines within ISO/IEC 27004:2009.

Internal auditing activities should be carried out taking into account the additional indications presented in the ISO/IEC 27007:2011.

5 Security policy

5.1 Information security policy

Objective: To provide management direction and support for information security. Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organisation.

5.1.1 Information security policy document

The controls recommended in ISO/IEC 27002:2005, 5.1.1, apply accordingly.

Implementation guidance specific to aviation

The information security policy should be coordinated with the various security requirements in other areas of aviation (e.g.: physical security of secure areas). The distinctions and mutual dependencies between the individual areas should be documented in the policy or in a separate document.

5.1.2 Review of the information security policy

The controls (and all subsequent similar sentences) recommended in ISO/IEC 27002:2005, 5.1.2, apply accordingly.

6 Organisational security

6.1 Internal organisation

Objective: To manage information security within the organisation.

A management framework should be established to initiate and control the implementation of information security within the organisation.

Management should approve the information security policy, assign security roles and coordinate and review the implementation of security across the organisation.

If necessary, a source of specialist information security advice should be established and made available within the organisation. Contacts with external security specialists or groups, including relevant authorities, should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when handling information security incidents. A multi-disciplinary approach to information security should be encouraged.

6.1.1 Management commitment to information security

The controls recommended in ISO/IEC 27002:2005, 6.1.1, apply accordingly.

6.1.2 Information security co-ordination

The controls recommended in ISO/IEC 27002:2005, 6.1.2, apply accordingly.

6.1.3 Allocation of information security responsibilities

The controls recommended in ISO/IEC 27002:2005, 6.1.3, apply accordingly.

Implementation guidance specific to aviation

The organisation should appoint a person responsible to serve as a point of contact for strategic information security issues for third parties (e.g. for the planning and implementation of joint measures, etc.).

6.1.4 Authorisation process for information processing facilities

The controls recommended in ISO/IEC 27002:2005, 6.1.4, apply accordingly.

6.1.5 Confidentiality agreements

The controls recommended in ISO/IEC 27002:2005, 6.1.5, apply accordingly.

6.1.6 Contact with authorities

The controls recommended in ISO/IEC 27002:2005, 6.1.6, apply accordingly.

Implementation guidance specific to aviation

The organisation should cooperate with the appropriate specialist and supervisory authorities, particularly in the areas of IT security and prosecution, and with other critical infrastructures as well.

This includes contacts to authorities involved in critical infrastructure protection at the national and European level.

6.1.7 Contact with special interest groups

The controls recommended in ISO/IEC 27002:2005, 6.1.7, apply accordingly.

Other information specific to aviation

The organisation should also be aware of the criticality of its services at a regional, national and international level. It may therefore participate in associations and alliances as well as national and international programs to provide comprehensive support to air safety.

Given the special nature of threats to air traffic, the organisation may need to cooperate with other aviation organisations to present an agreed position. Such a position should form the basis for the selection of adequate, preventive and reactive measures:

— *ensuring the interoperability of the selected measures;*

— *fostering the cooperation in raising the alarm in the event of IT crises affecting multiple organisations and in crisis management;*

— *based on lessons learned jointly from security incidents.*

6.1.8 Independent review of information security

The controls recommended in ISO/IEC 27002:2005, 6.1.8, apply accordingly.

6.2 External parties

Objective: To maintain the security of the organisation's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

The security of the organisation's information and information processing facilities should not be reduced by the introduction of external party products or services.

Any access to the organisation's information processing facilities and processing and communication of information by external parties should be controlled.

Where there is a business need for working with external parties that may require access to the organisation's information and information processing facilities, or in obtaining or providing a product and service from or to an external party, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in an agreement with the external party.

6.2.1 Identification of risks related to external parties

The controls recommended in ISO/IEC 27002:2005, 6.2.1, apply accordingly.

6.2.2 Addressing security when dealing with customers

The controls recommended in ISO/IEC 27002:2005, 6.2.2, apply accordingly.

6.2.3 Addressing security in third party agreements

The controls recommended in ISO/IEC 27002:2005, 6.2.3, apply accordingly.

Implementation guidance specific to aviation

Disclosure of identities to partners should be part of the agreements. They should clearly specify the conditions of disclosure.

Responsibilities for the security of assets (see Clause 7) should be precisely defined by contract for business processes that affect multiple organisations.

7 Asset management

7.1 Responsibility for assets

Objective: To achieve and maintain appropriate protection of organisational assets.

All assets should be accounted for and have a nominated owner.

Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets.

7.1.1 Inventory of assets

The controls recommended in ISO/IEC 27002:2005, 7.1.1, apply accordingly.

7.1.2 Ownership of assets

The controls recommended in ISO/IEC 27002:2005, 7.1.2, apply accordingly.

Implementation guidance specific to aviation

Where assets are used in business processes shared by multiple organisations the interests of the other organisations should be taken into account by the owners.

7.1.3 Acceptable use of assets

The controls recommended in ISO/IEC 27002:2005, 7.1.3, apply accordingly.

7.2 Information classification

Objective: To ensure that information receives an appropriate level of protection.

Information should be classified to indicate the need, priorities, and expected degree of protection when handling the information.

Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification scheme should be used to define an appropriate set of protection levels and communicate the need for special handling measures.

7.2.1 Classification guidelines

The controls recommended in ISO/IEC 27002:2005, 7.2.1, apply accordingly.

Implementation guidance specific to aviation

To ensure comparability across multiple organisations, an organisation should classify the information it uses in shared business processes in a way that is acceptable to and agreed by all partners in the business process. Such information should be classified to ensure that national and commercial interests are appropriately protected.

Confidentiality classes:

Information should be assigned to confidentiality classes on the basis of the anticipated damage to business processes if this information becomes known to unauthorised parties.

Public: information that will not result in any damage to the business process/the organisations involved if it becomes known

Internal: information that will result in low to medium damage to the business process/the organisations involved if it becomes known

Confidential: information that can result in major damage to the business process/the organisations involved if it becomes known

Strictly confidential: information that can result in substantial to existential damage to the business process/the organisations involved if it becomes known

Generally, information should only be shared on a need-to-know basis.

Other information specific to aviation

Business needs and the business impacts associated with these needs may include the public interest in the safe and expeditious provision of the service as well as the commercial interests of the individual stakeholders involved.

7.2.2 Information labelling and handling

The controls recommended in ISO/IEC 27002:2005, 7.2.2, apply accordingly.

8 Human resources security

8.1 Prior to employment

Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

Security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment.

All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs.

Employees, contractors and third party users of information processing facilities should sign an agreement on their security roles and responsibilities.

8.1.1 Roles and responsibilities

The controls recommended in ISO/IEC 27002:2005, 8.1.1, apply accordingly.

8.1.2 Screening

The controls recommended in ISO/IEC 27002:2005, 8.1.2, apply accordingly.

Implementation guidance specific to aviation

Multiple organisations should ensure that background verification checks are carried out by partner organisations to an appropriate level, to ensure that access to data/ information shared between partner organisations takes account of the national and commercial interests of all stakeholders.

8.1.3 Terms and conditions of employment

The controls recommended in ISO/IEC 27002:2005, 8.1.3, apply accordingly.

8.2 During employment

Objective: To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error.

Management responsibilities should be defined to ensure that security is applied throughout an individual's employment within the organisation.

An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities should be provided to all employees, contractors and third party users to minimise possible security risks. A formal disciplinary process for handling security breaches should be established.

8.2.1 Management responsibilities

The controls recommended in ISO/IEC 27002:2005, 8.2.1, apply accordingly.

8.2.2 Information security awareness, education, and training

The controls recommended in ISO/IEC 27002:2005, 8.2.2, apply accordingly.

Implementation guidance specific to aviation

Employee awareness, education and training should be performed especially in line with the relevant security provisions of the ICAO Convention annexes and other documents.

The organisation should ensure that the competency of application developers will enable them to implement secure applications.

8.2.3 Disciplinary process

The controls recommended in ISO/IEC 27002:2005, 8.2.3, apply accordingly.

8.3 Termination or change of employment

Objective: To ensure that employees, contractors and third party users exit an organisation or change employment in an orderly manner.

Responsibilities should be in place to ensure an employees, contractors or third party users exit from the organisation is managed, and that the return of all equipment and the removal of all access rights are completed.

Change of responsibilities and employments within an organisation should be managed as the termination of the respective responsibility or employment in line with this section, and any new employments should be managed as described in 8.1.

8.3.1 Termination responsibilities

The controls recommended in ISO/IEC 27002:2005, 8.3.1, apply accordingly.

8.3.2 Return of assets

The controls recommended in ISO/IEC 27002:2005, 8.3.2, apply accordingly.

8.3.3 Removal of access rights

The controls recommended in ISO/IEC 27002:2005, 8.3.3, apply accordingly.

9 Physical and environmental security

9.1 Secure areas

Objective: To prevent unauthorised physical access, damage, and interference to the organisation's premises and information.

Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorised access, damage, and interference.

The protection provided should be commensurate with the identified risks.

9.1.1 Physical security perimeter

The controls recommended in ISO/IEC 27002:2005, 9.1.1, apply accordingly.

9.1.2 Physical entry controls

The controls recommended in ISO/IEC 27002:2005, 9.1.2, apply accordingly.

9.1.3 Securing offices, rooms, and facilities

The controls recommended in ISO/IEC 27002:2005, 9.1.3, apply accordingly.

9.1.4 Protecting against external and environmental threats

The controls recommended in ISO/IEC 27002:2005, 9.1.4, apply accordingly.

9.1.5 Working in secure areas

The controls recommended in ISO/IEC 27002:2005, 9.1.5, apply accordingly.

9.1.6 Public access, delivery, and loading areas

The controls recommended in ISO/IEC 27002:2005, 9.1.6, apply accordingly.

9.2 Equipment security

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities.

Equipment should be protected from physical and environmental threats.

Protection of equipment (including that used off-site, and the removal of property) is necessary to reduce the risk of unauthorised access to information and to protect against loss or damage. This should also consider equipment siting and disposal. Special controls may be required to protect against physical threats, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

9.2.1 Equipment siting and protection

The controls recommended in ISO/IEC 27002:2005, 9.2.1, apply accordingly.

Implementation guidance specific to aviation

Equipment deployed in publicly accessible areas should be protected against unauthorised access, e.g. with fixed and lockable casings for PCs, physical and/or logical protection of network sockets, etc.

9.2.2 Supporting utilities

The controls recommended in ISO/IEC 27002:2005, 9.2.2, apply accordingly.

9.2.3 Cabling security

The controls recommended in ISO/IEC 27002:2005, 9.2.3, apply accordingly.

9.2.4 Equipment maintenance

The controls recommended in ISO/IEC 27002:2005, 9.2.4, apply accordingly.

9.2.5 Security of equipment off-premises

The controls recommended in ISO/IEC 27002:2005, 9.2.5, apply accordingly.

9.2.6 Secure disposal or re-use of equipment

The controls recommended in ISO/IEC 27002:2005, 9.2.6, apply accordingly.

9.2.7 Removal of property

The controls recommended in ISO/IEC 27002:2005, 9.2.7, apply accordingly.

10 Communications and operations management

10.1 Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.

Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating procedures.

Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

10.1.1 Documented operating procedures

The controls recommended in ISO/IEC 27002:2005, 10.1.1, apply accordingly.

10.1.2 Change management

The controls recommended in ISO/IEC 27002:2005, 10.1.2, apply accordingly.

10.1.3 Segregation of duties

The controls recommended in ISO/IEC 27002:2005, 10.1.3, apply accordingly.

10.1.4 Separation of development, test, and operational facilities

The controls recommended in ISO/IEC 27002:2005, 10.1.4, apply accordingly.

10.2 Third party service delivery management

Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

The organisation should check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party.

10.2.1 Service delivery

The controls recommended in ISO/IEC 27002:2005, 10.2.1, apply accordingly.

10.2.2 Monitoring and review of third party services

The controls recommended in ISO/IEC 27002:2005, 10.2.2, apply accordingly.

10.2.3 Managing changes to third party services

The controls recommended in ISO/IEC 27002:2005, 10.2.3, apply accordingly.

10.3 System planning and acceptance

Objective: To minimise the risk of systems failures.

Advance planning and preparation are required to ensure the availability of adequate capacity and resources to deliver the required system performance.

Projections of future capacity requirements should be made, to reduce the risk of system overload.

The operational requirements of new systems should be established, documented, and tested prior to their acceptance and use.

10.3.1 Capacity management

The controls recommended in ISO/IEC 27002:2005, 10.3.1, apply accordingly.

10.3.2 System acceptance

The controls recommended in ISO/IEC 27002:2005, 10.3.2, apply accordingly.

Implementation guidance specific to aviation

The acceptance of systems used in processes performed across multiple organisations should include a formal process that ensures that the system acceptance requirements and criteria are in line with the shared risk assessment described in Clause 4.

10.4 Protection against malicious and mobile code

Objective: To protect the integrity of software and information.

Precautions are required to prevent and detect the introduction of malicious code and unauthorised mobile code.

Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. Users should be made aware of the dangers of malicious code. Managers should, where appropriate, introduce controls to prevent, detect, and remove malicious code and control mobile code.

10.4.1 Controls against malicious code

The controls recommended in ISO/IEC 27002:2005, 10.4.1, apply accordingly.

10.4.2 Controls against mobile code

The controls recommended in ISO/IEC 27002:2005, 10.4.2, apply accordingly.

10.5 Back-up

Objective: To maintain the integrity and availability of information and information processing facilities.

Routine procedures should be established to implement the agreed back-up policy and strategy (see also 14.1) for taking back-up copies of data and rehearsing their timely restoration.

10.5.1 Information back-up

The controls recommended in ISO/IEC 27002:2005, 10.5.1, apply accordingly.

10.6 Network security management

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

The secure management of networks, which may span organisational boundaries, requires careful consideration to dataflow, legal implications, monitoring, and protection.

Additional controls may also be required to protect sensitive information passing over public networks.

10.6.1 Network controls

The controls recommended in ISO/IEC 27002:2005, 10.6.1, apply accordingly.

10.6.2 Security of network services

The controls recommended in ISO/IEC 27002:2005, 10.6.2, apply accordingly.

10.7 Media handling

Objective: To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities.

Media should be controlled and physically protected.

Appropriate operating procedures should be established to protect documents, computer media (e.g. tapes, disks), input/output data and system documentation from unauthorised disclosure, modification, removal, and destruction.

10.7.1 Management of removable media

The controls recommended in ISO/IEC 27002:2005, 10.7.1, apply accordingly.

10.7.2 Disposal of media

The controls recommended in ISO/IEC 27002:2005, 10.7.2, apply accordingly.

10.7.3 Information handling procedures

The controls recommended in ISO/IEC 27002:2005, 10.7.3, apply accordingly.

10.7.4 Security of system documentation

The controls recommended in ISO/IEC 27002:2005, 10.7.4, apply accordingly.

10.8 Exchange of information

Objective: To maintain the security of information and software exchanged within an organisation and with any external entity.

Exchanges of information and software between organisations should be based on a formal exchange policy, carried out in line with exchange agreements, and should be compliant with any relevant legislation (see Clause 15).

Procedures and standards should be established to protect information and physical media containing information in transit.

10.8.1 Information exchange policies and procedures

The controls recommended in ISO/IEC 27002:2005, 10.8.1, apply accordingly.

10.8.2 Exchange agreements

The controls recommended in ISO/IEC 27002:2005, 10.8.2, apply accordingly.

10.8.3 Physical media in transit

The controls recommended in ISO/IEC 27002:2005, 10.8.3, apply accordingly.

10.8.4 Electronic messaging

The controls recommended in ISO/IEC 27002:2005, 10.8.4, apply accordingly.

10.8.5 Business information systems

The controls recommended in ISO/IEC 27002:2005, 10.8.5, apply accordingly.

10.9 Electronic commerce services

Objective: To ensure the security of electronic commerce services, and their secure use.

The security implications associated with using electronic commerce services, including online transactions, and the requirements for controls, should be considered. The integrity and availability of information electronically published through publicly available systems should also be considered.

10.9.1 Electronic commerce

The controls recommended in ISO/IEC 27002:2005, 10.9.1, apply accordingly.

10.9.2 Online Transactions

The controls recommended in ISO/IEC 27002:2005, 10.9.2, apply accordingly.

10.9.3 Publicly available information

The controls recommended in ISO/IEC 27002:2005, 10.9.3, apply accordingly.

10.10 Monitoring

Objective: To detect unauthorised information processing activities.

Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified.

An organisation should comply with all relevant legal requirements applicable to its monitoring and logging activities.

System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

10.10.1 Audit logging

The controls recommended in ISO/IEC 27002:2005, 10.10.1, apply accordingly.

10.10.2 Monitoring system use

The controls recommended in ISO/IEC 27002:2005, 10.10.2, apply accordingly.

10.10.3 Protection of log information

The controls recommended in ISO/IEC 27002:2005, 10.10.3, apply accordingly.

10.10.4 Administrator and operator logs

The controls recommended in ISO/IEC 27002:2005, 10.10.4, apply accordingly.

10.10.5 Fault logging

The controls recommended in ISO/IEC 27002:2005, 10.10.5, apply accordingly.

10.10.6 Clock synchronisation

The controls recommended in ISO/IEC 27002:2005, 10.10.6, apply accordingly.

11 Access control

11.1 Business requirement for access control

Objective: To control access to information.

Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements.

Access control rules should take account of policies for information dissemination and authorisation.

11.1.1 Access control policy

The controls recommended in ISO/IEC 27002:2005, 11.1.1, apply accordingly.

11.2 User access management

Objective: To ensure authorised user access and to prevent unauthorised access to information systems.

Formal procedures should be in place to control the allocation of access rights to information systems and services.

The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

11.2.1 User registration

The controls recommended in ISO/IEC 27002:2005, 11.2.1, apply accordingly.

11.2.2 Privilege management

The controls recommended in ISO/IEC 27002:2005, 11.2.2, apply accordingly.

11.2.3 User password management

The controls recommended in ISO/IEC 27002:2005, 11.2.3, apply accordingly.

11.2.4 Review of user access rights

The controls recommended in ISO/IEC 27002:2005, 11.2.4, apply accordingly.

11.2.5 Digital Identity Management

Control

The organisation should operate a central Identity Management System to provide management of digital identities, their authentication, authorisation, roles and privileges. Validity of an identity should be traceably predetermined relative to the source system of the identity.

Implementation guidance

Source databases (e.g. LDAP, Active Directory, distributed databases such as SAP, etc.) of the Identity Management System should provide a unique relation between an identity and an entity of the central Identity Management System.

The following key processes for managing digital identities should be implemented:

— generation of digital identities;

— change (customise, extend, delete) of attributes of a digital identity;

— disabling/deleting of digital identities;

— systematic provision of digital identity information (including authentication data) to connected systems;

— processing of information (from personnel administration and organisational management) for automated administration of user groups, roles, and privileges (authorisation profiles);

— systematic provisioning of user groups, roles, and privileges in connected systems.

Each of the above processes associated to the digital Identity Management should be documented and be traceable.

Validity should be implemented through an attached personnel management system or via a connected corporate directory.

Provided manual processes have to be used the validity period should not exceed a maximum of one year, Revalidation should be done at least once a year by a review.

11.2.6 Unique representation of entities across organisations

Control

Inter-organisational Identity Management should use a unique representation of entities.

Implementation guidance

In inter-organisational Identity Management, the following entities should be considered:

— People;

— Organisational units (e.g. departments) and roles;

— Systems.

Each entity of the organisation should be represented by a unique digital identity in the central Identity Management System.

Other information

A unique scheme for representing entities across organisations ensures compatibility and inter-operability in Identity Management.

11.3 User responsibilities

Objective: To prevent unauthorised user access, and compromise or theft of information and information processing facilities.

The co-operation of authorised users is essential for effective security.

Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

A clear desk and clear screen policy should be implemented to reduce the risk of unauthorised access or damage to papers, media, and information processing facilities.

11.3.1 Password use

The controls recommended in ISO/IEC 27002:2005, 11.3.1, apply accordingly.

11.3.2 Unattended user equipment

The controls recommended in ISO/IEC 27002:2005, 11.3.2, apply accordingly.

11.3.3 Clear desk and clear screen policy

The controls recommended in ISO/IEC 27002:2005, 11.3.3, apply accordingly.

11.4 Network access control

Objective: To prevent unauthorised access to networked services.

Access to both internal and external networked services should be controlled.

User access to networks and network services should not compromise the security of the network services by ensuring:

a) appropriate interfaces are in place between the organisation's network and networks owned by other organisations, and public networks;

b) appropriate authentication mechanisms are applied for users and equipment;

c) control of user access to information services in enforced.

11.4.1 Policy on use of network services

The controls recommended in ISO/IEC 27002:2005, 11.4.1, apply accordingly.

11.4.2 User authentication for external connections

The controls recommended in ISO/IEC 27002:2005, 11.4.2, apply accordingly.

11.4.3 Equipment identification in networks

The controls recommended in ISO/IEC 27002:2005, 11.4.3, apply accordingly.

11.4.4 Remote diagnostic and configuration port protection

The controls recommended in ISO/IEC 27002:2005, 11.4.4, apply accordingly.

11.4.5 Segregation in networks

The controls recommended in ISO/IEC 27002:2005, 11.4.5, apply accordingly.

11.4.6 Network connection control

The controls recommended in ISO/IEC 27002:2005, 11.4.6, apply accordingly.

11.4.7 Network routing control

The controls recommended in ISO/IEC 27002:2005, 11.4.7, apply accordingly.

11.5 Operating system access control

Objective: To prevent unauthorised access to operating systems.

Security facilities should be used to restrict access to operating systems to authorised users. The facilities should be capable of the following:

a) authenticating authorised users, in accordance with a defined access control policy;

b) recording successful and failed system authentication attempts;

c) recording the use of special system privileges;

d) issuing alarms when system security policies are breached;

e) providing appropriate means for authentication;

f) where appropriate, restricting the connection time of users.

11.5.1 Secure log-on procedures

The controls recommended in ISO/IEC 27002:2005, 11.5.1, apply accordingly.

11.5.2 User identification and authentication

The controls recommended in ISO/IEC 27002:2005, 11.5.2, apply accordingly.

11.5.3 Password management system

The controls recommended in ISO/IEC 27002:2005, 11.5.3, apply accordingly.

11.5.4 Use of system utilities

The controls recommended in ISO/IEC 27002:2005, 11.5.4, apply accordingly.

11.5.5 Session time-out

The controls recommended in ISO/IEC 27002:2005, 11.5.5, apply accordingly.

11.5.6 Limitation of connection time

The controls recommended in ISO/IEC 27002:2005, 11.5.6, apply accordingly.

11.6 Application and information access control

Objective: To prevent unauthorised access to information held in application systems.

Security facilities should be used to restrict access to and within application systems.

Logical access to application software and information should be restricted to authorised users.

Application systems should

a) control user access to information and application system functions, in accordance with a defined access control policy,

b) provide protection from unauthorised access by any utility, operating system software, and malicious software that is capable of overriding or bypassing system or application controls,

c) not compromise other systems with which information resources are shared.

11.6.1 Information access restriction

The controls recommended in ISO/IEC 27002:2005, 11.6.1, apply accordingly.

11.6.2 Sensitive system isolation

The controls recommended in ISO/IEC 27002:2005, 11.6.2, apply accordingly.

11.6.3 Web Application Firewalls

Control

The organisation should deploy Web Application Firewalls for the protection of web applications.

Implementation guidance

In order to proactively detect, log, and block attack attempts against web applications, the implementation guidance below should be followed:

— a baseline of signatures (or rules) covering common attacks such as Cross-Site Scripting (XSS) and SQL Injection attacks should be used and maintained up to date;

— attack signatures (or rules) should be customised for each web application and maintained up to date as the applications are modified.

Other information

An Application Firewall is a form of firewall that controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls which do not meet the configured policy. Specifically, Web Application Firewall technology provides the capability to apply a set of rules to HTTP/HTTPS conversations, in order to identify and block many attack attempts.

11.7 Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

The protection required should be commensurate with the risks these specific ways of working cause.

When using mobile computing the risks of working in an unprotected environment should be considered and appropriate protection applied. In the case of teleworking the organisation should apply protection to the teleworking site and ensure that suitable arrangements are in place for this way of working.

11.7.1 Mobile computing and communications

The controls recommended in ISO/IEC 27002:2005, 11.7.1, apply accordingly.

11.7.2 Teleworking

The controls recommended in ISO/IEC 27002:2005, 11.7.2, apply accordingly.

12 Information systems acquisition, development and maintenance

12.1 Security requirements of information systems

Objective: To ensure that security is an integral part of information systems.

Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements should be identified and agreed prior to the development and/or implementation of information systems.

All security requirements should be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

12.1.1 Security requirements analysis and specification

The controls recommended in ISO/IEC 27002:2005, 12.1.1, apply accordingly.

Implementation guidance specific to aviation

The security requirements and controls should take into account the security requirements of affected external organisations involved in joint business processes.

12.1.2 Policy for web applications / web services

A policy for web applications / web services should be available.

Implementation guidance specific to aviation

The policy should cover especially the authenticity and integrity of the information used in web applications.

12.2 Correct processing in applications

Objective: To prevent errors, loss, unauthorised modification or misuse of information in applications.

Appropriate controls should be designed into applications, including user developed applications to ensure correct processing. These controls should include the validation of input data, internal processing and output data.

Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls should be determined on the basis of security requirements and risk assessment.

12.2.1 Input data validation

The controls recommended in ISO/IEC 27002:2005, 12.2.1, apply accordingly.

12.2.2 Control of internal processing

The controls recommended in ISO/IEC 27002:2005, 12.2.2, apply accordingly.

12.2.3 Message integrity

The controls recommended in ISO/IEC 27002:2005, 12.2.3, apply accordingly.

12.2.4 Output data validation

The controls recommended in ISO/IEC 27002:2005, 12.2.4, apply accordingly.

12.2.5 Development of web applications

Control

For web applications, secure development guidelines should be applied.

Implementation guidance

The following key areas of web application development should be covered:

— Security Architecture;

— Authentication;

— Session Management;

— Access Control;

— Input Validation;

— Output Encoding/Escaping;

— Cryptography;

— Error Handling and Logging;

— Data Protection;

— Communication Security;

— HTTP Security;

— Security Configuration.

Relevant security measures should be implemented for each specific web application.

Other information

The OWASP Development Guide explains how to build web applications that meet or exceed the application-level security verification requirements defined in the OWASP Application Security Verification Standard (ASVS). Application-level security focusses on the analysis of components that comprise the application layer of the OSI model. The Guide was developed with the following objectives:

— use as a reference;

— use to make design decisions;

— use as a guidance.

12.2.6 Code Reviews

Control

The organisation should ensure that code reviews are performed for business critical applications as a part of the implementation and change processes.

Implementation guidance

The organisation should perform code reviews using either automated static code analysis tools, manual inspection, or both.

Other information

A code review is a systematic examination of source code. It is intended to find and fix mistakes overlooked in the initial development phase, improving both the overall quality of software and the developers' skills.

12.3 Cryptographic controls

Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.
A policy should be developed on the use of cryptographic controls. Key management should be in place to support the use of cryptographic techniques.

12.3.1 Policy on the use of cryptographic controls

The controls recommended in ISO/IEC 27002:2005, 12.3.1, apply accordingly.

12.3.2 Key management

The controls recommended in ISO/IEC 27002:2005, 12.3.2, apply accordingly.

Implementation guidance specific to aviation

The organisation should operate a central certificate management system which is compatible with those of their partners. If an organisation operates a PKI, there should be a central certificate management system.

The following documents should exist for a PKI, which does not only serve technical purposes:

— *Certificate Policy (CP);*

— *Certificate Practice Statement (CPS).*

For any PKI that is used only for technical purposes, technical documentation shall exist that document the operation and security standards of the PKI.

For the granting and revocation of certificates, verifiable processes should be in place.

Validity of certificates should be documented.

Other information

The most common format for certificates is the ITU X509 format.

12.4 Security of system files

Objective: To ensure the security of system files.

Access to system files and program source code should be controlled, and IT projects and support activities conducted in a secure manner. Care should be taken to avoid exposure of sensitive data in test environments.

12.4.1 Control of operational software

The controls recommended in ISO/IEC 27002:2005, 12.4.1, apply accordingly.

12.4.2 Protection of system test data

The controls recommended in ISO/IEC 27002:2005, 12.4.2, apply accordingly.

12.4.3 Access control to programme source code

The controls recommended in ISO/IEC 27002:2005, 12.4.3, apply accordingly.

12.5 Security in development and support processes

Objective: To maintain the security of application system software and information.

Project and support environments should be strictly controlled.

Managers responsible for application systems should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

12.5.1 Change control procedures

The controls recommended in ISO/IEC 27002:2005, 12.5.1, apply accordingly.

12.5.2 Technical review of applications after operating system changes

The controls recommended in ISO/IEC 27002:2005, 12.5.2, apply accordingly.

12.5.3 Restrictions on changes to software packages

The controls recommended in ISO/IEC 27002:2005, 12.5.3, apply accordingly.

12.5.4 Information leakage

The controls recommended in ISO/IEC 27002:2005, 12.5.4, apply accordingly.

12.5.5 Outsourced software development

The controls recommended in ISO/IEC 27002:2005, 12.5.5, apply accordingly.

12.6 Technical Vulnerability Management

Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems, and any other applications in use.

12.6.1 Control of technical vulnerabilities

The controls recommended in ISO/IEC 27002:2005, 12.6.1, apply accordingly.

12.6.2 Penetration Tests of Applications

Control

The organisation should perform regular penetration tests of applications (web applications, client-server applications, databases, etc.).

Implementation guidance

Regular application penetration tests should be scheduled for business critical applications each year. Additionally, penetration tests should be performed after any significant application upgrade or modification (e.g. new application added to the environment, major functionality added to an application, etc.).

The frequency and level of tests should be commensurate with the degree of cross-organisational application exposure. In general, automated security scanners may be used, but scan results shall be integrated by manual inspection (in order to remove false positives and false negatives) and thorough tests based on a formal methodology.

The team performing the penetration tests may be external or internal to the organisation. Its members should have proven experience in the proactive security field and should attend regular security training, in order to ensure actionable results.

Other information

A penetration test is a proactive security service that consists in the execution of thorough ethical hacking tests. It is based on inferential attack techniques aimed at identifying vulnerabilities that cannot be detected just by means of automated security scanners. If properly performed, application penetration tests provide an objective and repeatable evaluation of the security posture of applications. As such, they can detect design, implementation, and configuration security flaws.

12.6.3 Penetration Tests of Infrastructure

Control

The organisation should perform regular penetration tests of critical infrastructure (servers, workstations, network equipment).

Implementation guidance

Regular infrastructure penetration tests should be scheduled each year. Additionally, penetration tests should be performed after any significant infrastructure upgrade or modification (e.g. operating system upgrade, new sub-network added to the environment, etc.).

The level of tests should be commensurate with the degree of cross-organisational system and network exposure. In general, automated security scanners may be used, but scan results shall be integrated by manual inspection (in order to remove false positives and false negatives) and thorough tests based on a formal methodology.

External points of connection should be regularly tested for security vulnerabilities according to current standards.

The team performing the penetration tests may be external or internal to the organisation. Its members should have proven experience in the proactive security field and should attend regular security training, in order to ensure actionable results.

Other information

A penetration test is a proactive security service that consists in the execution of thorough ethical hacking tests. It is based on inferential attack techniques aimed at identifying vulnerabilities that cannot be detected just by means of automated security scanners. If properly performed, infrastructure penetration tests provide an objective and repeatable evaluation of the security posture of systems and networks in general. One of the most widely adopted methodologies on penetration testing is the Open Source Security Testing Methodology Manual (see www.osstmm.org).

13 Information security incident management

13.1 Reporting information security events and weaknesses

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Formal event reporting and escalation procedures should be in place. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of organisational assets. They should be required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

13.1.1 Reporting information security events

The controls recommended in ISO/IEC 27002:2005, 13.1.1, apply accordingly.

Implementation guidance specific to aviation

The organisation should establish a security incident response team that is appropriately trained and has the skills to react immediately to security incidents and to implement the necessary measures. If a business process is operated by multiple organisations, the individual security incident response teams in place should be coordinated – in line with the requirements and risk assessment for this business process – or a joint security incident response team should be put in place by the organisations involved if appropriate. The organisation should appoint a person responsible for security incident management issues and the contacts for operational performance of security incident management.

The organisation should also participate in security incident management systems for multiple organisations operated by the government or private aviation organisations.

An appropriate reaction time of the team should be ensured.

13.1.2 Reporting security weaknesses

The controls recommended in ISO/IEC 27002:2005, 13.1.2, apply accordingly.

Implementation guidance specific to aviation

The organisation should report identified security weaknesses in business processes affecting multiple organisations to the other organisations involved immediately.

The organisation should participate in committees and forums already in place operated by the government or private aviation organisations to exchange information on security weaknesses with each other – if necessary and of interest for third parties.

13.2 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.

Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents.

Where evidence is required, it should be collected to ensure compliance with legal requirements.

13.2.1 Responsibilities and procedures

The controls recommended in ISO/IEC 27002:2005, 13.2.1, apply accordingly.

13.2.2 Learning from information security incidents

The controls recommended in ISO/IEC 27002:2005, 13.2.2, apply accordingly.

Implementation guidance specific to aviation

The organisation should participate in organisations already existing and operated by the government or private aviation organisations to learn jointly from security incidents for general business processes in particular and to derive appropriate measures.

13.2.3 Collection of evidence

The controls recommended in ISO/IEC 27002:2005, 13.2.3, apply accordingly.

Implementation guidance specific to aviation

The organisation should cooperate with information collecting and sharing organisations that are operated by the government or private aviation organisations.

14 Business continuity management

14.1 Information security aspects of business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

A business continuity management process should be implemented to minimise the impact on the organisation and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls.

This process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.

The consequences of disasters, security failures, loss of service, and service availability should be subject to a business impact analysis. Business continuity plans should be developed and implemented to ensure timely resumption of essential operations. Information security should be an integral part of the overall business continuity process, and other management processes within the organisation.

Business continuity management should include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

14.1.1 Including information security in the business continuity management process

The controls recommended in ISO/IEC 27002:2005, 14.1.1, apply accordingly.

14.1.2 Business continuity and risk assessment

The controls recommended in ISO/IEC 27002:2005, 14.1.2, apply accordingly.

Implementation guidance specific to aviation

The organisations involved in a shared business process should conduct the business impact analysis for the whole process.

Other information specific to aviation

The business impact analysis should include the following steps according to ISO/IEC 27031:2011:

— *selection of the organisational units and (individual) processes to be included;*

— *criticality analysis for the assets in question;*

— *determination of criticality categories and damage scenarios;*

— *determination of the assessment periods to be observed;*

— *special dates and events;*

— *criticality analysis;*

— *prioritisation of individual processes;*

— *survey of resources for normal and emergency operations;*

— *criticality and restart times for resources;*

— *reporting.*

If assets are exchanged in an ongoing process such that changes cannot be ruled out in the business impact analysis, the business impact analysis should be repeated. The partners involved in the business process should be informed of this immediately.

14.1.3 Developing and implementing continuity plans including information security

The controls recommended in ISO/IEC 27002:2005, 14.1.3, apply accordingly.

14.1.4 Business continuity planning framework

The controls recommended in ISO/IEC 27002:2005, 14.1.4, apply accordingly.

Implementation guidance specific to aviation

The organisations involved should prepare a cross organisational continuity plan framework on the basis of the business impact analysis. At a minimum, this should cover

— *persons in positions of responsibility for collaborative decision making,*

— *emergency scenarios affecting multiple organisations,*

— *alternative measures,*

— *alternative operating procedures,*

— *structure of continuity plans.*

Owing to the required high availability of business processes in aviation, the organisation should document in its operational processes the circumstances under which continuity or crisis plans are activated.

14.1.5 Testing, maintaining and re-assessing business continuity plans

The controls recommended in ISO/IEC 27002:2005, 14.1.5, apply accordingly.

Implementation guidance specific to aviation

A timetable for reviewing and updating continuity plans should be included in the continuity plan framework.

Continuity plans should be regularly and jointly tested by the organisations involved. The information gathered should be used as input for improving and updating continuity plans. Testing should be documented. The organisations involved should perform the following actions to ensure the correct functioning of continuity contingency plans:

Testing and acceptance of the plans should take place before

— *putting a system/business process into operation,*

— *critical changes in systems and processes.*

The scope of testing should be based on the criticality of the business process.

15 Compliance

15.1 Compliance with legal requirements

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements.

Advice on specific legal requirements should be sought from the organisation's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow).

15.1.1 Identification of applicable legislation

The controls recommended in ISO/IEC 27002:2005, 15.1.1, apply accordingly.

Other information specific to aviation

Obligations of critical infrastructure protection at the national and European level might be considered.

15.1.2 Intellectual property rights (IPR)

The controls recommended in ISO/IEC 27002:2005, 15.1.2, apply accordingly.

15.1.3 Protection of organisational records

The controls recommended in ISO/IEC 27002:2005, 15.1.3, apply accordingly.

15.1.4 Data protection and privacy of personal information

The controls recommended in ISO/IEC 27002:2005, 15.1.4, apply accordingly.

15.1.5 Prevention of misuse of information processing facilities

The controls recommended in ISO/IEC 27002:2005, 15.1.5, apply accordingly.

15.1.6 Regulation of cryptographic controls

The controls recommended in ISO/IEC 27002:2005, 15.1.6, apply accordingly.

15.2 Compliance with security policies and standards, and technical compliance

Objective: To ensure compliance of systems with organisational security policies and standards.

The security of information systems should be regularly reviewed.

Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with applicable security implementation standards and documented security controls.

15.2.1 Compliance with security policies and standards

The controls recommended in ISO/IEC 27002:2005, 15.2.1, apply accordingly.

15.2.2 Technical compliance checking

The controls recommended in ISO/IEC 27002:2005, 15.2.2, apply accordingly.

15.3 Information systems audit considerations

Objective: To maximise the effectiveness of and to minimise interference to/from the information systems audit process.

There should be controls to safeguard operational systems and audit tools during information systems audits.

Protection is also required to safeguard the integrity and prevent misuse of audit tools.

15.3.1 Information systems audit controls

The controls recommended in ISO/IEC 27002:2005, 15.3.1, apply accordingly.

15.3.2 Protection of information systems audit tools

The controls recommended in ISO/IEC 27002:2005, 15.3.2, apply accordingly.

Annex A
(informative)

Implementation examples

A.1 General

Annex A provides examples for the definition of levels of trust for an organisation (LoT-O) and for specific application areas (LoT-A) that play a specific role for the close cooperation of organisations in air traffic.

“Levels of Trust” can be achieved by observing defined criteria.

The “Level of Trust of the organisation” (LoT-O) is decisive for an efficient collaboration, the selection of suitable partners and the comparability of partners.

The following Table A.1 provides an overview of an example for LoT-O. A detailed example can be found in Annex B.

Table A.1

Controls	LT0	LT1	LT2	LT3
5. Information Security Policy	Mandatory	Mandatory	Mandatory	Mandatory
6. Organisation of information security	Mandatory	Mainly	Mainly	Partly
7. Asset management	Mandatory	Mandatory	–	–
8. Human resources security	Mandatory	Mainly	Mainly	Partly
9. Physical and Environmental Security	Mandatory	Mainly	Partly	–
10. Communications and Operations Management	Mandatory	Mainly	Partly	Partly
11. Access Control	Mandatory	Mainly	Partly	Partly
12. Information systems acquisition, development and maintenance	Mandatory	Partly	Partly	–
13. Information security incident management	Mandatory	Mainly	Mainly	–
14. Business Continuity Management	Mandatory	Partly	Partly	–
15. Compliance	Mandatory	Mainly	Partly	Partly

If collaboration is pursued in one specific application area, a Level of Trust for this application area has to be determined. Examples are given in the subsequent sections.

By doing so it has to be considered that the Level of Trust of the application area (LoT-A) cannot exceed the Level of Trust of the communication partner (LoT-O) (Minimum-principle).

EXAMPLE The Level of Trust of a certain connection is determined as LT1. The communication partner as an organisation is however only rated as LT2. As a result, the connection can only achieve LT2. The respective security controls have to be applied accordingly.

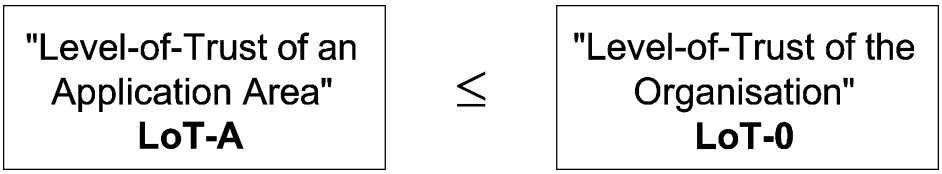


Figure A.1

A.2 Security of information in web applications and web services (LoT-A-WEB)

A.2.1 General

Objective: To ensure that information security is guaranteed within web applications/web services and the exchange between web applications/web services.

Aviation organisations are increasingly exchanging information via web applications/web services amongst themselves and with third parties. It is decisive for the security of the applications which internal information resources are provided to them.

A.2.2 Parameters for the Level of Trust of a web application / web service

The following parameters are used for the determination of the Level of Trust of the web application / web service:

— Policy for web applications / web services (see 12.1.2);

— Development of web applications (see 12.2.5);

— Code Reviews (see 12.2.6);

— Competency of application developers (see 8.2.2);

— Penetration tests of Applications (see 12.6.2);

— Penetration tests of Infrastructure (see 12.6.3);

— Web Application Firewalls (see 11.6.3).

A.2.3 Determination of the web application / the web service (LoT-A-WEB)

The Level of Trust of the web application / the web service is determined in Table A.2.

Table A.2

No.	Policy for web applica-tions / web services	Development of web applications	Code Reviews	Competence of Application Developers	Penetration tests of Applications	Penetration tests of infrastructures	Web Application Firewalls	Maximum achievable Level of Trust (LoT-A-WEB)
1	yes	yes	yes	yes	yes	yes	yes	LT1
2	yes	no	no	no	yes	yes	no	LT2
3	yes	no	no	no	yes	yes	no	LT3
4	yes	no	no	no	no	yes	no	LT3
5	no	n/a	n/a	n/a	n/a	n/a	n/a	UT
yes = Parameter fulfilled no = Parameter not fulfilled								

It should be considered that the level of Trust of the web application / the web service (LoT-A-WEB) cannot exceed the Level of Trust of the communication partner (LoT-O).

A.2.4 Consequences

The Level of Trust of the web application (LoT-A-WEB) has to reach at least the level of demand for protection that equates to the risk evaluation criteria already defined (see 4.3.1):

Table A.3

Demand for Protection (category)	Required LoT-A-WEB
Very high	LT1
High	LT1
Medium	LT2
Low	LT3

A.3 Connections between multiple organisations /external connections (LoT-A-NET)

Objective: To ensure, that cross organisational / External connections are operated in a secure way.

A.3.1 Determination of the necessary protection controls

A.3.1.1 General

The controls that have to be implemented for the protection of external connections to the organisations internal, should be determined according to the process in Figure A.2.

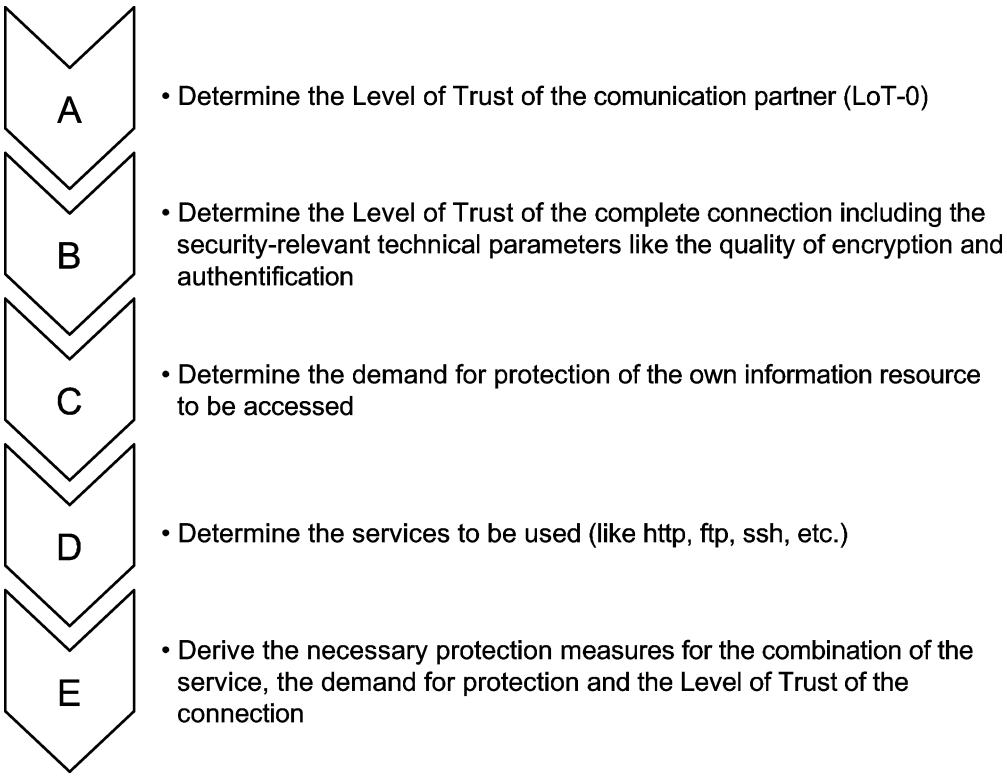


Figure A.2

A) Determine the Level of Trust of the communication partner (LoT-O)

The level of trust should be determined according to the rules described in 4.5.

B) Determine the Level of Trust of the connection (LoT-A-NET)

The Level of Trust of the connection should be determined based on the following parameters.

A.3.1.2 Identity of the User

Regarding the identity of the user, three categories should be distinguished:

a) Partner: natural person associated with the partner organisation;

b) Internal: natural person associated with the own organisation;

c) Technical: Entity of the partner, i.e. an IT system rather than a natural person.

A.3.1.3 Owner of the terminal device

Regarding the ownership of the terminal device – i.e. power of control over the devices - three categories should be distinguished:

a) Partner;

b) terminal devices administrated by the own organisation, either physical or virtualised (provided the device is appropriately isolated);

c) external terminal devices.

A.3.1.4 Connection point / Protection of the terminal device:

Regarding the connection point, respectively the protection of the terminal device four categories should be distinguished.

a) Partner network, protected (PPr):
Defines terminal devices and network connection points, that are physically protected from unauthorised access. This category includes also wireless connection points that are protected via state of the art cryptographic measures.

b) Partner network, public (PPu):
Defines permanently installed terminal devices and network connection points, that are located in publicly accessible areas, like service counter areas, foyers, lobby halls, airport terminals etc. This category includes also wireless connection points that are not protected by state of the art cryptographic measures.

c) Public, protected (PuP):
Defines terminal devices like mobile devices of field engineers and travellers, who are temporarily operated via public network connection points and who are protected by the user while in use respectively by physical protection from unauthorised access while not in use.

d) Public, unprotected (PuU):
Defines completely unprotected terminal devices, networks and network access points like publicly accessible internet terminals.

A.3.1.5 Authentication of the connection

Regarding the authentication, three categories should be distinguished:

a) User/PW: User identification and password;

b) 2-Factor authentication;

c) Certificate based authentication.

A.3.1.6 Transfer net

Regarding the transfer nets, three main categories should be distinguished which should be substructured based on application of cryptography:

a) Internet:

1) encrypted, Site-to-Site VPN (sts);

2) encrypted, Client-to-Site VPN (cts);

3) unencrypted (u);

b) Leased line (private or virtual private networks, like Leased Lines, own Backbone, MPLS VPN, SITA, Starnet, etc.):

1) encrypted (v);

2) unencrypted (u);

c) Dialup line (like ISDN/PSTN):

1) encrypted (v);

2) unencrypted (u).

The following Table A.4 shows the maximum Level of Trust depending on the respective technical parameters.

Table A.4

No.	Application Scenario	Identity of the user	Terminal Device Owner	Connection point / Terminal Device Protection	Authentifi-cation	Transfer Net	Maximum achievable Level of Trust
1	Staff of external partner, terminal devices of partner in the protected area of the partner network	Partner	Partner	PPr	User/PW, 2-Factor	Internet (sts), Leased Line (v,u), Dialup Line (v,u)	LT1
2	Staff of external partner with specially protected mobile devices (under staff (not partner control) any connection point	Partner	Own	PPr, PPu, PuP	2-Factor	Internet (sts), Leased Line (v,u), Dialup Line (v,u)	LT1
3	Staff of external partner with partner terminal device in the unprotected area of the partner-network, 2-factor authentification	Partner	Partner	PPu	2-Factor	Internet (sts), Leased Line (v,u), Dialup Line (v,u)	LT2
4	Staff of external partner with partner terminal device in the unprotected area of the partner network	Partner	Partner	PPu	User/PW	Internet (sts), Leased Line (v,u),	LT3

No.	Application Scenario	Identity of the user	Terminal Device Owner	Connection point / Terminal Device Protection	Authentifi-cation	Transfer Net	Maximum achievable Level of Trust
5	Mobile staff of the external partner with partner terminal device, unprotected connection point	Partner	Partner	PuP	2-Factor	Internet (cts)	LT2
6	Staff of external partner with any terminal device, any connection point	Partner	Foreign	PuU	2-Factor	Internet (cts)	LT3
7	System coupling, technical identities only, access from the partner computer centre only permitted for fixed IP-addresses	Partner system	Partner	PPr	User/PW, Certificate	Internet (sts), Leased Line (v,u),	LT1
8	System coupling, technical identities only, access from the publicly accessible area of the partner, certificate-based authentication	Partner system	Partner	PPu	Certificate	Internet (sts), Leased Line (v,u),	LT2

No.	Application Scenario	Identity of the user	Terminal Device Owner	Connection point / Terminal Device Protection	Authentifi-cation	Transfer Net	Maximum achievable Level of Trust
9	System coupling, technical identities only, access from the publicly accessible area of the partner, only permitted for fixed IP-addresses	Partner system	Partner	PPu	User/PW	Internet (sts), Leased Line (v,u),	LT3
10	Own staff travelling or working from home office with specially protected organisation-owned mobile devices, any connection point	Internal	Own	PPr, PPu, PuP	2-Factor	Internet (sts), Leased Line (v,u), Dialup Line (v,u)	T
11	Own staff with organisation-owned terminal device, connection via dialup line	Internal	Own	PPr, PPu, PuP	2-Factor	Dialup Line (v,u)	T
12	Own staff in the protected area of the partner network using a partner terminal device	Internal	Partner	PPr	User/PW, 2-Factor	Internet (sts), Leased Line (v,u), Dialup Line (v,u)	LT1
13	Own staff using a partner terminal device in the unprotected area of the partner	Internal	Partner	PPu	2-Factor	Internet (sts), Leased Line (v,u), Dialup Line (v,u)	LT1
14	Own staff using a partner terminal device in the unprotected area of the partner	Internal	Partner	PPu	User/PW	Internet (sts), Dialup Line (v,u)	LT3
15	Own staff using any terminal device, any connection point	Internal	Foreign	PuU	2-Factor	Internet (cts)	LT3

No.	Application Scenario	Identity of the user	Terminal Device Owner	Connection point / Terminal Device Protection	Authentifi-cation	Transfer Net	Maximum achievable Level of Trust
16	Own staff using any terminal device, connection via dialup line	Internal	Foreign	PuU	User/PW	Dialup Line (v,u)	LT3

Key
PuP = Public, Unprotected
PuU = Public, Unprotected
PPr = Partner net, Protected
PPu = Partner net, Unprotected
sts = Site-to-Site VPN
cts = Client-to-Site VPN
v = Encrypted
u = Unencrypted

C) Determine the demand for protection of the own information resource to be accessed

The demand for protection of an own information resource should be determined according to 4.3.1.

D) Determine the services to be used

The service needs to be identifiable from the connection pursued.

E) Derive the protection controls

Each organisation should define the necessary protection controls based on the demand for protection of the internal information resource and the Level of Trust of the connection for the relevant service. Additional Controls

A.3.2 Effects of the coupling of networks

Implications for classification LoT-A with "Limited Trust 1 or better"

— Organisations should allow the access by communication partners with a classification of "Limited Trust 1 or better" on applications according to the need-to-have principle. The connection shall be protected by a firewall. Any additional application-specific protection control at the network boundary (such as reverse proxy) shall not be applied mandatorily.

Implications for classification LoT-A with „Limited Trust 2"

— Organisations should allow the access by communication partners with a classification of "Limited Trust 2" to allow web applications and web services according to the need-to-have principle. The connection should be protected by a firewall and a reverse proxy to ensure that connections can be established only if the user has successfully authenticated at the network perimeter.

— An organisation should not allow access by a "Limited Trust 2" communication partner to data classified with very high protection requirements, if resulting security implications through external access were not examined in advance as part of a formal risk assessment.

Implications for classification LoT-A with "Limited Trust 3"

— Organisations should allow the access by communication partners with a classification of “Limited Trust 3” to internal applications only if a suitable proxy system on application level ensures that the application can only be used in the predetermined way.

— In general, all applications that are usable by communication partners with a classification of “Limited Trust 3” as part of an external communication connection shall be formally examined and tested in advance for their resistance against abuse attempts.

— An organisation should not allow access by communication partners with a classification of “Limited Trust 3” to data with high or very high protection requirements if resulting security implications through external access were not examined in advance as part of a formal risk assessment.

A.4 Certificates / Public Key Infrastructure (LoT-A-PKI)

Objective: Definition of cross-organisational agreements between companies to ensure their PKI solutions meet the protection requirements of cross-organisational business transactions for the secure exchange of information.

A.4.1 Parameters for the Level of Trust of the certificate management

The following parameters are used for the determination of the Level of Trust of Certificates / Public Key Infrastructure (PKI):

— Public key Infrastructure Management Policy / Certificates (see 12.3.1);

— Key management (see 12.3.2);

— Management of certificates (see 12.3.2).

A.4.2 Determination of the Level of Trust of the certificate management (LoT-A-PKI)

The trust of identity management is determined in Table A.5.

Table A.5

No.	PKI/Certificate Policy	Key management	Management of Certificates	Maximum achievable Level of Trust (LoT-A-PKI)
1	yes	yes (CP/CPS known to the partner)	yes	LT1
2	yes	yes	yes	LT2

A.4.3 Effects: Recognition of Certificates / PK

Recognition of Certificates / PKI should be based upon the classification of other organisations.

Impact on classification LoT-A-PKI with „Limited Trust 1“

— An organisation should acknowledge the PKI of another organisation classified either as „LoT-O 0“, or „LoT-O 1“ for all application areas (e.g. through cross-certification or import of the relevant CA certificates), e. g for

  — Authentication of Systems per Device Certificates,

— Code-Signatures,

— Authentication / Signature and Encryption.

Impact on classification LoT-A-PKI with „Limited Trust 2“

— An organisation should recognise certificates of individuals of an organisation classified as „LoT-O 2“ or higher subsequent to prior review. This is exclusively applicable for signature & encryption of information (e.g. email, documents).

A.5 Identity Management (LoT-A-IDM)

Objective: To define clear interfaces (technologies and standards) for multi-system platforms for the central management of users and roles, their accounts and possibly their authorisations in business processes in which multiple organisations participate (federation).

Alternative: Definition of unique and secure interfaces (technologies and standards) of system-wide platforms for centralised management of users, roles, accounts and permissions in cross-organisational business processes (Federation)

A.5.1 Parameters for the Level of Trust of Identity Management

The following parameters are used to determine the Level of Trust of the Identity Management:

— Access Control Policy (see 11.1.1);

— Digital Identity Management System (DIM) (see 11.2.5);

— Unique representation of entities across organisations (see 11.2.6);

— DIM – Administration of identities (see 11.2.5);

— Privilege management – revocation of identities (see 11.2.2);

— DIM – Traceability of entity validity (see 11.2.5);

— Third party agreements - Disclosure of identities (see 6.2.3).

A.5.2 Determination of the Level of Trust of the Identity Management (LoT-A-IDM)

The Level of Trust of the Identity Management is determined in Table A.6.

Table A.6

No.	Access Control Policy	Digital Identity Management System	Unique representation of entities across organisations	Administration of identities	Revocation of identities	Traceability of entity validity	Disclosure of identities	Maximum achievable Level of Trust (LoT-A-IDM)
1	yes	yes	yes	yes	yes	via an attached Corporate Directory or an attached Human Resource-Management-System	yes	LT1
2	yes	no	yes	no	yes	Validity < 365 d or annual check	yes	LT2
3	all other combinations							UT
yes = parameter met no = parameter not met								

It has to be kept in mind, that the level of trust of the Identity Management (LoT-A- IDM) cannot exceed the level of trust of the communication partner (LoT-O) (see also 16.1).

A.5.3 Effects: Recognition of identities

Recognition of identities should be based upon the classification of other organisations.

Impact on classification LoT-A-IDM with "Limited Trust 0", "Limited Trust 1" and "Limited Trust 2"

— An organisation should recognise identities of an organisation classified as "Limited Trust 0", "Limited Trust 1" or "Limited Trust 2" through a simple approval process. A coupling of IDM systems of different organisations (Federation) can only take place at LT 0 or LT1.

Impact on classification LoT-A-IDM with "Limited Trust 3" or "Untrusted"

Identities of an organisation classified as "Limited Trust 3" or "Untrusted" should be treated as external identities based on the controls defined in this European Standard and receive a digital identity with a unique identifier based upon an approval procedure, which is to be defined.

Annex B
(informative)

Level of Trust – Implementation Example

This table is an example of the security requirements appropriate to different levels of trust. It shows which controls need to be considered for implementation in a multi-party relationship which has been designated with the particular trust level. Level 0 is not included because at that level all controls will have been considered.

Table B.1

No. CoP.	Control	LT 1	LT 2	LT 3
5	**Information security policy**			
5.1	***Information security policy*** *Objective: To provide management direction and support for information security.*			
Controls				
5.1.1	Information security policy document	x	x	x
5.1.2	Review of the information security policy	x	x	x
6	**Organisational security**			
6.1	***Internal organisation*** *To manage information security within the organisation.*			
Controls				
6.1.1	Management commitment to information security	x	x	x
6.1.2	Information security co-ordination	x	x	x
6.1.3	Allocation of information security responsibilities	x	x	x
6.1.4	Authorisation process for information processing facilities	x	x	
6.1.5	Confidentiality agreements	x	x	x
6.1.6	Contact with authorities	x		
6.1.7	Contact with special interest groups	x		
6.1.8	Independent review of information security			
6.2	***External parties*** *Objective: To maintain the security of the organisation's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.*			
Controls				
6.2.1	Identification of risks related to external parties	x	x	x
6.2.2	Addressing security when dealing with customers	x	x	

No. CoP.	Control	LT 1	LT 2	LT 3
6.2.3	Addressing security in third party agreements	x	x	
7	**Asset management**			
7.1	***Responsibility for assets*** *Objective: To achieve and maintain appropriate protection of organisational assets.*			
Controls				
7.1.1	Inventory of assets	x	x	
7.1.2	Ownership of assets	x		
7.1.3	Acceptable use of assets	x		
7.2	***Information classification*** *Objective: To ensure that information receives an appropriate level of protection.*			
Controls				
7.2.1	Classification guidelines	x	x	x
7.2.2	Information labelling and handling	x	x	
8	**Human resources security**			
8.1	***Prior to employment*** *Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.*			
Controls				
8.1.1	Roles and responsibilities	x		
8.1.2	Screening	x	x	
8.1.3	Terms and conditions of employment			
8.2	***During employment*** *Objective: To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error.*			
Controls				
8.2.1	Management responsibilities	x	x	
8.2.2	Information security awareness, education, and training	x	x	x
8.2.3	Disciplinary process			

No. CoP.	Control	LT 1	LT 2	LT 3
8.3	***Termination or change of employment*** *Objective: To ensure that employees, contractors and third party users exit an organisation or change employment in an orderly manner.*			
Controls				
8.3.1	Termination responsibilities	x		
8.3.2	Return of assets	x	x	
8.3.3	Removal of access rights	x	x	x

9	**Physical and environmental security**			
9.1	***Secure areas*** *Objective: To prevent unauthorised physical access, damage, and interference to the organisation's premises and information.*			
Controls				
9.1.1	Physical security perimeter	x	x	x
9.1.2	Physical entry controls	x	x	x
9.1.3	Securing offices, rooms, and facilities	x		
9.1.4	Protecting against external and environmental threats	x		
9.1.5	Working in secure areas			
9.1.6	Public access, delivery, and loading areas	x		

9.2	***Equipment security*** *Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities.*			
Controls				
9.2.1	Equipment siting and protection	x	x	
9.2.2	Supporting utilities	x	x	x
9.2.3	Cabling security	x		
9.2.4	Equipment maintenance	x		
9.2.5	Security of equipment off-premises	x		
9.2.6	Secure disposal or re-use of equipment	x		
9.2.7	Removal of property			

10	**Communications and operations management**			
10.1	***Operational procedures and responsibilities*** *Objective: To ensure the correct and secure operation of information processing facilities.*			
Controls				
10.1.1	Documented operating procedures	x	x	
10.1.2	Change management	x		

No. CoP.	Control	LT 1	LT 2	LT 3
10.1.3	Segregation of duties			
10.1.4	Separation of development, test, and operational facilities			

10.2	***Third party service delivery management*** *Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.*			
Controls				
10.2.1	Service delivery	x		
10.2.2	Monitoring and review of third party services			
10.2.3	Managing changes to third party services			

10.3	***System planning and acceptance*** *Objective: To minimise the risk of systems failures.*			
Controls				
10.3.1	Capacity management			
10.3.2	System acceptance	x		

10.4	***Protection against malicious and mobile code*** *Objective: To protect the integrity of software and information.*			
Controls				
10.4.1	Controls against malicious code	x	x	x
10.4.2	Controls against mobile code			

10.5	***11.5 Backup*** *Objective: To maintain the integrity and availability of information and information processing facilities.*			
Controls				
10.5.1	Information back-up	x	x	

10.6	***Network security management*** *Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.*			
Controls				
10.6.1	Network controls	x	x	x
10.6.2	Security of network services			

No. CoP.	Control	LT 1	LT 2	LT 3
10.7	***Media handling*** *Objective: To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities.*			
Controls				
10.7.1	Management of removable media	x		
10.7.2	Disposal of media	x		
10.7.3	Information handling procedures			
10.7.4	Security of system documentation			

10.8	***Exchange of information*** *Objective: To maintain the security of information and software exchanged within an organisation and with any external entity.*			
Controls				
10.8.1	Information exchange policies and procedures	x	x	
10.8.2	Exchange agreements	x		
10.8.3	Physical media in transit			
10.8.4	Electronic messaging			
10.8.5	Business information systems			

10.9	***Electronic commerce services*** *Objective: To ensure the security of electronic commerce services, and their secure use.*			
Controls				
10.9.1	Electronic commerce	x	x	
10.9.2	Online Transactions	x	x	
10.9.3	Publicly available information	x	x	

10.10	***Monitoring*** *Objective: To detect unauthorised information processing activities.*			
Controls				
10.10.1	Audit logging	x		
10.10.2	Monitoring system use			
10.10.3	Protection of log information			
10.10.4	Administrator and operator logs	x	x	
10.10.5	Fault logging			
10.10.6	Clock synchronisation	x		

11	**Access control**			

No. CoP.	Control	LT 1	LT 2	LT 3
11.1	***Business requirement for access control*** *Objective: To control access to information.*			
Controls				
11.1.1	Access control policy	x	x	x

11.2	***User access management*** *Objective: To ensure authorised user access and to prevent unauthorised access to information systems.*			
Controls				
11.2.1	User registration	x	x	x
11.2.2	Privilege management	x	x	x
11.2.3	User password management	x	x	
11.2.4	Review of user access rights	x	x	
11.2.5	Digital Identity Management	see Annex A		
11.2.6	Unique representation of entities across organisations	see Annex A		

11.3	***User responsibilities*** *Objective: To prevent unauthorised user access, and compromise or theft of information and information processing facilities.*			
Controls				
11.3.1	Password use	x	x	x
11.3.2	Unattended user equipment	x	x	x
11.3.3	Clear desk and clear screen policy			

11.4	***Network access control*** *Objective: To prevent unauthorised access to networked services.*			
Controls				
11.4.1	Policy on use of network services			
11.4.2	User authentication for external connections	x	x	x
11.4.3	Equipment identification in networks			
11.4.4	Remote diagnostic and configuration port protection			
11.4.5	Segregation in networks			
11.4.6	Network connection control	x	x	x
11.4.7	Network routing control			

11.5	***Operating system access control*** *Objective: To prevent unauthorised access to operating systems.*			
Controls				

No. CoP.	Control	LT 1	LT 2	LT 3
11.5.1	Secure log-on procedures	x	x	x
11.5.2	User identification and authentication	x	x	x
11.5.3	Password management system	x	x	x
11.5.4	Use of system utilities			
11.5.5	Session time-out			
11.5.6	Limitation of connection time			

11.6	***Application and information access control*** *Objective: To prevent unauthorised access to information held in application systems.*			
Controls				
11.6.1	Information access restriction	x	x	x
11.6.2	Sensitive system isolation			
11.6.3	Web Application Firewall	see Annex A		

11.7	***Mobile computing and teleworking*** *Objective: To ensure information security when using mobile computing and teleworking facilities.*			
Controls				
11.7.1	Mobile computing and communications	x		
11.7.2	Teleworking			

12	**Information systems acquisition, development and maintenance**			
12.1	***Security requirements of information systems*** *Objective: To ensure that security is an integral part of information systems.*			
Controls				
12.1.1	Security requirements analysis and specification	x		
12.1.2	Policy for web applications / web services	x		

12.2	***Correct processing in applications*** *Objective: To prevent errors, loss, unauthorised modification or misuse of information in applications.*			
Controls				
12.2.1	Input data validation	x		
12.2.2	Control of internal processing			
12.2.3	Message integrity			
12.2.4	Output data validation			
12.2.5	Development of web applications	see Annex A		

No. CoP.	Control	LT 1	LT 2	LT 3
12.2.6	Code Reviews	see Annex A		

12.3	***Cryptographic controls*** *Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.*			
Controls				
12.3.1	Policy on the use of cryptographic controls	x		
12.3.2	Key management	x		

12.4	***Security of system files*** *Objective: To ensure the security of system files.*			
Controls				
12.4.1	Control of operational software			
12.4.2	Protection of system test data			
12.4.3	Access control to program source code			

12.5	***Security in development and support processes*** *Objective: To maintain the security of application system software and information.*			
Controls				
12.5.1	Change control procedures	x		
12.5.2	Technical review of applications after operating system changes	x		
12.5.3	Restrictions on changes to software packages			
12.5.4	Information leakage			
12.5.5	Outsourced software development			

12.6	***Technical Vulnerability Management*** *Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.*			
Controls				
12.6.1	Control of technical vulnerabilities	x	x	x
12.6.2	Penetration Tests of Applications	see Annex A		
12.6.3	Penetration Tests of Infrastructure	see Annex A		

13	**Information security incident management**			
13.1	***Reporting information security events and weaknesses*** *Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.*			

No. CoP.	Control	LT 1	LT 2	LT 3
Controls				
13.1.1	Reporting information security events	x	x	
13.1.2	Reporting security weaknesses	x		

13.2	*Management of information security incidents and improvements* *Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.*			
Controls				
13.2.1	Responsibilities and procedures	x		
13.2.2	Learning from information security incidents	x		
13.2.3	Collection of evidence			

14	**Business continuity management**			
14.1	***Information security aspects of business continuity management*** *Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.*			
Controls				
14.1.1	Including information security in the business continuity management process			
14.1.2	Business continuity and risk assessment			
14.1.3	Developing and implementing continuity plans including information security			
14.1.4	Business continuity planning framework			
14.1.5	Testing, maintaining and re-assessing business continuity plans			

15	**Compliance**			
15.1	***Compliance with legal requirements*** *Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.*			
Controls				
15.1.1	Identification of applicable legislation			
15.1.2	Intellectual property rights (IPR)			
15.1.3	Protection of organisational records			
15.1.4	Data protection and privacy of personal information	x	x	x
15.1.5	Prevention of misuse of information processing facilities			
15.1.6	Regulation of cryptographic controls			

No. CoP.	Control	LT 1	LT 2	LT 3
15.2	***Compliance with security policies and standards, and technical compliance*** *Objective: To ensure compliance of systems with organisational security policies and standards.*			
Controls				
15.2.1	Compliance with security policies and standards	x	x	x
15.2.2	Technical compliance checking	x	x	x

15.3	***Information systems audit considerations*** *Objective: To maximise the effectiveness of and to minimise interference to/from the information systems audit process.*			
Controls				
15.3.1	Information systems audit controls			
15.3.2	Protection of information systems audit tools			

Bibliography

[1] ICAO Annex 17 to the Convention on International Civil Aviation – Security – Safeguarding International Civil Aviation Against Acts of Unlawful Interference

[2] ICAO Doc 8973, *Aviation Security Manual (Restricted)*

[3] ITU X 509, *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*

[4] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

[5] ISO/IEC 27004:2009, *Information technology — Security techniques — Information security management — Measurement*

[6] ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

[7] ISO/IEC 27007:2011, *Information technology — Security techniques — Guidelines for information security management systems auditing*

[8] ISO/IEC 27031:2011, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™