WEB APPLICATION SECURITY
ASSURANCE STANDARDS

Architecture, Standards and Planning Branch
Office of the CIO ● Province of BC
People ● Collaboration ● Innovation

Version 1.6

March 25, 2014
# Table of Contents

Document Control .................................................................................................................. 3  
NOTES to Reviewers .............................................................................................................. 4  
Introduction .............................................................................................................................. 5  
Conceptual Framework of the Standards ................................................................................. 5  
1. Level of Security Assurance .............................................................................................. 7  
2. Security Assurance Assessments ....................................................................................... 15  
   2.1 Vulnerability Scanning .................................................................................................. 17  
   2.2 Penetration Testing ....................................................................................................... 23  
   2.3 Security Threat and Risk Assessments (STRAs) ............................................................ 27  
   2.4 Recovery Exercises of Application and Its Components .............................................. 29  
   2.5 Incident Response Exercises ....................................................................................... 32  
   2.6 Self-Imposed Independent Audits ............................................................................... 35  
3. Valid Evidence ..................................................................................................................... 37  
   3.1 Compliance to Reputable and Independent Benchmarks ............................................. 38  
   3.2 Qualified and Independent Assessors .......................................................................... 41  
   3.3 Assessment Reports ..................................................................................................... 43  
4. Assertions for Equivalently the Same Environments .......................................................... 47  
5. Direct Evidence ................................................................................................................... 49  
6. Vendor Benchmarks ......................................................................................................... 51  
Appendix A - Glossary ........................................................................................................... 53
## Document Control

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Version</th>
<th>Change Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 24, 2014</td>
<td>Sarah Louie</td>
<td>1.5</td>
<td>Draft for ASRB review</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.6</td>
<td>Reputable tools guidance 3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.6</td>
<td>D. Ehle feedback</td>
</tr>
</tbody>
</table>
The intent of this suite of standards is to create awareness of some security practices used by the BC Services Card project. This awareness is specifically targeted at other high profile and ‘failure is unacceptable’ projects within government. In formalizing practices, additional requirements have been specified to make practices more explicit and more suitable for a standard.

The BC Services Card project has served as a test case for obtaining some of the security assessment services that are required within this standard. Work is in-progress to facilitate the availability of security assessment services as an iStore catalogue items. Static and Dynamic application analysis are available as an iStore HP/AS Professional Services request. Services will be performed by HP Fortify. Other security assessments are expected to also be available through Telus Professionals Services. In addition, the results of server vulnerability scans performed by HP/AS as part of their contractual obligation to government are available by request from OCIO IT Security Operations (Steven Radin).

There is also some effort in-progress in evaluating common application components (e.g. server build images) provided by the Province’s service providers to eliminate some of the assessment effort of ministries. This will provide a baseline assessment but will not eliminate the need to assess completely. Server build images are customized based on the server purpose and application requirements. For example, ports opened and services enabled would be different for each application, and need to be assessed to ensure only the required ports and services are opened or enabled. Other work in-progress are those that will resolve specific testing issues (e.g. different SAG requirements to facilitate external tester access to the internal network zone).

Since there is still on-going effort in facilitating testing and services, the suite of standards has a compliance date of ‘to be determined (TBD)’. This is also to allow time for these standards to be ‘tried on for size’ and then ‘right sized’ at a later date.

Funding security assessments is often an expressed concern and some work is also in-progress for this as well. In the meantime, high profile projects may want to consider adding a line item in their project budget of 15% when submitting to DCMTT. 15% is an industry standard estimate of the cost of security.

This suite of standards represent a step forward in improving government’s application security posture and in addressing the concerns of the Auditor General’s Office who have been performing tests on random samples of government’s applications.
INTRODUCTION

Once security controls have been designed and implemented, there needs to be a means to assess their effectiveness prior to implementation and during the lifetime of the application after its deployment. This is crucial when the application is operationally critical for the business and/or contains sensitive or confidential information.

Performing security assessments is the means to assess how secure an application is. The focus of the Security Assurance Suite of Standards is to identify the level of confidence i.e. security assurance that can be associated with security assessments as reflecting an accurate state of application security and risk.

CONCEPTUAL FRAMEWORK OF THE STANDARDS

This suite of standards applies to all existing and new web applications or web services that support government services. In particular, they target web applications with a B.C. government Information Security Classification of ‘high’ and ‘medium’ sensitivity. Web applications that are classified as low sensitivity can also use these standards as guidance.

The Security Assurance Standards address the following concerns:

1. What security assessments must be performed to assess application security and risk state?
2. How reliable and accurate are the security assessments?
3. What kind of confidence can be placed on assessment conclusions in reflecting the actual security and risk state of an application?

Standard 1.0 introduces the concept of a ‘level of security’ which represents the level of confidence that you can have in security assessment conclusions. It also identifies the requirements to achieve a specific level of security assurance based on the sensitivity of an application.

Standard 2.0 identifies the different types of assessments that need to be performed to meet the predetermined level of security assurance. The standard subtopics address the quality issue when assessments are performed to ensure that results are meaningful.

Standard 3.0 specifies the rules that will ensure that assessment results reflect accurately the state of application risks, making them suitable as evidence for inclusion within a Security Threat and Risk Assessment (STRA) or suitable for review and acceptance by an auditor. Each standard subtopic is an individual rule towards achieving the ‘valid’ evidence designation.

Standards 4.0, 5.0, and 6.0 are specialized rules for what constitutes valid evidence. In certain situations, the assertions made for an environment may be made based on the assessment of another environment. Standard 4.0 specifies the rules when an environment can be considered as equivalently the same as another. Standard 5.0 defines situations when evidence can be treated
as though the assessor had generated the evidence directly. Standard 6.0 discusses the issue of how to treat vendor supplied benchmarks as evidence.

**Terminology**

The term “MUST” is defined as an absolute requirement of the specification.

“SHOULD” (when written in all upper case) means that there may be valid reasons in particular circumstances to use alternate methods, but the full implications must be understood and carefully weighed before choosing a different course. The use of an alternate method requires the approval of the ADM of the information owner. For the purposes of these standards “information owner” is defined in the Province’s Information Security Policy as having “the responsibility and decision making authority for information throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure.”

**Additional Guidance**

Appendix A - Glossary

**References**

- OCIO – Information Security Policy 8.2 Correct processing in applications
1. **Level of Security Assurance** | Effective Date: TBD
---|---
| Scheduled Review: TBD

**Purpose**

This standard helps business owners determine the requirements they need to satisfy in order to achieve the required level of application security assurance.

The strategic aim of this standard is to support the Government’s goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

**Context**

This standard does not determine how secure your application is. This standard determines the confidence that can be placed on security assessments accurately reflecting your actual application security and risk state. This level of confidence is referred to as a ‘level of security assurance’ within this standard.

An accurate reflection of application security and risk ultimately contributes to the protection of the application’s assets from unauthorized access, disclosure, and modification. This enables business owners to intentionally and selectively remediate risk according to their level of risk tolerance and to make effective use of their resources.

**Standard**

This standard applies to all existing and new web applications or web services that support government services. Re-assessments must occur after major changes to the application that may result in a different Information Security Classification of the application’s sensitivity; otherwise, at a minimum, annually prior to performing new security assessments as required in Standard 2.0.

1. Web applications MUST be classified according to their level of sensitivity.
2. The level of sensitivity MUST be based on the Province’s Information Security Classification Framework (see ref.).
3. Web applications MUST be assessed to determine their security assurance level.
4. A web application’s security assurance level is determined from Table 1.0.
5. Web applications MUST meet the assurance requirements corresponding to their security assurance level.
6. The assurance requirements for the various security assurance levels are specified in Table 2.0.

All applications must achieve a specific level of security assurance based on its level of sensitivity. This standard identifies the requirements that must be met to obtain that level of security assurance.

**Table 1.0 Associated Security Assurance Level for Application Sensitivity Classification**

<table>
<thead>
<tr>
<th>Application Sensitivity Classification</th>
<th>Minimum Security Assurance Level Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>2</td>
</tr>
<tr>
<td>Medium</td>
<td>4</td>
</tr>
<tr>
<td>Low</td>
<td>Guidance</td>
</tr>
</tbody>
</table>
## Table 2.0 Level of Security Assurance and its Requirements

<table>
<thead>
<tr>
<th>Security Assurance Level to be Achieved</th>
<th>Standard 2.0 Security Assessments Performed</th>
<th>Standard 3.0 Valid Evidence Rules Met</th>
<th>Assertions for Environment Assessed (See Standard 4.0 on Equivalent Environments)</th>
<th>Standard 5.0 Direct Evidence Sources</th>
<th>Standard 6.0 Vendor Benchmarks</th>
<th>Level Classification Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (Highest)</td>
<td>ALL of 2.1-2.6 met.</td>
<td>ALL of 3.1-3.3 met</td>
<td>Actual Environment</td>
<td>Direct</td>
<td>None</td>
<td>Vendor benchmarks covered by Standard 3.1 recognized benchmarks assessments.</td>
</tr>
<tr>
<td>2</td>
<td>ALL of 2.1-2.6 met.</td>
<td>ALL of 3.1-3.3 met</td>
<td>Equivalent Environment</td>
<td>Direct</td>
<td>None</td>
<td>Since equivalent means there are still differences present from the actual environment.</td>
</tr>
<tr>
<td></td>
<td>ALL of 2.1-2.6 met.</td>
<td>Partial 3.1 Reputable and Independent Benchmarks. ALL of 3.1-3.2 met.</td>
<td>Actual Environment</td>
<td>Direct</td>
<td>Vendor Benchmarks Used Where Independent Benchmarks are Unavailable.</td>
<td>Since equivalent means there are still differences present from the actual environment. Reputable and independent benchmarks are not always available and so vendor benchmarks are second best solution.</td>
</tr>
<tr>
<td>3</td>
<td>ALL of 2.1-2.6 met.</td>
<td>Partial 3.1 Reputable and Independent</td>
<td>Equivalent Environment</td>
<td>Direct</td>
<td>Vendor Benchmarks Used Where</td>
<td>Since equivalent means there are still differences present from the actual environment. Reputable and independent benchmarks are not always available and so vendor benchmarks are second best solution.</td>
</tr>
<tr>
<td></td>
<td>Benchmarks</td>
<td>Independent Benchmarks are Unavailable.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>------------</td>
<td>----------------------------------------</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 4 | ALL of 2.1-2.5 met.  
2.6 Self-Imposed Audit is performed by MISO and not an auditor. | None or Vendor Benchmarks Used Where Independent Benchmarks are Unavailable. | MISO can provide a summary of the conclusions of the individual assessment assertions.  
MISO’s are trained in security and not necessarily in auditing practices and their assessment cannot be considered independent. |
| 5 | ALL of 2.1-2.5 met.  
2.6 Self-Imposed Audit Not Met | Vendor Benchmarks Used Where Independent Benchmarks are Unavailable. | Self-Imposed Audit is mechanism to verify and coherently summarize ALL assessment evidence; therefore, presents the most accurate assertion of application security and risks. Individual types of assessments provide a piecemeal view only. |
| 6 | (Lowest) | | Essentially Level 6 is anything that does not meet Level 5 requirements. For example, where partial requirements exist for any |
**NOTE:**

- There are 6 security assurance levels. All requirements for each column must be met in order to obtain the category of security assurance denoted by the row. Some levels are listed more than once because they may be achieved more than one way.

- The highest level of security assurance, ‘1’ means that there is a high level of confidence that the state of application security and risks has been assessed and determined accurately. A medium level of security assurance ‘3’ means that there exists a comfortable level of confidence but there exists a likelihood of errors in assessing and determining the state of application security and risks. A low level of security assurance ‘6’ means that there is little confidence in the accuracy of the assessing and determining the state of application security and risks.
Additional Guidance

- Security Assurance Level

  Quality of Assessments Performed **AND** Validity as Evidence **AND** Environment (Asserted for and Assessed Against) **AND** Evidence Source (direct or indirect)

- A working example of following steps 1-3 in using the standard:

  1. Based on the Information Security Classification, there is likely to be ‘severe’ impact by a breach of the application. Your application is considered as ‘High’ sensitivity.

  2. Based on Table 1.0, a ‘High’ sensitivity application must achieve a security assurance level of ‘4’.

  3. Based on Table 2.0, there are 2 ways to achieve this level ‘2’ of assurance explained as Path 1 and Path 2:

<table>
<thead>
<tr>
<th>Security Assurance Level to be Achieved</th>
<th>Standard 2.0 Security Assessments Performed</th>
<th>Standard 3.0 Valid Evidence Rules Met</th>
<th>Assertions for Environment Assessed (See Standard 4.0 on Equivalent Environments)</th>
<th>Standard 5.0 Direct Evidence Sources</th>
<th>Standard 6.0 Vendor Benchmarks</th>
<th>Level Classification Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>ALL</td>
<td>ALL</td>
<td>Equivalent Environment</td>
<td>Direct</td>
<td>None</td>
<td>Since equivalent means there are still differences present from the actual environment.</td>
</tr>
<tr>
<td>2</td>
<td>ALL</td>
<td>Partial 3.1 Reputable and Independent Benchmarks</td>
<td>Actual Environment</td>
<td>Direct</td>
<td>Vendor Benchmarks Used Where Independent Benchmarks are Unavailable</td>
<td>Since equivalent means there are still differences present from the actual environment. Reputable and independent benchmarks are not always available and so vendor benchmarks are second best solution.</td>
</tr>
</tbody>
</table>

Path 1: The first way is requirements specified by row 1 for level ‘2’. You must:

a. Perform all the security assessments as specified under Standard 2.0 **AND**

b. Meet all the rules specified under Standard 3.0 **AND**

c. Meet all the rules specified for an equivalently the same environment as specified under Standard 4.0 **AND**

d. Meet all the rules specified under Standard 5.0 that classifies the evidence provided as ‘Direct’ Evidence **AND**

e. Not have used any vendor benchmarks which are specified in Standard 6.0 as part of your assessments.

Path 2: Alternatively, the second way is to meet all the requirements specified by row 2 for level ‘2’. You must:

a. Perform all the security assessments as specified under Standard 2.0 **AND**
b. Meet all the rules specified under Standard 3.0 except that some application component could not have been assessed against reputable and independent benchmarks \textbf{AND}

c. Meet the rule of having assessment results for the actual environment \textbf{AND}

d. Meet all the rules specified under Standard 5.0 that classifies the evidence provided as ‘Direct’ Evidence \textbf{AND}

e. As a result of b. some vendor benchmarks where used as specified in Standard 6.0 as part of your assessments.

- Security assurance should not be confused with the concept of how secure your application is. The following 2 examples illustrate the differences and how the 2 concepts inter-relate.

1. Example 1: If assessments met the requirements of security level assurance of ‘1’, you can conclude with the highest level of confidence that assessments accurately reflect the actual application security and risk state.

   If your assessments report that:

   a. Your application mostly complied with security benchmarks.

   b. There are identified only low risk issues.

   You can have the highest confidence that your application is secure since the assessments accurately reports that your application complies with benchmarks and only low risk issues exist.

2. Example 2: If assessments met the requirements of security level assurance of ‘1’, you can conclude with the highest level of confidence that assessments accurately reflect the actual application security and risk state.

   a. Assessment conclusions are that your application does not comply with most security benchmarks.

   b. There is identified multiple high risk issues.

   You can have the highest confidence that your application is insecure since the assessments accurately report that your application basically does not comply with benchmarks and there exist high risk issues. You can then move from this insecure state by remediating the issues identified by the assessments. Once remediation has been completed, you can reassess so that hopefully you can have the highest confidence in assessment results that your application is secure.

\textbf{NOTE:} Based on the Province’s Information Security Policy, business owners of applications are accountable for the security of their applications and for their own determined level of risk tolerance. It is not the intent of this standard to define owner risk tolerance levels. If repeated breaches occur, the OCIO may investigate the level of risk and security controls that exists.

\textbf{References}

- Information Security Classification Framework
http://www.cio.gov.bc.ca/cio/informationsecurity/classification/information_security_classification_framework.page
Introduction

The actual state of application security and risk is dependent on the security controls implemented. Security controls are most effective when security requirements are considered early in the application lifecycle. Once security has been designed, documented, and then implemented, there needs to be a means to verify if controls are functioning as designed and are effective. This is the function of security assessments.

The standard subtopics 2.1-2.6 address the quality issue when assessments are performed to ensure that results are meaningful. This is accomplished by specifying the objective to be met by each assessment type and the minimal assessment tasks that must be completed. These requirements can then be utilized within the procurement process for services.

The quality issue is also addressed by specifying the minimum set of assessments that must be performed in order to provide a relatively accurate picture of the actual state of application security and risk.

Although this standard is not intended to address the question of how secure is my application, it is indirectly answered by performing the following set of assessments. (See Standard 1.0 Additional Guidance examples of the 2 concepts: security assurance and security of application.)

1. Vulnerability scans
2. Penetration testing (PEN Testing)
3. Security threat and risk assessments (STRAs)
4. Recovery exercises of application and its component
5. Incident response procedures exercises
6. Self-imposed independent audits

This standard represents a defence-in-depth strategy by specifying the required security assessments that will reduce the number of risks that can be leveraged and their subsequent impact when a breach has occurred.
Additional Guidance

References

- OCIO – Information Security Policy 8.2 Correct processing in applications
- OCIO – Information Security Policy 11.2.2 Technical compliance checking
- OCIO – Information Security Policy 11.3 Compliance – Information systems audit considerations
2. **SECURITY ASSURANCE ASSESSMENTS**

<table>
<thead>
<tr>
<th>2.1 VULNERABILITY SCANNING</th>
<th>Effective Date: TBD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Review: TBD</td>
<td></td>
</tr>
</tbody>
</table>

**Purpose**

This standard helps business owners to identify the types of vulnerability scans that need to be performed as part of a security assessment to objectively reflect the actual state of application security and risk. This standard also specifies assessment requirements to produce meaningful results.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

**Context**

This standard requires vulnerability scanning to identify vulnerabilities that can be leveraged in a malicious attack. It also identifies the assessment objectives and assessment task requirements in order to produce meaningful results at the end of the engagement.

Vulnerability scans are best performed early in the application lifecycle to avoid having to propagate remediation through multiple environments. Likewise, identifying poor coding practices early on will prevent the requirement to change large portions of application code.

Testing should include the use of automated tools and should be supplemented by manual testing. Automating testing eliminates the likelihood of human error. Manual testing is necessary to remove false positives and to perform tests against vulnerabilities that are not possible using automated tools.

**Standard**

This standard applies to all existing and new web applications or web services that support government services. Re-assessments must occur after major changes to the application or to its components; otherwise, at a minimum, every three years.

This standard requires Vulnerability scanning, as per Table 2.0, meet the following requirements:

1. Vulnerability scanning MUST at a minimum address each entry listed in Table 3.0.
2. Identified vulnerabilities MUST be reviewed by the business application owner.
3. The business application owner MUST decide to remediate or intentionally accept the risk based on the assessment report.
### Table 3.0 Assessment Objectives and Requirements

<table>
<thead>
<tr>
<th>Assessment Type</th>
<th>Assessment Objectives</th>
<th>Assessment Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability Scans</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Network Scans</td>
<td>To enable the verification that network access and installed content on devices is based on documented requirements for secure use.</td>
<td>MUST report on: 1. Assets are inappropriately visible from the external and internal network perspectives (e.g. intranet zone assets are not visible externally or potentially accessible). Inappropriate network control rules (e.g. ACL verification such as source and destination location, open ports, and enabled traffic protocols). 2. Inappropriate network accessibility between different application environments (e.g. from UAT into production).</td>
</tr>
<tr>
<td>B. Server Scans</td>
<td>To enable the verification that server access and installed content is based on documented requirements for secure use.</td>
<td>MUST report on: 1. Unauthorized software installed and its patch level. 2. Inappropriately opened server ports, enabled protocols, and enabled services. 3. Misconfiguration and inappropriate enablement of high risk services e.g. ftp and telnet. 4. Credentials inappropriately stored within batch jobs, scripts, or plain text files. 5. Inappropriate local accounts that exist with non-expiring passwords. NOTE: OCIO ISP exemption required for this as well as proper management. 6. Inadequacy of encryption method and level used. 7. Ability to gain unauthorized access to encryption keys. 8. Weak strength server passwords not meeting policy (e.g. via password cracking).</td>
</tr>
</tbody>
</table>
C. Application Scans
   i. Static Analysis

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>To enable the verification that secure coding practices are occurring by assessing source code, byte code, and/or binary code.</td>
</tr>
<tr>
<td>MUST report on:</td>
</tr>
<tr>
<td>1. Results from automated scanning, and the identification and removal of false positives by tester manually or by cross-correlating with automated tool results.</td>
</tr>
<tr>
<td>2. Results from manual code review and testing of what cannot be performed by automated tools.</td>
</tr>
<tr>
<td>3. The existence of Logic Bombs or Backdoors.</td>
</tr>
<tr>
<td>4. Enabled debugging features.</td>
</tr>
<tr>
<td>5. Credentials inappropriately stored within code.</td>
</tr>
<tr>
<td>NOTE: The ability to assess byte and binary code makes it possible to assess COTS products.</td>
</tr>
</tbody>
</table>

ii. Dynamic Analysis

| To enable the verification that secure coding practices are occurring by assessing logical errors while the application is executing (e.g. bypassing workflow). |
| MUST report on: |
| 1. Results from automated scanning, and the identification and removal of false positives by tester manually or by cross-correlating with automated tool results. |
| 2. Results from manual testing for tests supplementing automated testing to identify false positives or to perform important risk tests that cannot be automated. |
| 3. Insecure API calls or responses. |
| 4. Enabled or insecure cross application interfaces. |
| 5. Insecure coding of functionality or of customized code within COTS products and/or any code utilizing COTS APIs. |
| 6. Insecure coding and functionality of sensitive application functions or of any privileged access interfaces such as application administrator screens. |
| 7. Ability to execute commands or inject code (e.g. OS commands, SQL injection, Cross-site Scripting, LDAP injection). |
| 8. Inadequacy of session management controls. |
| 9. Ability to perform URL path
<table>
<thead>
<tr>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>10. Ability to cause overflow conditions (e.g. parameter overflow and buffer overflow).</td>
</tr>
<tr>
<td>11. Ability to perform character encoding attacks.</td>
</tr>
<tr>
<td>12. Ability to supply inappropriate input values (i.e. fuzz testing).</td>
</tr>
<tr>
<td>13. Results from business logic testing (e.g. application access by different roles, process workflows, etc.).</td>
</tr>
<tr>
<td>14. All publicly accessible webpages identified by an unauthenticated scan.</td>
</tr>
<tr>
<td>15. Any security flaws within Web Services (REST-based and SOAP) used by the application.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D. Middleware Scans (e.g. web servers)</th>
</tr>
</thead>
<tbody>
<tr>
<td>To enable the verification that middleware server access and installed content is based on documented requirements for secure use.</td>
</tr>
<tr>
<td>NOTE:</td>
</tr>
<tr>
<td>• Special attention should be paid to open source software.</td>
</tr>
<tr>
<td>• There may be some overlap with dynamic analysis. Some will assess web servers and application servers.</td>
</tr>
<tr>
<td>MUST report on:</td>
</tr>
<tr>
<td>1. Results from automated scanning, and the identification and removal of false positives by tester manually or by cross-correlating with automated tool results.</td>
</tr>
<tr>
<td>2. Results from manual testing for tests supplementing automated testing to identify false positives or to perform important risk tests that cannot be automated</td>
</tr>
<tr>
<td>3. Misconfiguration</td>
</tr>
<tr>
<td>4. Inappropriate default configuration settings.</td>
</tr>
<tr>
<td>5. Unauthorized directories that can be traversed or displayed (aka directory enumeration).</td>
</tr>
<tr>
<td>6. Unauthorized server side application files that are accessible for downloading or inspection by clients (e.g. Viewing php, jsp, or asp file contents)</td>
</tr>
<tr>
<td>7. Unnecessary product information displayed (e.g. installed modules).</td>
</tr>
<tr>
<td>8. Unnecessary accounts or features enabled.</td>
</tr>
<tr>
<td>10. Inappropriate default configuration settings.</td>
</tr>
</tbody>
</table>
| E. Database Scan and PEN Testing | To enable the verification that both database server and database access and installed content is based on documented requirements for secure use. | Must include verification of:  
1. Results from automated scanning, and the identification and removal of false positives by tester manually or by cross-correlating with automated tool results.  
2. Results from manual testing for tests supplementing automated testing to identify false positives or to perform important risk tests that cannot be automated  
3. Misconfiguration.  
4. Inappropriate default configuration settings.  
5. Unnecessary accounts or features enabled.  
6. Default passwords.  
7. Excessive privileges granted to database objects or to database OS files.  
8. Inappropriate local accounts with non-expiring passwords. NOTE: OCIO ISP exemption required for this as well as proper management.  
9. Credentials inappropriately stored within batch jobs or scripts.  
10. Inadequate segregation of duties to roles exists.  
11. Existence of privileged utilities or enabled debugging features in the production environment.  
12. Inadequacy of encryption method and level used.  
13. Ability to gain unauthorized access to encryption keys.  
15. Weak strength database passwords (e.g. via password cracking).  
17. Database replication over insecure channels.  
18. Ability to read, modify, copy, and/or remove configuration data, logs and access control. |
19. Inadequacy of controls to prevent outsider and insider attacks.
20. Inadequacy of controls for all entrance and exit points of the database.

Additional Guidance

- It is strongly recommended that an assessment plan be provided by the assessor and that it is used to discuss what the engagement should entail. The assessment plan should be approved by the business area prior to the assessment beginning.
- Prior to assessment, risk should be identified:
  - Concerning privileges granted to assessors. In some cases, a privileged account is required in order for tools to perform a comprehensive assessment. For example, in dynamic analysis, only the webpages that can be accessed by the testing credentials will be scanned. This means that not ALL webpages of an application are scanned by default.
  - The tools used are from a reputable source and are accessible only by testers.
  - The potential impact of assessments (especially to operational stability of production environments and exposure of personally identifiable information).
- Service providers and all stakeholders should be notified in advance of any security assessments for approval prior to the assessment starting.

References

- OCIO – Information Security Policy 8.6 Information Systems Acquisition, Development and Maintenance – Vulnerability management
- OCIO – Information Security Policy 11.3.1 Audit requirements and activities involving checks on operational systems must be planned and approved to minimize disruption to business processes.
- OCIO – Information Security Policy 11.2.2 Information systems must be regularly checked for compliance with security policies and standards.
- OCIO – Information Security Policy 11.3 Compliance – Information systems audit considerations
2. **Security Assurance Assessments**

<table>
<thead>
<tr>
<th>2.2 Penetration Testing</th>
<th>Scheduled Review: TBD</th>
</tr>
</thead>
</table>

**Purpose**

This standard identifies the requirement for Penetration Testing (PEN Testing) to be performed as part of a security assessment to objectively reflect the actual state of application security and risk. This standard also specifies assessment requirements to produce meaningful results.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

**Context**

This standard requires PEN Testing to identify what vulnerabilities can be leveraged for an attack. It also identifies the assessment objectives and assessment tasks requirements in order to produce meaningful results at the end of the engagement.

PEN Testing is best performed once the application code release is stable and its underlying components have been built. This is to reduce the number of PEN Tests to be performed during the application lifecycle. It is also recommended that after remediation has occurred that re-testing be performed.

PEN Testing should include the use of automated tools and should be supplemented by manual testing. Automating testing eliminates the likelihood of human error. Manual testing is necessary to remove false positives and to perform tests against vulnerabilities that are not possible using automated tools.

**Standard**

This standard applies to all existing and new web applications or web services that support government services. Re-assessments must occur after major changes to the application or to its components; otherwise, at a minimum, every three years.

This standard requires PEN Testing as per Table 2.0:

1. PEN Testing MUST at a minimum address each entry listed in Table 4.0.
2. Identified issues MUST be reviewed by the business application owner
3. The business application owner MUST decide to remediate or intentionally accept the risk based on the assessment report.
### Table 4.0 Assessment Objectives and Requirements

<table>
<thead>
<tr>
<th>Assessment Type</th>
<th>Assessment Objectives</th>
<th>Assessment Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Penetration Testing</strong></td>
<td><strong>A. Application PEN Testing</strong></td>
<td>MUST report on:</td>
</tr>
<tr>
<td></td>
<td>To identify risks and its impact where vulnerabilities can be leveraged by both insider and outsider attacks by perpetrating simulated attacks.</td>
<td>1. Results from automated scanning, and the identification and removal of false positives by tester manually or by cross-correlating with automated tool results.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Vulnerability scans and residual risk identification from STRAs can be used as input for the PEN Testing plan.</td>
<td>2. Results from manual testing for tests supplementing automated testing to identify false positives or to perform important risk tests that cannot be automated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Misconfiguration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Inappropriate default configuration settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Unnecessary accounts or features enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. Default passwords.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. Excessive privileges.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. Ability to bypass normal application access paths.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. Inadequacy of session management controls.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10. Inadequate segregation of infrastructure, data, etc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11. Weak strength application passwords not meeting policy (e.g. via password cracking).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12. Inadequate asset segregation by purpose and environment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13. Privileged access to the server not via the administrative gateway.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15. Ability to exfiltrate data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>16. Ability to store malicious content.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>17. Ability to gain unauthorized access to data and to installed product files.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>18. Ability to gain unauthorized access to encryption keys.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>19. Ability to gain unauthorized access to administrative interfaces and tools.</td>
<td>20. Ability to read, modify, copy, and/or remove configuration data, logs and access control.</td>
<td>21. Existence of privileged utilities or enabled debugging features in the production environment.</td>
</tr>
<tr>
<td>22. Inadequacy of encryption method and level used.</td>
<td>23. Ability to gain unauthorized access to encryption keys.</td>
<td>24. Inadequacy of signing hashes.</td>
</tr>
<tr>
<td>25. Inadequate application resiliency to common attacks such as DDoS, and session replay.</td>
<td>26. Inappropriate access or application functionality is not restricted based on accesses granted to user roles.</td>
<td>27. Inadequacy of controls to prevent outsider and insider attacks.</td>
</tr>
<tr>
<td>28. Adequacy of controls for all entrance and exit points of an application.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**B. Database PEN Testing**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>See info under Vulnerability Scans – Database Scan and PEN Testing</td>
<td>Must be targeted and verified as a separate assessment from Application PEN Testing.</td>
<td></td>
</tr>
</tbody>
</table>
Additional Guidance

- PEN Testing MAY be performed from a black box, gray box, or white box perspective. The perspective is dependent on the amount of information provided to the tester based on what pre-testing assumptions are made e.g. easily gathered information was provided to tester to save time or escalation of privilege is possible.
- It is strongly recommended that an assessment plan be provided by the assessor and that it is used to discuss what the engagement should entail. The assessment plan should be approved by the procurer of the service prior to the assessment beginning.
- Prior to assessment, risk should be identified:
  - Concerning privileges granted to assessors. In some cases, a privileged account is required in order for tools to perform a comprehensive assessment.
  - The tools used are from a reputable source and are accessible only by testers.
  - The potential impact of assessments (especially to operational stability of production environments and exposure of personally identifiable information).
- Activity log of penetration testing activities be provided by the PEN Tester to be used for verifying incident response procedures.
- Service providers and all stakeholders should be notified in advance of any security assessments for approval prior to the assessment starting.

References

- OCIO – Information Security Policy 8.6 Information Systems Acquisition, Development and Maintenance – Vulnerability management
- OCIO – Information Security Policy 11.3.1 Audit requirements and activities involving checks on operational systems must be planned and approved to minimize disruption to business processes.
- OCIO – Information Security Policy 11.2.2 Information systems must be regularly checked for compliance with security policies and standards.
- OCIO – Information Security Policy 11.3 Compliance – Information systems audit considerations
2. SECURITY ASSURANCE ASSESSMENTS

<table>
<thead>
<tr>
<th>2.3 SECURITY THREAT AND RISK ASSESSMENTS (STRAS)</th>
<th>Effective Date: TBD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Review: TBD</td>
<td></td>
</tr>
</tbody>
</table>

**Purpose**

This standard identifies additional requirements for a Security Threat and Risk Assessment (STRA) to be performed as part of security assessments to objectively reflect the actual state of application security and risk. This standard also specifies assessment requirements to produce meaningful results.

The strategic aim of this standard is to support the Government’s goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

**Context**

As per the Information Security Policy, STRAs must be performed by business owners in order to provide understanding of application security and risk state. This standard also identifies the assessment objectives and assessment tasks requirements in order to produce meaningful results at the end of the assessment.

STRAs are important to assess risk from the view of the business as a whole and also covering areas such as physical security and process security that can be ascertained by any automated assessment.

See the Reference Section of this standard for information on the methodology and on the government’s tool iSMART.

**Standard**

This standard applies to all existing and new web applications or web services that support government services. Re-assessments must occur after major changes to the application or to its components; otherwise, at a minimum, every three years as specified by the Information Security Policy.

This standard requires that STRAs as per Table 2.0 meet the following requirements:

1. STRAs MUST be performed to ascertain business risk as a whole.
2. STRAs MUST be performed to supplement other security assessments where risk cannot be determined by automated testing.
3. STRAs MUST at a minimum address each entry listed in Table 5.0.
4. As per the Information Security Policy, an STRA MUST be performed during the conceptual phase and prior to deployment. This standard requires that with each successive phase of a project, as new details become known and new risks surface, additional STRAs SHOULD be performed.

5. As per the Information Security Policy:
   a. Identified issues MUST be reviewed by the business application owner.
   b. Business application owner MUST decide to remediate or intentionally accept the risk based on the assessment report.

### Table 5.0 Assessment Objectives and Requirements

<table>
<thead>
<tr>
<th>Assessment Type</th>
<th>Assessment Objectives</th>
<th>Assessment Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>STRAs</td>
<td>1. To measure compliance with security best practices (e.g. ISP 27001 and ISF SoGP) and identify residual risk.</td>
<td>STRAs MUST: 1. Include responses verifiable by accompanying evidence.</td>
</tr>
<tr>
<td></td>
<td>2. To track risk and associated decisions and its treatment or acceptance.</td>
<td>2. Perform independent auditing of the STRA and its evidence (See standard subtopic 2.6.)</td>
</tr>
</tbody>
</table>

### Additional Guidance

### References

- Information Security Policy 2.2 New Systems, 8.1.1 Security Requirements, 8.4.1 Prior to System Implementation
- Chapter 13 STRA Methodology Supplemental Document
2. SECURITY ASSURANCE ASSESSMENTS

<table>
<thead>
<tr>
<th>2.4 RECOVERY EXERCISES OF APPLICATION AND ITS COMPONENTS</th>
<th>Effective Date: TBD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Scheduled Review: TBD</td>
</tr>
</tbody>
</table>

Purpose

This standard identifies the requirement for Recovery Exercises to be performed as part of a security assessment to objectively reflect the actual state of application security and risk. This standard also specifies assessment requirements to produce meaningful results.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

This standard requires recovery exercises of an application and its components to ensure the availability of the application and the continuity of the business. It also identifies the assessment objectives and assessment tasks requirements in order to produce meaningful results at the end of the exercise.

Recovery to a known safe state removes any risks of security assessors leaving behind any malicious content or retaining any access after the engagement has completed. There is potential also that security assessments may result in unintentional impacts to an application and its components, requiring a recovery.

As per the Information Security Policy, this standard assumes that Business Continuity/Disaster Recovery (BCP/DRP) documentation exists and has been assessed for their effectiveness and the completeness prior to the requirement of an actual recovery. It is also assumed that documentation will be made available upon request from an auditor (official and unofficial as in the case of a self-imposed independent audit. See topic 2.6).

Standard

This standard applies to all existing and new web applications or web services that support government services. Re-assessments must occur after major changes to the application or to its components; otherwise, at a minimum, every three years.

This standard requires that recovery exercises as per Table 2.0 meet the following requirements:

1. Recoverability MUST have been proven prior to any security assessments being performed.
2. Recovery exercises MUST be performed in pre-production environments prior to application deployment into the production environment.

3. Recovery exercises should be performed after PEN Tests that involve high risk activities that may have potentially impacted the application and its components.

4. Recovery exercises MUST at a minimum address each entry listed in Table 6.0.

5. Evidence of the success of these recovery exercises MUST include:
   a. Log entry snapshots for the application and its component that shows recovery occurring and any status/error messages.
   b. Checklist of steps performed during the recovery from the documented recovery procedures.
   c. Checklist of steps performed to verify successful recovery e.g. data samples matching those for a specified point-in-time, application regression test results, etc.

6. All team lead technical staff involved in the recovery exercises MUST sign and date evidence.

7. All evidence MUST be dated, signed, collected, and stored by business owner responsible for the application and made available for any self-imposed audits.

8. Identified risk issues MUST be reviewed by the business application owner.

9. The business application owner MUST decide to remediate or intentionally accept the risk based on the assessment report.

### Table 6.0 Assessment Objectives and Requirements

<table>
<thead>
<tr>
<th>Assessment Type</th>
<th>Assessment Objectives</th>
<th>Assessment Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application and its Components</strong></td>
<td><strong>Recovery Exercises</strong></td>
<td>MUST report on:</td>
</tr>
<tr>
<td></td>
<td>To enable verification that:</td>
<td>1. Inability of meeting all recovery types to meet business scenarios. Where applicable,</td>
</tr>
<tr>
<td></td>
<td>1. Backup types and frequency will enable recovery for the identified business</td>
<td>a. Full recoveries</td>
</tr>
<tr>
<td></td>
<td>scenarios and within expected business timeframes.</td>
<td>b. Point-in-time recoveries</td>
</tr>
<tr>
<td></td>
<td>2. Recovery scenarios are identified and documented as procedures, and the procedures</td>
<td>c. Recovery of specific logical structures (e.g. schemas).</td>
</tr>
<tr>
<td></td>
<td>are current, effective, and complete in enabling a recovery.</td>
<td>2. Unacceptable levels of business data loss for a point-in-time recovery and on the</td>
</tr>
<tr>
<td></td>
<td>3. Reset to a known and safe state is possible.</td>
<td>inadequacy of the procedures for re-populating lost data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Unacceptable length of outage or its severity to those corresponding with the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>application STRA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Unacceptable alignment of support contracts with recovery objectives (e.g. recovery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>timelines).</td>
</tr>
</tbody>
</table>
5. Inability to reset all privileged account passwords and encryption keys.

Additional Guidance

- Activity log of penetration testing activities be provided by the Penetration Tester to be used for verifying incident response procedures.

References

- OCIO – Information Security Policy 6.5.1 Information and information systems must be backed up and the recovery process tested regularly.
2. SECURITY ASSURANCE ASSESSMENTS

Effective Date: TBD

2.5 INFORMATION SECURITY INCIDENT RESPONSE EXERCISES

Scheduled Review: TBD

Purpose
This standard identifies the requirement for Security Incident Response Exercises to be performed as part of a security assessment to objectively reflect the actual state of application security and risk. This standard also specifies assessment requirements to produce meaningful results.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context
This standard requires information security incident response exercises to be performed to ensure the effectiveness and the completeness of handling potential breaches. It also identifies the assessment objectives and assessment tasks requirements in order to produce meaningful results at the end of the exercise.

This standard assumes that documented incident response procedures exist and that an activity log has been requested from the assessor performing PEN Testing. It is also assumed that documentation will be made available upon request from an auditor (official and unofficial as in the case of a self-imposed independent audit. See topic 2.6).

Standard
This standard applies to all existing and new web applications or web services that support government services. Re-assessments must occur after major changes to the application or to its components; otherwise, at a minimum, every three years.

This standard requires that recovery exercises as per Table 2.0 meet the following requirements:

1. Information security incident Response procedures MUST be documented and exercised prior to an application being deployed.
2. Information security incident Response exercises MUST at a minimum address each entry listed in Table 7.0.
3. Any PEN Testing performed on an application and its components MUST be leveraged as an opportunity to assess the ability to respond to potential breaches.
4. Minimally, Incident Response Exercises MAY be performed as a tabletop exercise.

5. Evidence of the success of these exercises that verify detection and handling of the potential incident that coincides with the Penetration Tester’s activity log and MUST include:
   a. Log entry snapshots for the application and its component.
   b. Any email notifications of a potential incident in order.
   c. Checklist of steps performed from the documented Incident Response procedures including what incident evidence was captured and preserved for safe-keeping.
   d. Exercise worksheet with details of decisions made in investigation, in containment, and in preventing future reoccurrences.

6. All team lead technical staff involved in the recovery exercises including the investigator/forensic team leader MUST sign and date evidence.

7. All evidence MUST be dated, signed, collected, and stored by business owner responsible for the application and made available for any self-imposed audits.

8. Identified risk issues MUST be reviewed by the business application owner.

9. The business application owner MUST decide to remediate or intentionally accept the risk based on the assessment report.

<table>
<thead>
<tr>
<th>Assessment Type</th>
<th>Assessment Objectives</th>
<th>Assessment Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information security incident Response Exercises</strong></td>
<td>To enable verification that:</td>
<td>MUST report on:</td>
</tr>
<tr>
<td></td>
<td>1. Documented incident response procedures are complete and understood by responders.</td>
<td>1. Inability to meet the level of logging details or retention requirements as specified in the Province’s ARCS/ORCS to enable investigation and forensics of breaches.</td>
</tr>
<tr>
<td></td>
<td>2. Requirements to support investigation of incidents have been met e.g. logging levels.</td>
<td>2. Inability to detect PEN Tester’s activities.</td>
</tr>
<tr>
<td></td>
<td>3. Automated detection and notification systems are functioning correctly.</td>
<td>3. Inability to generate and receive expected notifications and alerts of a potential breach.</td>
</tr>
<tr>
<td></td>
<td>4. Reset to a safe state is possible.</td>
<td>4. Inability to change all application and infrastructure privileged access passwords in the event of a breach.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Inadequacy of any cross-organizational response procedures as well as internal organizational procedures.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. Inadequacy of remediation strategy to contain or prevent reoccurrence in the future of the identified incidents.</td>
</tr>
</tbody>
</table>
7. Inability to reset all privileged account passwords and encryption keys as a result of a breach.

Additional Guidance

References

- Administrative Records Classification System (ARCS) on logging which is applicable government-wide
  http://www.gov.bc.ca/citz/iao/arcs/section6/information_technology/6820.html

- Operational Records Classification System (ORCS) on logging which is applicable to a specific ministry

- Information Incident Management Process

- OCIO – Information Security Policy 6.10 Monitoring
2. SECURITY ASSURANCE ASSESSMENTS | Effective Date: TBD

2.6 SELF-IMPOSED INDEPENDENT AUDITS | Scheduled Review: TBD

Purpose
This standard identifies the requirement for self-imposed independent audits to be performed as part of a security assessment to objectively reflect the actual state of application security and risk. This standard also specifies assessment requirements to produce meaningful results.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context
This standard requires self-imposed independent audits as a means of confirming in advance the ability to pass an official audit and to satisfy reviews by external authoritative bodies (e.g. Office of the Information and Privacy Commissioner). It also identifies the objectives of the assessment and the requirements as to what should have been achieved by the end of the assessment engagement.

Standard
This standard applies to all existing and new web applications or web services that support government services. Re-assessments must occur after major changes to the application or to its components; otherwise, at a minimum, every three years.

This standard requires that a self-imposed audit as per Table 2.0 meet the following requirements:

1. Self-imposed audits MUST at a minimum address each entry listed in Table 8.0.
2. Self-imposed audits MUST assess all evidence provided.
3. Self-imposed audits MUST occur to achieve the highest level of assurances for a Security Threat and Risk Assessment (STRA).
4. Auditor for the self-imposed audit MUST summarize and state a conclusion about the ability for the application to pass an official audit.
5. Identified risk issues MUST be reviewed by the business application owner.
6. The business application owner MUST decide to remediate or intentionally accept the risk based on the assessment report.
Table 8.0 Assessment Objectives and Requirements

<table>
<thead>
<tr>
<th>Assessment Type</th>
<th>Assessment Objectives</th>
<th>Assessment Requirements</th>
</tr>
</thead>
</table>
| Self-imposed Independent Audit | To enable verification that the application would pass an audit if one should be required by OAG or if due diligence is to be proven to an external body (e.g. OIPC). | MUST report on:  
1. Inadequacy of the results of all of the other assessment types listed in standard topic 2.0.  
2. Any missing evidence that is required to pass an audit.  
3. Inadequacy of the application documentation (e.g. requirements, design, solution, deployment, operational and maintenance guide, user guides, testing strategy/plan/cases, BCP/DRP, incident response procedures, asset registers). |

Additional Guidance

- See Standard 3.2 Qualified Assessors for rules that need to be met in order to be considered an independent auditor.

References
3. **VALID EVIDENCE**

<table>
<thead>
<tr>
<th>Effective Date: TBD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Review: TBD</td>
</tr>
</tbody>
</table>

**Introduction**

The act of performing security assessments, in itself, is not guaranteed to provide an accurate picture of application security and risk. There is the potential that at the end of an assessment engagement that the results may not be considered as valid evidence and may lead to a false sense of comfort about application security. This necessitates that parameters be specified to produce assessment results that could be considered as valid evidence. Suitable evidence is required for inclusion within a Security Threat and Risk Assessments (STRAs) or for review and acceptance by an official audit.

Standard subtopics 3.1-3.3 specify the requirements for valid evidence as those that:

1. Measure compliance against recognized standards or best practices.
2. Engage a ‘qualified’ assessor to perform security assessments.
3. Contain appropriate details within a report.

In the case of recovery and incident response exercises, the above requirements do not apply.

**Additional Guidance**

**References**
3. **Valid Evidence**

<table>
<thead>
<tr>
<th>3.1 Compliance to Reputable and Independent Benchmarks</th>
<th>Effective Date: TBD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Review: TBD</td>
<td></td>
</tr>
</tbody>
</table>

**Purpose**

This standard helps business owners to identify suitable benchmark requirements to ensure that security assessments produce objective and meaningful proof of the actual state of application security and risk.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

**Context**

To generate valid evidence, the benchmark used to measure compliance is a key criterion. The benchmark should be pre-determined and agreed upon along with the instrument used for performing the measurement (e.g. automated tools, checklist, manual testing, etc.). This standard identifies recognized benchmarks for applications and the technology supporting them. This standard considers benchmarks as independent when they have been developed and reviewed by an unbiased consortium of participants and is a not-for-profit organization.

(For vendor-supplied benchmarks, see Standard 6.0)

**Standard**

This standard applies to all existing and new web applications or web services that support government services. Re-assessments must occur when new security assessments are planned; otherwise, at a minimum, annually.

All assessments of the security and risk state of an application and its components MUST be measured for compliance against recognized benchmarks as per Table 2.0 and MUST meet the following requirements:

2. Vulnerability scans and PEN Testing MUST minimally verify application code compliance with current SANS Top 25 Most Dangerous Software Errors, OWASP Top 10, and if applicable, Payment Card Industry (PCI) standards.
3. Evidence produced by vulnerability scans and PEN Testing not meeting the above requirements MUST be considered as lesser value evidence.
Additional Guidance

- Other equivalent international benchmarks may be considered in lieu of those specified above but require OCIO Information Security Branch’s approval.

References

- CIS benchmarks: [https://benchmarks.cisecurity.org/index.cfm](https://benchmarks.cisecurity.org/index.cfm)
- PCI Standards: [https://www.pcisecuritystandards.org/](https://www.pcisecuritystandards.org/)
3. **Valid Evidence**  

<table>
<thead>
<tr>
<th>3.2 Qualified and Independent Assessors</th>
<th>Effective Date: TBD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Scheduled Review: TBD</td>
</tr>
</tbody>
</table>

**Purpose**

This standard helps business owners to identify suitable assessor requirements to ensure that security assessments produce objective and meaningful proof of the actual state of application security and risk.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

**Context**

To have valid evidence, the expertise of the assessor is just as important as measuring the application against proper benchmarks. This standard identifies suitable certifications to expect from qualified assessors and the requirements for an assessor to be considered ‘independent’.

**Standard**

This standard applies to all existing and new web applications or web services that support government services. Re-assessments must occur when new security assessments are planned; otherwise, at a minimum, annually.

This standard requires that, to be deemed as a qualified assessor as per Table 2.0, the following requirements must be met (as applicable to the type of the assessment performed):

2. Security assessors MUST have knowledge and experience as indicated in a resume in the use of reputable security assessment tools and in the interpretation of assessment tool results.
3. Security assessors SHOULD have knowledge and experience as indicated in a resume of the technologies implemented within the application and its components.
4. PEN Testers MUST hold an active certification which is US Department of Defence directive (doDD) 8570 approved such as of the Global Information Assurance Certification (GIAC), International Council of E-Commerce Consultants (EC-Council) Certifications, and Mile2 Certifications.
5. Security auditors MUST hold an active Certified Information System Auditor (CISA) certification.
6. A qualified assessor MUST also be an ‘independent’ assessor. The following requirements MUST be met to qualify as an ‘independent’ assessor:
   a. Assessors MUST belong to a different firm than those contracted to develop or maintain the application, or from those configuring or providing other application components services e.g. application infrastructure and application database. This will provide an unbiased security assessment.
   b. Is not an employee of the business area that owns or is the custodian of the application and its components.
7. Assessors not meeting the above requirements MUST be considered as lesser qualified assessors.

Additional Guidance

- Other equivalent certification may be considered in lieu of those specified above but require OCIO Information Security Branch’s approval.
- Contact the OCIO Information Security Branch with any questions about the reputation of security assessment tools to be used by an assessor.

References

- Links with details on certification:
  - [http://www.giac.org/certifications/security-administration](http://www.giac.org/certifications/security-administration)
  - [http://mile2.com/about-us.html](http://mile2.com/about-us.html)
3. **VALID EVIDENCE**

| 3.3 ASSESSMENT REPORTS | Effective Date: TBD  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Scheduled Review: TBD</td>
</tr>
</tbody>
</table>

Purpose

This standard helps business owners to identify what content and information must be contained in assessment results and reports to produce objective and meaningful proof of the actual state of application security and risk.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

To have valid evidence, the content of the assessment report is just as important as measuring the application against proper benchmarks and as having qualified assessors. The term ‘assessment report’ refers to any manually written report by an assessor that provides conclusions about the security and risk state of an application and its components.

Standard

This standard applies to all existing and new web applications or web services that support government services. Re-assessments must occur when new security assessments are planned; otherwise, at a minimum, annually.

This standard requires that assessment report as per Table 2.0 meet the following:

1. Assessment reports MUST be written minimally after all assessment activities listed under the Standard 2.0. Optionally, they can be written after each type of assessment activity to be referenced in a final report.
2. An assessment report MUST contain minimally the following content and information to be considered valid evidence:
   a. Title Page with report title, assessor’s name, company name, certifications, and the date of the report.
   b. ‘Medium Sensitivity’ report designation in the report footer, watermark of report status e.g. ‘Draft Confidential’.
   c. Ownership and distribution restriction information, and distribution contact information.
   d. Executive Summary (to ensure business owners and executives understand and can reach a conclusion about the security and risk state of their application and its components)
i. Name and version of the application and the components that were assessed. The business owner supplied Information Security Classification of the application.

ii. Summary of the categories of failed assessments (e.g. failure type and the number of occurrences)

iii. Approach of the assessment:
   - Tools used to perform the assessment and what types of assessments were performed using them.
   - What assessments were performed manually.
   - Benchmark and its version used to measure compliance.
   - Perspective of testing e.g. outsider or insider testing.
   - Assumptions made prior to testing e.g. easily gathered information was provided to tester to facilitate time requirements for assessment.

iv. Assessor conclusions which would include an assertion if the application and/or its components met compliance with the specified benchmark and what residual risk may still remain.

e. Assessment Details:
   i. What each assessment task (i.e. individual tests) proved.
   ii. Potential level of risk that exists, rated as ‘high’, ‘med’, or ‘low’ Severity.
   iii. Potential impact if risk was leveraged, rated as ‘high’, ‘med’, or ‘low’ Severity.
   iv. Suggested remediation, priority, and effort rated as ‘high’, ‘med’, or ‘low’ Severity.
   v. Associated descriptions explaining implication of failed assessment task, risk, impact, and the remediation required.
   vi. Remediation plan recommendations.
   vii. Identification of attempted exploits that failed which confirmed the adequacy of existing controls.
   viii. Identification of any missing assessments or assessment tasks that would have contributed to a more accurate picture of application security and risk state. The reason for omitting them SHOULD be provided.
   ix. The identification of what within the application and its components that could not be assessed.
   x. Any limitations of the assessments e.g. non-privileged credentials were provided, so not ALL webpages were scanned for vulnerabilities during dynamic analysis of the application.

f. Assessment results in its raw format as generated by automated tools or as recorded for manual tests to collaborate report and summary included in the appendices.

g. Assessor profile and resume.

3. Assessment reports MAY remove the following details without degrading the validity of the report:
   a. Identification of what false positives may exist.
   b. Any issues rated at a low level of severity i.e. low risk and low impact issues.
4. Any assessment reports that don’t meet the above requirements MUST be considered as having lesser value as valid evidence.
Additional Guidance

- Although assessor may identify some residual risks in the application, these risks must be reviewed by the business owner. Business owners are accountable to explain the reasons for the decision to remediate or accept those risks based on their determined level of risk tolerance.

- In procurement documents, the following should also be specified pertaining to report and assessment information:
  - Written confirmation is required that any assessment related information has been destroyed at the request and sole discretion of the Province.
  - The ownership and control of access and distribution of all assessment results and reports must belong solely to the Province.

References

- Information Security Classification Framework
## Purpose

This standard helps business owners to identify the requirements for an assessed environment to be considered equivalently the same as another environment where application security and risk assertions are required.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

## Context

In some scenarios, it is not possible to test against the actual environment where assertions are required of its application security and risk state e.g. 24x7 production environments. Assertions based on an equivalent environment may be considered as the ‘next best’ valid evidence based on the rules identified within this standard. The best valid evidence is when assertions are performed against the actual environment. The least valid evidence is when assertions are performed against an environment completely different.

## Standard

This standard applies to all existing and new web applications or web services that support government services. Re-assessments must occur after major changes to the application or to its components; otherwise, at a minimum, annually.

This standard deems an environment equivalently the same as per Table 2.0 when the assessed environment is:

1. The standby or failover environment or the load-balancing environment of a server cluster.
2. Situations other than stated in #1, equivalency of the assessed environment to the asserted environment must be proven by additional evidence including:
   a. Proof that both environments were replicated identically.
      i. Automated deployment scripts of the application and of the build of its components.
      ii. Documented procedures on how the deployment is verified.
b. Documented evidence that the physical and/or logical characteristics of the application components are the same e.g. same server characteristics, same software version and patch level, etc.

c. Documented evidence explaining the difference in user access and privileges, and the reason they are acceptable e.g. Quality Assurance staff and developers have access to UAT but not to the production environment based on compliance to the Information Security Policy.

3. Assertions based on equivalently the same environments MUST be considered as having lower value than assertions based on the actual environment.

4. All other situations not meeting the above MUST be considered as a different environment and assertions based on them as having lesser value than those for equivalently the same environments and actual environments.

Additional Guidance

- Standby, failover, or load-balancing servers are not considered the actual environment since differences may exist:
  - In its geographical location from the actual environment.
  - In its logical location e.g. different network segment from the actual environment.
  - In that it is a representative sample of a group of assets e.g. a single server of a cluster.

References

  
5. **DIRECT EVIDENCE**

<table>
<thead>
<tr>
<th>Effective Date: TBD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Review: TBD</td>
</tr>
</tbody>
</table>

**Purpose**

This standard helps business owners to understand when evidence can be treated as direct evidence even when the assessor did not generate the assessment used as evidence.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs in the future.

**Context**

An assessment report may be based on evidence that the assessor personally generated and assessed, or may be a summary based on evidence generated by other assessors.

This standard identifies the circumstances when other evidence sources can be treated as a direct source. This issue is important since indirect sources of evidence should be considered as having lesser value than direct sources. Normally, evidence is considered direct evidence only when the evidence was generated by the person making assertions on the results.

**Standard**

This standard applies to all existing and new web applications or web services that support government services. Re-assessments must occur when new security assessments are planned; otherwise, at a minimum, annually.

Assertions will be considered as though based on direct evidence as per Table 2.0 when evidence:

1. Produced by another assessor meets the requirements in Standards 2.0 and 3.0 and,
   a. Is based on vulnerability testing results performed by another assessor and used by a PEN Tester. Or,
   b. Is provided to an auditor during a self-imposed audit (subtopic 2.6). Or,
   c. Is based on assessments results performed by a junior assessor, and confirmed and used by a more senior assessor of the same firm.
2. All other evidence not meeting the above MUST be considered as indirect evidence and having lesser value.
Additional Guidance

References
6. **VENDOR BENCHMARKS**

<table>
<thead>
<tr>
<th>Effective Date: TBD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Review: TBD</td>
</tr>
</tbody>
</table>

**Purpose**

This standard identifies to business owner the requirement to use vendor-supplied benchmarks when independent benchmarks are unavailable. It also identifies its value in relation to independent benchmarks.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

**Context**

To generate valid evidence, the benchmark used to measure compliance is a key criterion. Standard 3.1 discusses the use of reputable and independent benchmarks. In some situations, these are not available and so vendor-supplied benchmarks are used as another measure of compliance.

Prior to an assessment, the benchmark should be pre-determined and agreed upon along with the instrument used for performing the measurement (e.g. automated tools, checklist, manual testing etc.).

**Standard**

This standard applies to all existing and new web applications or web services that support government services. Re-assessments must occur when new security assessments are planned; otherwise, at a minimum, annually.

This standard requires as per Table 2.0 that:

1. Manual assessment should verify compliance against any vendor-supplied checklists for secure configuration and vendor documentation on security best practices for the relevant application or component technologies when recognized benchmarks are not available.
2. The results of assessment against vendor-supplied checklists must be considered as having lesser value than against independently recognized benchmarks.
Additional Guidance

- Vendor supplied checklists are considered to be of lower value since:
  - They are not independently developed or reviewed benchmarks (as listed in standard topic 3.1) and
  - Compliance assessments cannot be performed in an automated manner which reduces the likelihood of human error.

References

-
APPENDIX A - GLOSSARY

**Application** – software that performs a function. In the context of this standard, it should be considered to include the application code and all its underlying components that support it.

**Application components** – all underlying assets supporting the application i.e. network, server, middleware, database, etc.

**Application lifecycle** – the lifecycle for an application includes its development phases and also the post-implementation phase of application retirement and destruction when end-of-life has been reached.

**Application sensitivity** – the sensitivity classification associated with the application as defined by the Information Security Classification Framework.

**Audit** – is an examination of the facts to render an opinion and would include testing evidence to support the opinion.

**Benchmarks** – a baseline that another object is measured against to gauge compliance

**Breach** – an event that bypasses or contravenes security policies, practices, or procedures to gain unauthorized access to assets

**Business Application Owner** – government program area representative (usually an executive director) designated by the Information owner that is responsible for the application that supports the services for that program area.

**Commercial-off-the-shelf (COTS)** – commercially available products that can be purchased and integrated with little or no customization.

**Dynamic Code Analysis** – an assessment of executing code to identify potential logic errors and vulnerabilities that can be leveraged in a potential malicious attack.

**Equivalently the Same Environment** – term used in the context of this standard to denote a situation whereby an environment is not the actual environment but is a reasonable replication of it.

**Event** – is an identified occurrence of a system or service state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

**Evidence** - a body of facts to support a claim

**Fuzz Testing** – manual or automated tests by supplying invalid input to an application to identify inappropriate error management or exploitable conditions by hackers.
**Information Owners** – have the responsibility and decision making authority for information throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure.
Within the Government of British Columbia, information ownership flows from the Crown to government Ministers to Deputy Ministers (or equivalent). Information ownership may be further delegated by the Deputy Minister.

**Information Security Incident Response** - responding to an event that may include investigating, containing and remediating the causes of the event.

**Middleware** – is the layer of software that performs services between the application and the operating system. Examples are web servers and databases. In the context of this standard, databases may be mentioned separately for emphasis around its requirements.

**Ministry Information Security Officer (MISO)** - responsible for co-ordinating the ministry security program for protecting the confidentiality, integrity and availability of government information.

**Recovery** – the act of restoring back to a formerly captured state.

**Password Cracking** – manual and automated testing to attempt to gain unauthorized access to passwords

**Penetration Testing (PEN Testing)** – is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. This typically involves more active and potentially more aggressive tests than performing vulnerabilities scans which is passive testing. Typically a combination of automated tests and manual tests are used to limit potential impact.

**Risk** – Potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.

**Secure Access Gateway (SAG)** – administrative gateway used to access administrative tools to maintain intranet zone assets

**Security Assessment** – an evaluation performed from a security perspective that results in an indication of the state of security or the risks that may exist.

**Security Assurance Level** – the level of confidence that can be associated with security assessments as reflecting an accurate state of application security and risk.

**Security Posture** – the security status of the technical infrastructure and information systems to known vulnerabilities and attacks.
Security Threat and Risk Assessment (STRA) – a component of a risk analysis specifically aimed at identifying security exposures.

Self-imposed Independent Audit(s) – an audit that is not required by any mandatory governance body but is voluntarily initiated and engaged in. A characteristic of this audit is its unbiased nature which requires it to be performed by an external party.

Static Code Analysis – manual review or an automated assessment of coding practices pertaining to compliance against a specified standard e.g. OWASP Top 10, SANS 25 Programming Errors. Scanning can be performed against source code, byte code, or native binary code. This is performed without the application executing at the time of the scan.

Threat – in the security context, any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. A threat may be deliberate, accidental or of natural origin.

Vulnerability – in the security context, a weakness in security procedures, processes, or controls that could be exploited to gain unauthorized access to information or disrupt critical processing.