

# **Application Service Provider Security Standard**

---

# Application Service Provider Security Standard

Published 16 May 2009

Copyright © 2001, 2002, 2003, 2009 Frank O'Dwyer

This document specifies technical and non-technical security policy for ASP implementations and applies to any ASP service regardless of technology to be used.

This standard contains 22 baseline controls, and 3 above baseline controls, for a total of 25 controls.

## **Important**

All of these Security Standards and Security Policies are copyrighted. THEY ARE NOT IN THE PUBLIC DOMAIN. They are however distributed under a liberal open-source license, see Publishing these Security Standards and Policies.

---

---

---

# Table of Contents

1. Introduction .....	1
1.1. Objectives .....	1
1.2. Scope .....	1
1.3. Not In Scope .....	1
1.4. Giving Feedback .....	1
1.5. Publishing these Security Standards and Policies .....	1
1.6. Related Documents .....	2
1.6.1. Generic Security Standards .....	2
1.6.2. Operating System Security Standards .....	2
1.6.3. Database Security Standards .....	3
1.7. Definitions .....	3
2. Security Compliance .....	4
2.1. Security Management .....	4
2.1.1. Obtain a copy of the suppliers information security service descriptions .....	4
2.1.2. Ensure that ASP contracts include a schedule detailing the security services provided and references a service level agreement for the provision of those services. ....	5
2.1.3. Obtain a copy of the suppliers information security organisational structure ...	5
2.1.4. Obtain a description of the suppliers arrangements for auditing the services that they provide. ....	6
2.1.5. Ensure that the supplier is bound by confidentiality agreements to prevent leakage of your data to other parties who may also use the ASP service. ....	7
2.1.6. Obtain a copy of the suppliers information security policy .....	8
2.1.7. Avoid ASPs who are unwilling to disclose their security capabilities even under non-disclosure agreements .....	8
2.1.8. Ensure that ASP personnel are subject to equivalent background checks as staff within your own organisation .....	9
2.1.9. Ensure that hardening of the components of the solution takes place in line with the policies and standards that are applicable within your organisation. ....	10
2.1.10. Ensure that a regime of measuring the security services provided are in place and the ASP provides these at an agreed frequency .....	11
2.1.11. Ensure that ASP contracts of employment place equivalent or greater emphasis on information security as that in your organisation's own contracts of employment	12
2.1.12. Ensure that the ASP management practices in relation to the components that make up the solution do not introduce vulnerabilities .....	12
2.1.13. Ensure that the ASP has a well defined audit capability .....	13
2.1.14. Ensure that the supplier provides contact names and details for each element of their security organisation that will deliver security services to your organisation. .	14
2.1.15. Ensure the ASP has a well defined information security organisation with clearly defined responsibilities .....	15
3. Network Security Configuration .....	16
3.1. Internet Considerations .....	16
3.1.1. Vulnerability scanning/penetration testing should be performed prior to any new service going live .....	16
3.1.2. The new service should be protected by a firewall .....	16
4. Auditing and Monitoring .....	18
4.1. Events to be alerted in real-time .....	18
4.1.1. Intrusion detection should be deployed .....	18
4.2. Events to be audited .....	18
4.2.1. Monitoring of the platforms of the ASP components should take place to flag when any components move out of alignment with the hardened build specification. ....	18
4.2.2. The ASP should provide monitoring of the firewall rule base .....	19

5. Other .....	21
5.1. Ensure that the Application Service Provider and your organisation develop and agree incident handling processes and procedures .....	21
5.1.1. Standard .....	21
5.1.2. Detailed Steps .....	21
5.1.3. Risks Addressed .....	21
5.2. Ensure that for a high availability requirement service that a fault tolerant implementation is deployed .....	22
5.2.1. Standard .....	22
5.2.2. Detailed Steps .....	22
5.2.3. Risks Addressed .....	22
5.3. Ensure a risk analysis is performed on the service to be provided .....	22
5.3.1. Standard .....	22
5.3.2. Detailed Steps .....	22
5.3.3. Risks Addressed .....	23
5.4. The security provided by the service provider must equate to the same or greater level of security that would be put in place were you to host it using your own organisation's capabilities. ....	23
5.4.1. Standard .....	23
5.4.2. Detailed Steps .....	23
5.4.3. Risks Addressed .....	23
5.5. Incident handling processes and procedures should be tested .....	24
5.5.1. Standard .....	24
5.5.2. Detailed Steps .....	24
5.5.3. Risks Addressed .....	24
6. Checklist .....	25

---

---

---

# Chapter 1. Introduction

## 1.1. Objectives

The objectives of this document are:

- To specify a security policy and standards for ASP delivered solutions.
- To provide guidance to administrators, developers and security personnel in securely implementing ASP solutions.

## 1.2. Scope

## 1.3. Not In Scope

Compliance with this standard will not provide “in depth” security architecture or intelligent security design guidance to projects. As a consequence, for high impact or safety-critical business applications, additional guidance will still need to be sought from the Information Security team consultancy function.

This is an ASP security policy. Controls specific to technologies used in the service are not defined here but will be the subject of additional standards. This document should also be read in conjunction with the generic security standards and the technology specific standards, which specifies controls applicable for particular technologies.

Compliance with this standard does not negate the need for an overall security review of a proposed application or service. Contact the Information Security team if you are in doubt.

## 1.4. Giving Feedback

Your feedback to improve this document is welcome. Please let me know of your experiences in applying the controls and guidance in this standard. Are the controls effective, easy to implement, too onerous, clear, unclear, something missing? Does an exceptional case need to be covered? Let me know. Please send your comments to frankodwyer AT netscape.net. Your comments will be used to produce better free security standards for the IT community.

I also request that you give feedback where you think the controls and guidance is correct. This will let us gauge whether or not specific controls are controversial or broadly acceptable to the community, and will help us to resolve cases where we have conflicting feedback on particular content.

## 1.5. Publishing these Security Standards and Policies

This document may be reproduced and distributed in whole or in part, free of charge, subject to the following conditions:

- All copyright and trademark notices, and this permission notice must be preserved complete on all complete or partial copies.
- Any translation or derivative work of this document must be approved by Frank O'Dwyer in writing before distribution.
- If you distribute this guide in part, instructions for obtaining the complete version of this manual must be included, and a means for obtaining a complete version provided.
- Small portions may be reproduced as illustrations for reviews or quotes in other works without this permission notice if proper citation is given.
- Neither Frank O'Dwyer's name nor the names of any contributors may be used to endorse or promote products derived from this document without specific prior written permission.

THIS DOCUMENT IS PROVIDED BY FRANK O'DWYER AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL FRANK O'DWYER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

I would like to be informed of any plans to publish or distribute these documents, just so I know how they're being used and where they are becoming available. If you are publishing or distributing or planning to publish or distribute any of these documents, please send mail to frankodwyer AT netscape.net

## 1.6. Related Documents

This document should be read and applied in conjunction with the technology specific security standards that are available from the frankodwyer.com web site. Please note that some of the documents below are currently under development and as such may not as yet be available. Check back frequently for updates to this document and those documents listed below.

### 1.6.1. Generic Security Standards

*Generic Security Standards*

<http://www.frankodwyer.com/standards/index.html#generic>

*Data Protection European Union Security Standard*

<http://www.frankodwyer.com/standards/index.html#generic>

*Application Service Provider Security Standards*

<http://www.frankodwyer.com/standards/index.html#generic>

### 1.6.2. Operating System Security Standards

*Generic Unix Security Standards*

<http://www.frankodwyer.com/standards/index.html#os>

*Windows NT4.0 Generic Security Standards*

<http://www.frankodwyer.com/standards/index.html#os>

*Windows NT4.0 Workstation Security Standards*

<http://www.frankodwyer.com/standards/index.html#os>

*Windows NT4.0 Server Security Standards*

<http://www.frankodwyer.com/standards/index.html#os>

*Windows NT4.0 Domain Security Standards*

<http://www.frankodwyer.com/standards/index.html#os>

### **1.6.3. Database Security Standards**

*Oracle Security Standards*

<http://www.frankodwyer.com/standards/index.html#db>

## **1.7. Definitions**

An “Information Asset” equates to any computerised information system or component thereof and thus includes an application, an item of off the shelf software, hardware, media, a data item, a data item repository and associated communications networks.

The specification of the Information Asset in question will usually be given so that this document is unambiguous, except where a control relates to any “Information Asset”.

The use of “must” or “will” indicates what the author considers to be a mandatory control.

However, whether the controls listed here are mandatory for your organisation is entirely at your organisation's discretion and thus they should be interpreted as representing the strongest recommendation of the author.

The use of “should” or “recommended” or “ought” indicates that the author believes that the controls in question are worthwhile and should be implemented unless such an implementation is impossible, onerous or impractical. Again, the implementation of controls so recommended in this document is entirely at your organisation's discretion.

---

# Chapter 2. Security Compliance

## 2.1. Security Management

### 2.1.1. Obtain a copy of the suppliers information security service descriptions

ID	Version	Level	Enforcement
ASP-SECMAN-3	1.0	baseline	mandatory

#### 2.1.1.1. Standard

The suppliers information security service descriptions should be obtained and analysed for consistency against the supplier security organisation and against your organisation's security service requirements.

#### 2.1.1.2. Detailed Steps

- Obtain the suppliers information security service descriptions
- Analyse the services in view of their stated organisational structure, their service capability claims and against your organisation's security service requirements.
- Identify areas where the suppliers services appear to be unsupported by their structure and re-sourcing
- In the context of the service to be provided analyse the impact of the disparities
- Feed the results into your analysis of the proposed service

#### 2.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Required security services may not be delivered
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

### 2.1.2. Ensure that ASP contracts include a schedule detailing the security services provided and references a service level agreement for the provision of those ser-

## vices.

ID	Version	Level	Enforcement
SECMAN-11	1.0	baseline	mandatory

### 2.1.2.1. Standard

Ensure that ASP contracts include a schedule detailing the security services provided and references a service level agreement for the provision of those services.

### 2.1.2.2. Detailed Steps

- Identify the security services required
- Identify the service level required for each security service
- Ensure that the contract for the application service provision references these services and the service level required

### 2.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The effectiveness of the service provision claims may be unsupported
- The effectiveness of the service provision claims may be unremediable through legal means
- Incident management may be ineffective
- Legal and regulatory responsibilities may not be met
- Procedural security may be wholly inappropriate
- Personnel security may be wholly inappropriate
- Technical security may be wholly inappropriate
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.1.3. Obtain a copy of the suppliers information security organisational structure

ID	Version	Level	Enforcement
ASP-SECMAN-2	1.0	baseline	mandatory

### 2.1.3.1. Standard

The suppliers information security organisational structure must be obtained and analysed for consistency with the stated policies and claimed security services.

### 2.1.3.2. Detailed Steps

- Obtain the suppliers information security organisational structure
- Analyse the structure in view of the stated policies and security services
- Identify areas where the suppliers defined structure appears unable to support the claimed policy objectives and the claimed security services.
- In the context of the service to be provided analyse the impact of the disparities
- Feed the results into your analysis of the proposed service

### 2.1.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- A wholly inappropriate technical security solution may be implemented
- A wholly inappropriate security management solution may be implemented
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.1.4. Obtain a description of the suppliers arrangements for auditing the services that they provide.

ID	Version	Level	Enforcement
ASP-SECMAN-4	1.0	baseline	mandatory

### 2.1.4.1. Standard

Auditing provides independent management checks on the functioning of controls, therefore obtain a description of the suppliers arrangements for auditing the services that they provide and compare this to

the regime that would be implemented were it in your own organisation.

### 2.1.4.2. Detailed Steps

- Obtain the description of the auditing provided by the supplier
- Ensure that the auditing to be provided equates at least to that which would be provided were the application hosted in-house

### 2.1.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The service may be operated in such a way as to be out of control
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.1.5. Ensure that the supplier is bound by confidentiality agreements to prevent leakage of your data to other parties who may also use the ASP service.

ID	Version	Level	Enforcement
SECMAN-12	1.0	baseline	mandatory

### 2.1.5.1. Standard

Ensure that the supplier is bound by confidentiality agreements to prevent leakage of your data to other parties who may also use the ASP service.

### 2.1.5.2. Detailed Steps

- Ensure that the ASP contract includes supplier confidentiality clauses
- Determine whether further more stringent confidentiality measures are required from the risk analysis

### 2.1.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Legal and regulatory responsibilities may not be met

- Business information may be disclosed.

## 2.1.6. Obtain a copy of the suppliers information security policy

ID	Version	Level	Enforcement
ASP-SECMAN-1	1.0	baseline	mandatory

### 2.1.6.1. Standard

The suppliers information security policy should be obtained and analysed for consistency with that of your own organisation.

### 2.1.6.2. Detailed Steps

- Obtain the suppliers information security policy
- Perform a comparative analysis between the suppliers policy and your own
- Identify areas where the suppliers policy requirements do not meet yours
- In the context of the service provided analyse the impact of the disparities
- Feed the results into your analysis of the proposed service

### 2.1.6.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- A wholly inappropriate technical security solution may be implemented
- A wholly inappropriate security management solution may be implemented
- An inappropriate security cultural solution may be implemented
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.1.7. Avoid ASPs who are unwilling to disclose their security capabilities even under non-disclosure agreements

ID	Version	Level	Enforcement
SECMAN-10	1.0	baseline	mandatory

### 2.1.7.1. Standard

Avoid using ASPs who are unwilling to disclose their security capabilities even under non-disclosure agreements

### 2.1.7.2. Detailed Steps

- Determine whether the supplier is willing to disclose their security capabilities
- Avoid those, who even under NDA will not disclose their security service capabilities

### 2.1.7.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The effectiveness of the service provision claims may be unsupportable
- Incident management may be ineffective
- Legal and regulatory responsibilities may not be met
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.1.8. Ensure that ASP personnel are subject to equivalent background checks as staff within your own organisation

ID	Version	Level	Enforcement
SECMAN-13	1.0	baseline	mandatory

### 2.1.8.1. Standard

Ensure that ASP personnel who will be working on the ASP solution are subject to equivalent background checks as staff within your own organisation

### 2.1.8.2. Detailed Steps

- Determine what background checks are performed by the ASP
- Compare these checks to those performed by your own organisation
- Determine whether there are any major mismatches and thus, exposures.

### 2.1.8.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Legal and regulatory responsibilities may not be met
- Technical security controls may be undermined
- Procedural security controls may be undermined
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.1.9. Ensure that hardening of the components of the solution takes place in line with the policies and standards that are applicable within your organisation.

ID	Version	Level	Enforcement
SECMAN-16	1.0	baseline	mandatory

### 2.1.9.1. Standard

Ensure that hardening of the components of the solution takes place in line with the policies and standards that are applicable within your organisation.

### 2.1.9.2. Detailed Steps

- Obtain details of the component hardening that the ASP performs
- Compare the hardening process used against the steps that your organisation would take.
- Identify any substantive differences that would reduce the security of the solution when compared to hosting it by your own organisation

### 2.1.9.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Legal and regulatory responsibilities may not be met
- Technical security controls may be undermined
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## **2.1.10. Ensure that a regime of measuring the security services provided are in place and the ASP provides these at an agreed frequency**

<b>ID</b>	<b>Version</b>	<b>Level</b>	<b>Enforcement</b>
SECMAN-9	1.0	baseline	mandatory

### **2.1.10.1. Standard**

Ensure that a regime of measuring the security services provided are in place and the ASP provides these at an agreed frequency

### **2.1.10.2. Detailed Steps**

- For each of the security services provided as part of the ASP define measures of effectiveness
- For each of the measures of effectiveness determine the frequency of report to be provided by the ASP.

### **2.1.10.3. Risks Addressed**

Where this control is not applied, the following residual risks exist:

- The effectiveness of the service provision claims may be unmeasured
- Incident management may be ineffective
- Legal and regulatory responsibilities may not be met
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## **2.1.11. Ensure that ASP contracts of employment place**

## equivalent or greater emphasis on information security as that in your organisation's own contracts of employment

ID	Version	Level	Enforcement
SECMAN-14	1.0	baseline	mandatory

### 2.1.11.1. Standard

Ensure that ASP contracts of employment place equivalent or greater emphasis on information security as that in your organisation's own contracts of employment

### 2.1.11.2. Detailed Steps

- Determine the information security clauses within your organisation's contract of employment
- Determine the information security clauses within the ASP contracts of employment
- Determine whether any mismatches are significant

### 2.1.11.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Legal and regulatory responsibilities may not be met
- Technical security controls may be undermined
- Procedural security controls may be undermined
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.1.12. Ensure that the ASP management practices in relation to the components that make up the solution do not introduce vulnerabilities

ID	Version	Level	Enforcement
SECMAN-15	1.0	baseline	mandatory

### 2.1.12.1. Standard

Ensure that the ASP management practices in relation to the components that make up the solution, do not introduce vulnerabilities

### 2.1.12.2. Detailed Steps

- Obtain the management procedures for the solution components from the ASP
- Compare these management procedures to those that would be applied were the solution hosted by your own organisation
- Identify substantive differences that may give rise to security vulnerabilities

### 2.1.12.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Legal and regulatory responsibilities may not be met
- Technical security controls may be undermined
- Procedural security controls may be undermined
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.1.13. Ensure that the ASP has a well defined audit capability

ID	Version	Level	Enforcement
SECMAN-8	1.0	baseline	mandatory

### 2.1.13.1. Standard

Ensure that the ASP undertakes periodic audits

### 2.1.13.2. Detailed Steps

- Obtain a description of the audit cycle for the service
- If one does not exist or if the cycle is too long this should be considered a deficiency

### 2.1.13.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The effectiveness of the service provision claims may be unmeasured
- Incident management may be ineffective
- Security responsibilities may be confused
- Legal and regulatory responsibilities may not be met
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

### 2.1.14. Ensure that the supplier provides contact names and details for each element of their security organisation that will deliver security services to your organisation.

ID	Version	Level	Enforcement
ASP-SECMAN-5	1.0	baseline	mandatory

#### 2.1.14.1. Standard

It must be ensured that the supplier provides contact names and details for each element of their security organisation that will deliver security services.

#### 2.1.14.2. Detailed Steps

- Using the supplier organisation chart and the security services that are to be supplied ensure that all contact details have been supplied.
- Ensure that the number of services to be provided by each individual named are reasonable
- Ensure that the contact info is maintained in an appropriate form such that incidents and responses can be appropriately dealt with.

### 2.1.14.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The service provision claims may be unsupported

- Incident management may be unfeasible
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 2.1.15. Ensure the ASP has a well defined information security organisation with clearly defined responsibilities

ID	Version	Level	Enforcement
SECMAN-7	1.0	baseline	mandatory

### 2.1.15.1. Standard

Ensure the ASP has a well defined information security organisation with clearly defined responsibilities

### 2.1.15.2. Detailed Steps

- Obtain the information security organisation from the ASP
- Correlate the security services provided with the security organisation
- Identify any significant mismatches
- Correlate the security services provided against the security services required
- Identify any significant mismatches

### 2.1.15.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The service provision claims may be unsupportable
- Incident management may be unfeasible
- Security responsibilities may be confused
- Legal and regulatory responsibilities may not be met
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

---

# Chapter 3. Network Security Configuration

## 3.1. Internet Considerations

### 3.1.1. Vulnerability scanning/penetration testing should be performed prior to any new service going live

ID	Version	Level	Enforcement
NETSEC-1	1.0	above baseline	recommended

#### 3.1.1.1. Standard

Where the new service is to be host by an ASP vulnerability scanning/penetration testing should be performed prior to the new service going live

#### 3.1.1.2. Detailed Steps

- Identify whether the ASP provides any monitoring of the platform builds

#### 3.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Security vulnerabilities may go undetected and lead to site compromise
- Legal and regulatory responsibilities may not be met
- Technical security controls may be undermined
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

### 3.1.2. The new service should be protected by a firewall

ID	Version	Level	Enforcement
NETSEC-2	1.0	baseline	recommended

### **3.1.2.1. Standard**

The new ASP hosted service should be protected by a firewall

### **3.1.2.2. Detailed Steps**

- Identify whether the ASP can supply the service with firewall protection in place

### **3.1.2.3. Risks Addressed**

Where this control is not applied, the following residual risks exist:

- Security vulnerabilities associated with non-essential services may lead to compromise of the system
- Legal and regulatory responsibilities may not be met
- Technical security controls may be undermined
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

---

# Chapter 4. Auditing and Monitoring

## 4.1. Events to be alerted in real-time

### 4.1.1. Intrusion detection should be deployed

ID	Version	Level	Enforcement
SECMON-1	1.0	above baseline	recommended

#### 4.1.1.1. Standard

Intrusion detection systems should be deployed in order to identify attacks against the service

#### 4.1.1.2. Detailed Steps

- Determine from the risk analysis of the system it's importance
- For important systems deploy an intrusion detection solution to monitor for attempted breaches

#### 4.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Attempts to breach the system may go undetected.
- Legal and regulatory responsibilities may not be met
- Technical security controls may be undermined
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 4.2. Events to be audited

**4.2.1. Monitoring of the platforms of the ASP components should take place to flag when any components move out of alignment with the hardened build specification.**

ID	Version	Level	Enforcement
SECMON-2	1.0	baseline	recommended

#### 4.2.1.1. Standard

Monitoring of the platforms of the ASP components should take place to flag when any components move out of alignment with the hardened build specification.

#### 4.2.1.2. Detailed Steps

- Identify whether the ASP provides any monitoring of the platform builds

#### 4.2.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Security breaches of the platforms may go undetected
- Legal and regulatory responsibilities may not be met
- Technical security controls may be undermined
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

### 4.2.2. The ASP should provide monitoring of the firewall rule base

ID	Version	Level	Enforcement
SECMON-3	1.0	baseline	recommended

#### 4.2.2.1. Standard

The ASP should provide monitoring of the firewall rule base

#### 4.2.2.2. Detailed Steps

- Identify whether the ASP can monitor firewall rule changes and reconcile the changes to valid, authorised changes.

### **4.2.2.3. Risks Addressed**

Where this control is not applied, the following residual risks exist:

- Unregulated rule changes may introduce security vulnerabilities that may lead to compromise of the system
- Legal and regulatory responsibilities may not be met
- Technical security controls may be undermined
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

---

# Chapter 5. Other

## 5.1. Ensure that the Application Service Provider and your organisation develop and agree incident handling processes and procedures

ID	Version	Level	Enforcement
OTHER-2	1.0	baseline	mandatory

### 5.1.1. Standard

Ensure that the Application Service Provider and your organisation develop and agree incident handling processes and procedures

### 5.1.2. Detailed Steps

- Define security incidents that require a response
- Determine the responses to be taken in the event of a security incident
- Determine the party responsible for taking the response
- Capture the above in a process document
- Define procedures to be followed to execute the process
- Implement the process and procedures between your organisation and the ASP.

### 5.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Remedial action may fail to be taken in the event of an incident
- Inappropriate and potentially more damaging action may be taken in the event of an incident
- Legal, regulatory or contractual obligations may be breached
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 5.2. Ensure that for a high availability requirement service that a fault tolerant implementation is deployed

ID	Version	Level	Enforcement
OTHER-1	1.0	above baseline	mandatory

### 5.2.1. Standard

Ensure that for a high availability requirement service that a fault tolerant implementation is deployed

### 5.2.2. Detailed Steps

- Ensure that the service is deployed with RAID, fault tolerant power supplies, online backups, mirroring, diverse network connections

### 5.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information and applications may be unavailable.

## 5.3. Ensure a risk analysis is performed on the service to be provided

ID	Version	Level	Enforcement
ASP-OTHER-1	1.0	baseline	mandatory

### 5.3.1. Standard

A risk analysis must be performed on the service to be hosted to ensure that appropriate controls are built into the solution

### 5.3.2. Detailed Steps

- Perform a risk analysis on the application to determine the control requirements

### 5.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- A wholly inappropriate security solution may be implemented
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

## 5.4. The security provided by the service provider must equate to the same or greater level of security that would be put in place were you to host it using your own organisation's capabilities.

ID	Version	Level	Enforcement
ASP-OTHER-2	1.0	baseline	mandatory

### 5.4.1. Standard

The security provided by the service provider should equate to a same or greater level of security that would be put in place were you to host it by your own organisation.

### 5.4.2. Detailed Steps

- Determine the appropriate level of security control required using risk analysis
- Determine the security capability of the provider
- Determine whether this delivers the control required against the risk analysis
- Determine whether this delivers the same control as that were you to host the service yourselves.

### 5.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The security solution delivered may be wholly inappropriate for the service
- Business information may be accidentally or maliciously altered.

- Business information may be disclosed.
- Business information and applications may be unavailable.

## 5.5. Incident handling processes and procedures should be tested

ID	Version	Level	Enforcement
OTHER-3	1.0	baseline	recommended

### 5.5.1. Standard

Incident handling processes and procedures should be tested

### 5.5.2. Detailed Steps

- Define and agree scenarios to be tested with the ASP
- Simulate the scenario and execute the incident handling procedure
- Measure deficiencies with the plan and its execution and re-develop the process and procedure accordingly

### 5.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Remedial action may fail to be effective in the event of an incident
- Inappropriate and potentially more damaging action may be taken in the event of an incident
- Legal, regulatory or contractual obligations may be breached
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

# Chapter 6. Checklist

<i>Security Compliance</i>		
<i>Security Management</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
ASP-SECMAN-3	Has the suppliers information security service claims been analysed for consistency with their organisational structure, resourcing level and your organisation's security service requirements.	
SECMAN-11	Does the ASP contract define the security services to be provided and the service levels?	
ASP-SECMAN-2	Has the suppliers information security organisational structure been analysed for consistency with the stated policies and the claimed security services.	
ASP-SECMAN-4	Does the description of the suppliers arrangements for auditing the services that they provide equate to or exceed the level of auditing that would be provided were it performed in-house?	
SECMAN-12	Is the supplier bound by confidentiality agreements to prevent leakage of your data to other parties who might also use the ASP service.	
ASP-SECMAN-1	Has the suppliers information security policy been obtained and analysed for consistency with that of your own organisation?	
SECMAN-10	Is the ASP willing to provide details of their security capabilities?	
SECMAN-13	Are ASP personnel working on the ASP solution subject to equivalent background checks as staff within your own organisation?	
SECMAN-16	Is it ensured that hardening of the components of the solution takes place in line with the policies and standards that are applicable within your organisation?	
SECMAN-9	Is there a regime for measuring the security services provided at an appropriate frequency?	
SECMAN-14	Do the ASP contracts of employment place equivalent or greater emphasis on information security as that in your organisation's own contracts of employment?	
SECMAN-15	Has it been ensured that the ASP management practices in relation to the components that make up the solution do not introduce vulnerabilities?	
SECMAN-8	Is the ASP subject to periodic audits?	
ASP-SECMAN-5	Has the supplier provided contact names and details for each element of the security organisation that is to deliver security services to your organisation?	
SECMAN-7	Does the ASP have a well defined information security organisation with clearly defined responsibilities?	
<i>Network Security Configuration</i>		
<i>Internet Considerations</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>

Checklist

NETSEC-1	Will vulnerability scanning/penetration testing be performed prior to the new service going live?	
NETSEC-2	Is the new ASP hosted service protected by a firewall?	
<i>Auditing and Monitoring</i>		
<i>Events to be alerted in real-time</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
SECMON-1	Has an intrusion detection system been deployed in order to identify attacks?	
<i>Events to be audited</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
SECMON-2	Will the solution provide perform monitoring of the platforms of the ASP components to flag when any components move out of alignment with the hardened build specification?	
SECMON-3	Does the ASP provide monitoring of the firewall rule base?	
<i>Other</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
OTHER-2	Have incident handling processes and procedures been developed and agreed with the Application Service Provider?	
OTHER-1	Has a fault tolerant implementation been deployed?	
ASP-OTHER-1	Has a risk analysis been performed on the service to be hosted?	
ASP-OTHER-2	Is the security provided by the service provider equivalent or greater than the level of security that would be put in place were it hosted by your own organisation?	
OTHER-3	Have incident handling processes and procedures been tested?	