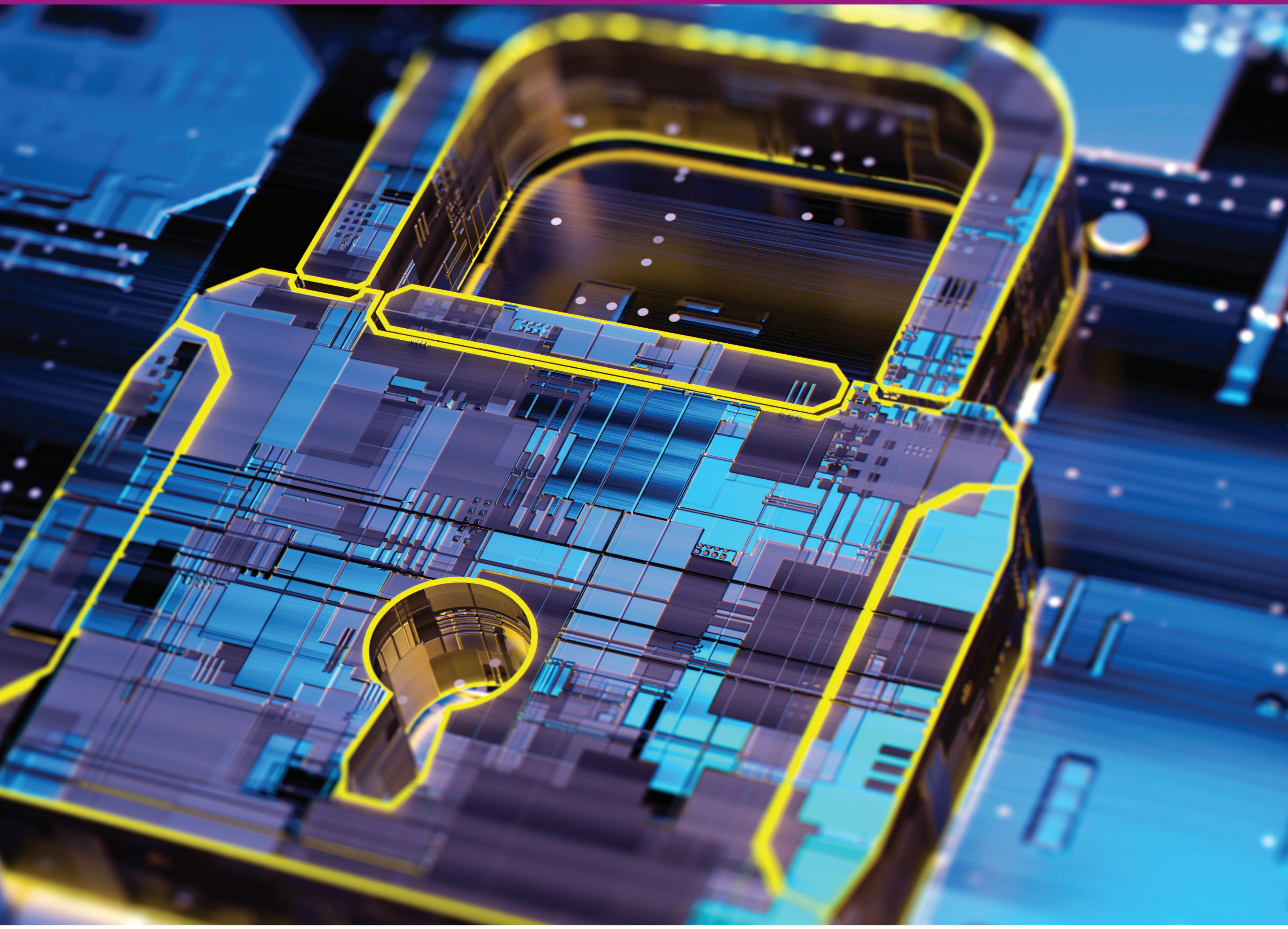
Report of the
Auditor-General

Auditor-General's
Department

Report 10 of 2021

# ICT vulnerability management in South Australian public sector entities



Government of
South Australia

[P.P.4Y

# Report of the Auditor-General

## Report 10 of 2021

## ICT vulnerability management in South Australian public sector entities

Tabled in the House of Assembly and ordered to be published, 8 June 2021

Second Session, Fifty-Fourth Parliament

By authority: S. Smith, Government Printer, South Australia

2021

*The Auditor-General's Department acknowledges and respects Aboriginal people as the State's first people and nations, and recognises Aboriginal people as traditional owners and occupants of South Australian land and waters.*

**Auditor-General's**
Department

www.audit.sa.gov.au

Enquiries about this report should be directed to:

Auditor-General
Auditor-General's Department
Level 9, 200 Victoria Square
Adelaide SA 5000

ISSN 0815-9157

Government of South Australia
Auditor-General's Department

Level 9
State Administration Centre
200 Victoria Square
Adelaide SA 5000

Tel +618 8226 9640
Fax +618 8226 9688

ABN 53 327 061 410

audgensa@audit.sa.gov.au
www.audit.sa.gov.au

7 June 2021

President
Legislative Council
Parliament House
ADELAIDE SA 5000

Speaker
House of Assembly
Parliament House
ADELAIDE SA 5000

Dear President and Speaker

**Report of the Auditor-General:**
**Report 10 of 2021 *ICT vulnerability management in South Australian public sector entities***

As required by the *Public Finance and Audit Act 1987*, I present to each of you Report 10 of 2021 *ICT vulnerability management in South Australian public sector entities*.

**Content of the Report**

The objective of this high-level review was to understand the level and maturity of the penetration testing and vulnerability scanning processes in a number of public sector entities. This involved confirming the types of public facing ICT environments maintained by each entity, the number and frequency of testing and scanning reviews performed over the past three years, the resources used to perform these reviews, and the level of remediation.

We related with the following public sector entities to obtain specific information about their penetration testing and vulnerability scanning of public facing websites, applications and devices:

- Attorney-General's Department
- Department of Infrastructure and Transport
- Department of Treasury and Finance
- Department of the Premier and Cabinet
- South Australia Police
- Courts Administration Authority
- South Australian Housing Trust
- Flinders University

- University of Adelaide
- University of South Australia.

We concluded that these entities did not always effectively manage the penetration testing and vulnerability scanning of their public facing environments.

We found that the level of penetration testing and vulnerability scanning conducted by most of these entities in the last three years was limited and adhoc. We identified several environments holding sensitive information that were not tested or scanned.

## Acknowledgements

The audit team for this Report was Andrew Corrigan, Brenton Borgman, Tyson Hancock, Abhinav Tomar and Spoorthy Chitti.

We appreciate the cooperation and assistance given by staff of the public sector entities we reviewed.

Yours sincerely

Ian McGlen
**Acting Auditor-General**

# Contents

**Appendices**

# 1 Executive summary

## 1.1 Introduction

South Australian government agencies and universities (public sector entities) govern and manage the security of their ICT systems by implementing specific cyber security controls to protect their financial and operational services.

Public facing environments are programs or systems that are accessible not only from within an entity's internal network but also from the internet. These environments are responsible for either providing services to the public or allowing access to the internal network. Given this public access, these types of programs or systems are particularly vulnerable to hackers and cyber attacks.

Penetration testing[1] and vulnerability scanning[2] help to detect and manage ICT system vulnerabilities. They are important defences for the public facing environments that are maintained by public sector entities, which include external websites, applications and devices.

This is a report on the results of a high-level review we conducted of 10 public sector entities (entities) to understand the level and maturity of their penetration testing and vulnerability scanning. The review involved confirming the types of public facing ICT environments maintained by each entity, the number and frequency of testing and scanning reviews performed in the last three years, the resources used to perform these reviews and the level of remediation.

We use a number of technical terms in this report that we explain in Appendix 1.

## 1.2 Conclusion

The entities we reviewed did not always effectively manage the penetration testing and vulnerability scanning of their public facing environments.[3]

We found that the level of penetration testing and vulnerability scanning conducted by most of these entities in the last three years was limited and ad hoc. We identified several environments holding sensitive information that were not tested or scanned.

The entities we reviewed highlighted several challenges to performing penetration testing and vulnerability scanning, including:

- ICT budget considerations
- ICT staff resourcing, including attracting and retaining skilled staff
- the rapidly changing ICT landscape.

[1] Refer Appendix 1 for an expanded definition.

[2] ibid.

[3] This excluded environments outsourced and managed by third parties.

While penetration testing and vulnerability scanning performed by these entities increased in the last 12 months, they need to further strengthen their overall management of vulnerability management security controls. This includes:

- developing comprehensive policies and procedures
- performing more assessments on a frequent basis
- improving the monitoring and tracking of testing outcomes
- improving the effectiveness of remediation.

## 1.3 What we found

| Focus area | Key findings and observations |
|---|---|
| Public facing environments (section 2) | The 10 entities we reviewed maintain 292 public facing environments comprising:<br>• 95 websites<br>• 168 applications<br>• 29 devices or supporting services. |
| | The data classifications assigned to these public facing environments were:<br>• 153 official sensitive<br>• 69 official<br>• 70 official (public). |
| General observations (sections 4 and 5) | 70% of the entities we reviewed did not have an approved policy and procedure for penetration testing and/or vulnerability scanning. |
| | Major challenges entities experience when performing penetration testing and vulnerability scanning include:<br>• ICT budget limitations<br>• lack of internal resourcing<br>• difficulty attracting and retaining skilled ICT staff<br>• difficulty keeping up with rapid changes in the ICT landscape. |
| | The top three exception areas identified in penetration testing were:<br>• configuration management<br>• information gathering<br>• authentication. |
| Penetration testing (section 6.1) | 79% of total environments reviewed were not tested in the last three years. |
| | 47% of environments that were not tested held data classified as official sensitive or above. |
| | 30% of entities do not perform any additional penetration testing after the initial implementation. |
| | 30% of entities performing penetration testing do not track the remediation of issues raised. |
| | 60% of entities do not reperform penetration testing to ensure the adequacy of remediation undertaken. |

| Focus area | Key findings |
|---|---|
| Vulnerability scanning (section 6.2) | 40% of total environments reviewed were not subject to vulnerability scanning in the last three years. |
| | 51% of environments that were not scanned held data classified as official sensitive or above. |
| | 50% of entities do not perform ongoing vulnerability scanning. |
| | 50% of entities performing vulnerability scanning do not track the remediation of matters raised. |
| | 40% of the entities do not reperform vulnerability scanning to ensure the adequacy of remediation undertaken. |

## 1.4 What we recommended

| Focus area | Recommendation |
|---|---|
| Security governance (section 4) | Public sector entities need to develop penetration testing and vulnerability scanning policies and procedures that align with best practices and frameworks such as the South Australian Cyber Security Framework and the International Standard ISO/IEC 27001 *Information Security Management*. |
| Penetration testing and vulnerability scanning detailed findings (section 6) | Public sector entities should conduct periodic penetration testing and vulnerability scanning to evaluate vulnerabilities across their public facing environments.<br>The results of these activities should be documented, tracked in an ICT risk register and reported to the governance committee responsible for ICT. |

# 2 Background

## 2.1 Overview

Many Australian companies and government entities have fallen victim to cyber security attacks and data breaches.[4] As such all entities need to proactively identify and remediate any security vulnerabilities in their ICT environments.

While entities seek to establish risk management plans/strategies to assist in remediating potential operational threats, a key input to this process should be penetration testing and vulnerability scanning.

## 2.2 Relevant ICT frameworks and standards

To identify and understand their responsibilities and obligations to safeguard data and ensure their ICT risks are managed effectively, public sector entities should consider applying a number of ICT frameworks and standards, including:

- ISO 27001 *Information Security Management Standard*
- South Australian Cyber Security Framework
- Commonwealth Information Security Manual.

### 2.2.1 ISO/IEC 27001 *Information Security Management*

ISO/IEC 27001 is an international standard that outlines the key cyber security processes and approaches that a business should adopt to their environment.

The 'management of technical vulnerabilities' control states:

> *Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.*

### 2.2.2 South Australian Cyber Security Framework

This is a risk-based framework developed to assist with preserving the confidentiality, integrity and availability of information by applying appropriate management processes. It is a mandatory framework for SA Government agencies.

[4] Refer to <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2020/>.

The framework requires the establishment of a vulnerability management strategy that includes:

- developing a policy relating to vulnerability scanning and penetration testing
- conducting vulnerability scanning and penetration tests for systems throughout their lifecycle
- analysing security vulnerabilities to determine their potential impact on the confidentiality, integrity and availability of data
- undertaking appropriate mitigations or treatments based on effectiveness, cost and existing security controls.

### 2.2.3 Commonwealth Information Security Manual

The Australian Cyber Security Centre has developed prioritised strategies to help IT security professionals mitigate cyber security incidents caused by various external and/or internal threats.

The information security manual recommends that, as part of continuous monitoring, IT security controls should include:

- testing of systems for security vulnerabilities before being used in a production environment
- conducting vulnerability scans for systems at least monthly
- conducting penetration tests or vulnerability scanning for systems at least annually
- analysing identified security vulnerabilities to determine their potential impact
- appropriate mitigations based on effectiveness, cost and existing security controls
- using a risk-based approach to prioritise the implementation of identified mitigations.

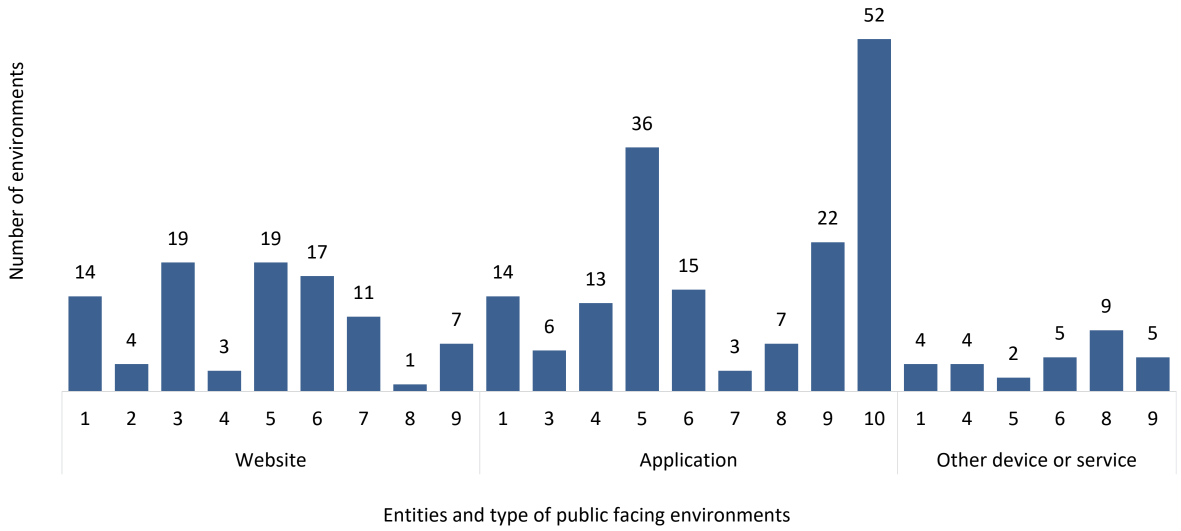
## 2.3 Summary of public facing environments

We identified 292 public facing environments across the seven agencies and three universities we reviewed. There were 95 websites, 168 applications and 29 devices[5] or other services.[6]

[5] Examples of public facing devices include firewalls and network load balancers.

[6] Examples of other services that are public facing include remote access connections such as Citrix systems.

**Figure 2.1: Public facing environments across the entities we reviewed**

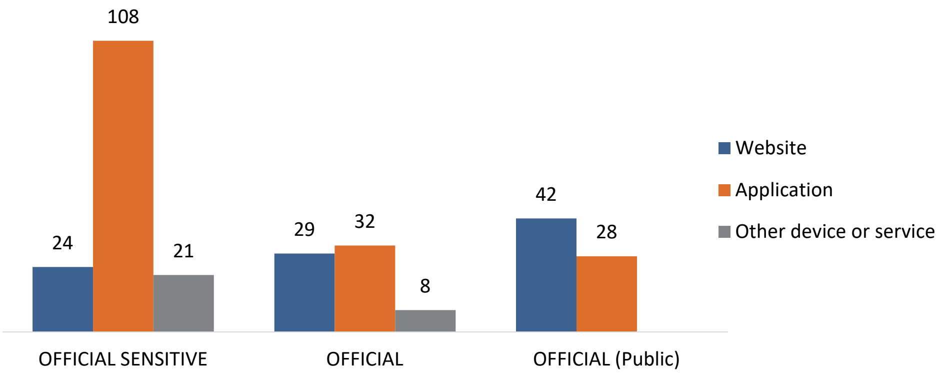


* The numbering of entities in this table is random and does not correlate with the entity listing in section 3.

These public facing environments are on-premises and do not include environments that are outsourced (such as a Cloud environment) and managed by an external third party.

Of the 292 identified environments, we confirmed that 222 hold or access information classified as official sensitive[7] or official.[8] The remaining 70 environments are classified as official but also contain publicly available information.[9] These classifications are in line with the applicable Commonwealth and/or South Australian Cyber Security Framework data classification directives.

**Figure 2.2: Information classification by environment type**



[7] Official sensitive as defined by the Commonwealth indicates that compromise of this type of information may result in limited damage to an individual, organisation or government generally.

[8] Official as defined by the Commonwealth is information that was created or processed by the South Australian public sector with a low business impact.

[9] Publicly available information is defined as information that has been formally authorised for release into the public domain.

# 3 Review objective, scope and approach

## 3.1 Our mandate

The Auditor-General has authority to conduct this review under section 36(1)(a)(iii) of the *Public Finance and Audit Act 1987*.

## 3.2 Our objective, scope and approach

The objective of our review was to understand the extent and impact of penetration testing and vulnerability scanning of public facing environments in public sector entities. As part of this review, we sought high-level information from a number of public sector entities.

We sent questionnaires to the following public sector entities to obtain specific information about their use of penetration testing and vulnerability scanning of public facing websites, applications and devices:

- Attorney-General's Department
- Department for Infrastructure and Transport
- Department of Treasury and Finance
- Department of the Premier and Cabinet
- South Australia Police
- Courts Administration Authority
- South Australian Housing Trust
- Flinders University
- University of Adelaide
- University of South Australia.

The information we sought from these entities detailed:

- which of them had performed penetration testing and vulnerability scanning of their public facing websites, applications and devices. We also obtained copies of the most recent assessments they had conducted in the last three years
- the type of scanning and testing undertaken specific to the public facing websites, applications and/or devices
- the frequency of their penetration testing and vulnerability scanning reviews, where applicable
- the resourcing and support arrangements used to perform penetration testing and vulnerability scanning.

We relied on the completeness and accuracy of the information provided by these entities.

# 4 Security governance

## 4.1 Policy and procedure weaknesses

### 4.1.1 Most entities did not have formal policies and procedures for penetration testing and vulnerability scanning

#### What we recommend

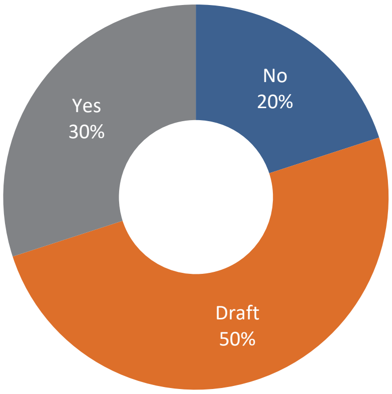
We recommend that all entities develop policies and procedures for penetration testing and vulnerability scanning. These should align with best practices and frameworks such as the South Australian Cyber Security Framework and the International Standard ISO/IEC 27001.

#### Finding

We found that most of the entities we reviewed did not have a formally documented policy and procedure describing the requirements for penetration testing and vulnerability scanning.

Several entities advised us that they are currently developing these guidance documents.

**Figure 4.1: Number of entities with policies and procedures for penetration testing and vulnerability scanning**



#### Why this is important

Policies and procedures help to establish a clear direction on how penetration testing and vulnerability scanning should be consistently managed within the entity. They should include an appropriate definition of accountability and responsibilities.

# 5 Common ICT security observations

## 5.1 Common observations

### 5.1.1 Key ICT security weaknesses and challenges

We asked entities to tell us what ICT related weaknesses and challenges they currently experience that could impact their overall ICT security. Entities indicated that potential weaknesses and challenges to perform such testing included:

- ICT budget limitations
- lack of internal resourcing
- inability to attract and retain skilled ICT staff
- ongoing use of legacy applications
- inability to keep up with the rapidly changing ICT landscape.

### 5.1.2 Half of the entities we reviewed had experienced a security incident in a public facing environment

Half of the entities we reviewed reported that they had experienced a security incident in a public facing environment in the past two years.

Some of these incidents related to a Denial of Services attack and attempts to:

- exploit existing security vulnerabilities
- deface an entity’s website(s)
- access various entity’s system(s)
- commit fraud.

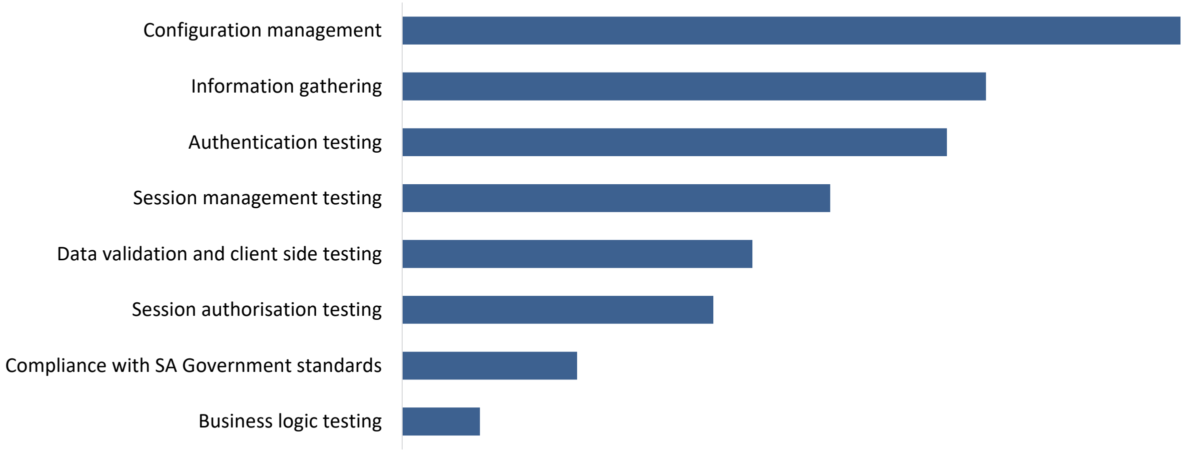
### 5.1.3 Common penetration test observations from the last three years

We asked the 10 entities we reviewed to provide us with reports on any penetration testing they had performed in the last three years. We received 54 penetration testing reports.

Collectively, these reports identified 316 findings (many were similar between entities) across multiple environments that required action. Five actions were rated critical, 45 were rated high and 79 were rated medium.

We summarised the reported findings into common categories shown in figure 5.1.

**Figure 5.1: Common penetration test findings**



We note that the top three penetration test findings are in the areas of configuration management, information gathering, authentication and session management.

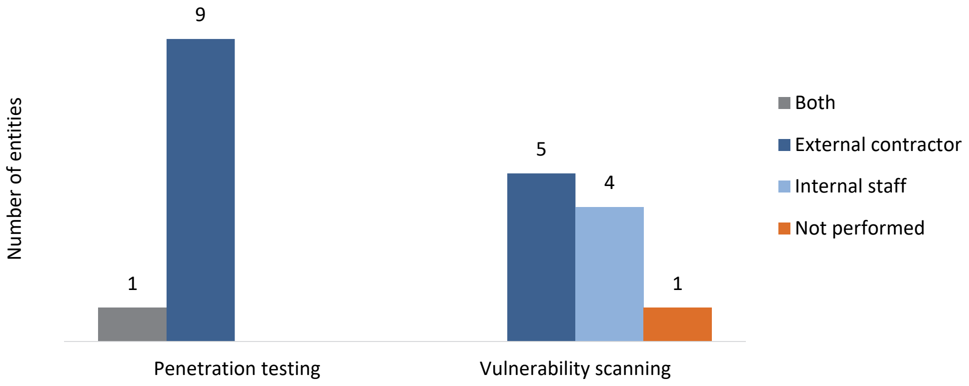
### 5.1.4 Both internal and external resources are used for penetration testing and vulnerability scanning

We asked entities what resources they used to conduct penetration testing and vulnerability scanning of their public facing environments. Most entities responded that they tended to use external contractors for penetration testing.

The resourcing of vulnerability scanning was evenly split between internal resources and external contractors. One entity does not perform any vulnerability scanning at this stage.

Entities that outsourced this testing advised us that this was done primarily to gain independent assurance and because of a lack of available internal skilled resources.

**Figure 5.2: Resources used to conduct penetration testing and vulnerability scanning**



# 6 Penetration testing and vulnerability scanning detailed findings

Penetration testing and vulnerability scanning are crucial to an entity's security by:

- understanding and highlighting potential areas of risk and breaches that may arise
- uncovering major system vulnerabilities before undertaking significant changes or other IT application and infrastructure changes
- providing solutions to help detect and prevent cyber security attacks.

### What we recommend

Entities should conduct periodic penetration testing and vulnerability scanning to evaluate information security controls of all public facing environments.

The results of these activities should be documented and tracked in the ICT risk register and reported to the governance committee responsible for ICT.

## 6.1 Penetration testing detailed findings

Our review of the 10 selected entities focused on identifying the level of penetration testing they performed over the last three years on their public facing websites, applications and devices.

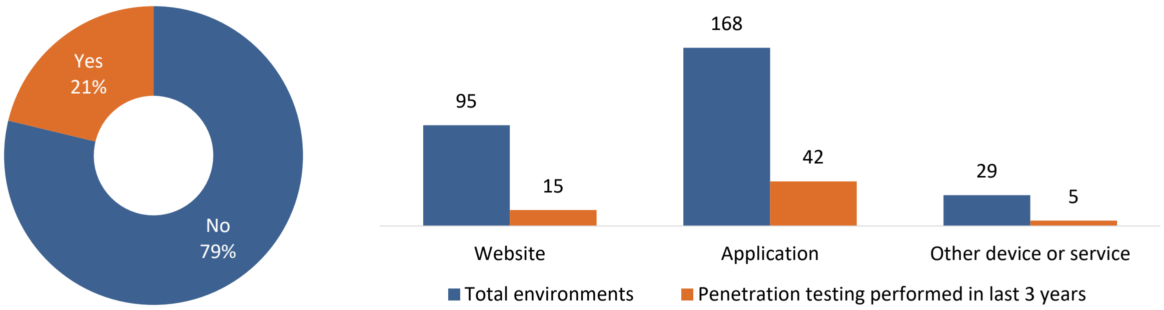
### 6.1.1 Most entities had not performed penetration testing of their public facing environments in the last three years

Of the total 292 environments we identified, only 62 (21%) were subject to penetration testing in the last three years. Of those, 15 were websites, 42 were applications and five were devices or other services.

Of the 10 entities we reviewed, eight used external contractors to perform penetration testing. The other two used both internal and external resources.

The entities stated that they engaged external contractors primarily because they did not have adequate skilled resources or tools to perform this type of testing and were also seeking to gain a level of independent assurance.

**Figure 6.1: Penetration testing performed in the last three years**



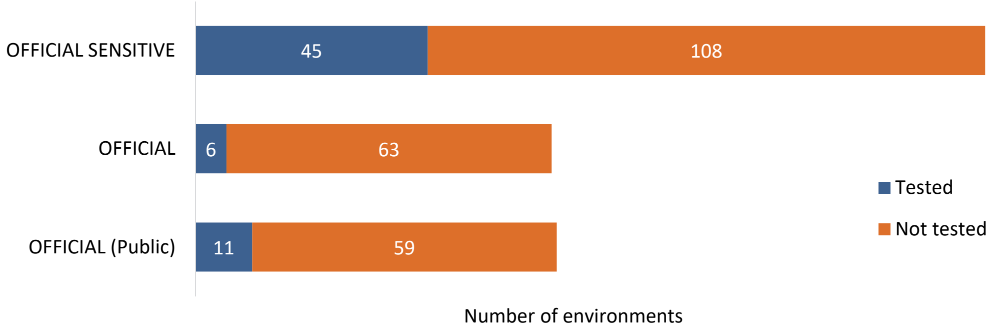
## Why this is important

Without regular penetration testing being performed the entity may not be aware of potential security weaknesses in their environment that could be exploited.

## 6.1.2 For environments that were not tested in the last three years, nearly half were classified official sensitive

We noted that of the 230 public facing environments that were not subject to a penetration test in the last three years, 108 (47%) were classified as official sensitive.

**Figure 6.2: Extent of penetration testing performed by data classification**



## Why this is important

Environments that contain official sensitive data would by definition potentially cause limited damage to an individual, organisation or government generally and hence may be more valuable to a hacker than other public facing environments.

## 6.1.3 Frequency of penetration testing of public facing environments

All of the entities we reviewed advised us that they perform penetration testing of their public facing environments on implementation. Three entities advised that they had not performed any further testing.

Six entities advised us that they performed penetration testing on some of their public facing environments after implementation, for example after a major upgrade. Only one entity advised they performed annual penetration testing of all their public facing environments.

**Figure 6.3: Frequency of penetration testing**

| Frequency | Number of entities |
|---|---|
| Only on implementation | 3 |
| On implementation and after a major upgrade | 6 |
| On implementation, after a major upgrade and annually | 1 |

## Why this is important

Penetration testing should be regularly conducted, regardless of the level of change during the environmental life cycle of the ICT system. This is because new ICT vulnerabilities are regularly discovered and should be tested.

## 6.1.4 Some entities had not tracked previously raised penetration testing issues

We found that only seven of the 10 entities we reviewed were tracking the remediation of issues raised in previous penetration tests.  These entities were using various software tools to do this.

Where issues were identified in a penetration test, only four of the 10 entities reperformed the testing to confirm that the issue had been appropriately remediated.

**Figure 6.4: Tracking and remediation of penetration testing issues**

| Entity* | Effective tracking of remediation | Reperform penetration testing of identified issues |
|---|---|---|
| 1 | ✓ | ✗ |
| 2 | ✓ | ✓ |
| 3 | ✗ | ✗ |
| 4 | ✓ | ✗ |
| 5 | ✓ | ✗ |
| 6 | ✗ | ✓ |
| 7 | ✓ | ✗ |
| 8 | ✓ | ✓ |
| 9 | ✓ | ✗ |
| 10 | ✗ | ✓ |

* The numbering of entities in this table is random and does not correlate with the entity listing in section 3.

## Why this is important

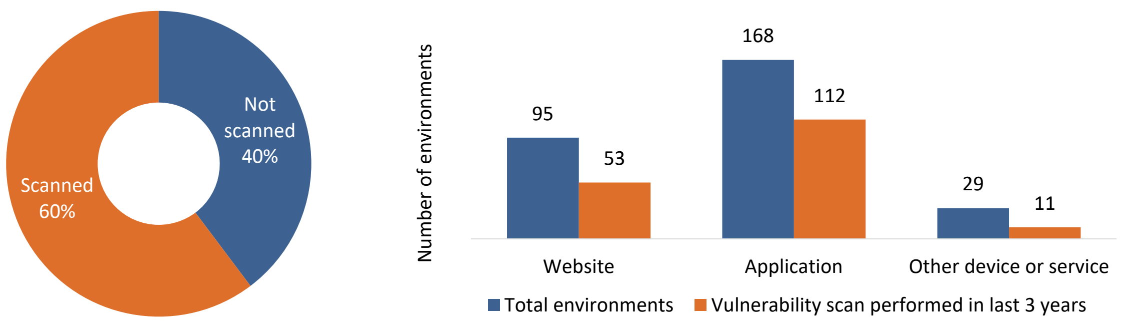
Insufficient tracking and remediation of previously raised penetration testing issues may result in identified vulnerabilities not being addressed in a timely manner.  This increases the risk of cyber security incidents occurring.

## 6.2 Vulnerability scanning detailed findings

### 6.2.1 Some environments had not recently been subject to vulnerability scans

Of the 292 environments in the 10 entities we reviewed, we found that only 176 (60%) were subject to a vulnerability scan in the last three years.

**Figure 6.5: Number of vulnerability scans conducted in the entities we reviewed**



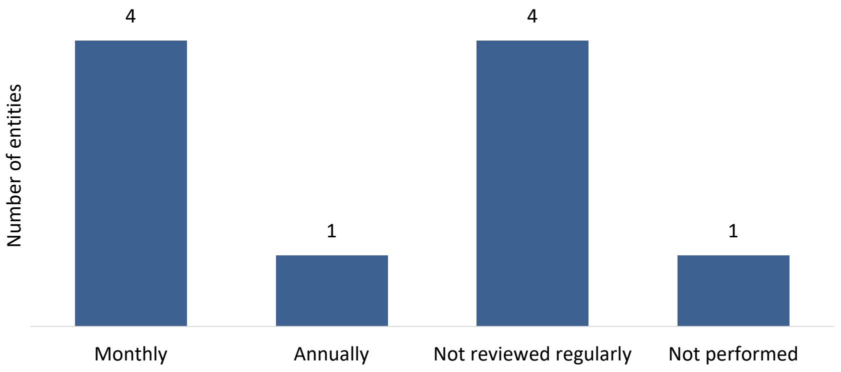
### Why this is important

Vulnerability scanning helps to identify, classify and prioritise potential security weaknesses in entities' public facing websites, applications and devices. This can help entities to implement suitable countermeasures that will mitigate the risks/weaknesses.

### 6.2.2 Half of the entities we reviewed were not regularly scanning their public facing environments for vulnerabilities

Of the 10 entities we reviewed, five were not regularly scanning their public facing environments for vulnerabilities.

**Figure 6.6: Frequency of vulnerability scanning in the entities we reviewed**



We also sought to understand which public facing environments, based on the classification of the data that they held, were subject to vulnerability scanning.

Of the 292 environments across the 10 entities we reviewed, 116 were not subject to any vulnerability scanning in the last three years. Of these 116 environments, 59 environments (51%) contained official sensitive data.

**Figure 6.7: Vulnerability scanning by data classification**

| Data classification | Public facing environments | Vulnerability scan performed in last three years | Percentage |
|---|---|---|---|
| Official Sensitive | 153 | 94 | 61% |
| Official | 69 | 59 | 86% |
| Official (Public) | 70 | 23 | 33% |
| Total | 292 | 176 | 60% |

## Why this is important

Hackers are constantly trying to develop new ways to compromise ICT systems.

Performing proactive regular vulnerability scanning of an entity's public facing websites, applications and devices helps entities to find and remediate vulnerabilities that could be potentially used by hackers.

### 6.2.3 Some entities were not remediating and tracking previous issues raised

Five of the 10 entities we reviewed reported that they were performing monthly vulnerability scanning. However, some of them were not remediating and tracking previous issues raised.

**Figure 6.8: Tracking and remediation of vulnerability scanning issues**

| Entity* | Effective tracking of remediation | Reperform vulnerability scanning of identified issues |
|---|---|---|
| 1 | ✓ | ✓ |
| 2 | ✓ | ✓ |
| 3 | ✗ | ✓ |
| 4 | ✗ | ✗ |
| 5 | ✓ | ✗ |
| 6 | ✗ | ✓ |
| 7 | Do not perform scans | Do not perform scans |
| 8 | ✓ | ✓ |
| 9 | ✓ | ✓ |
| 10 | Do not perform scans | Do not perform scans |

* The numbering of entities in this table is random and does not correlate with the entity listing in section 3.

## Why this is important

Insufficient tracking and remediation of previously raised vulnerability testing issues may result in them not being addressed in a timely manner. This increases the risk of cyber security incidents occurring.

# Appendix 1 – Explanation of terms used in this Report

| Term | Description |
|---|---|
| Penetration testing | a security exercise where a cyber security expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots that could be exploited by hackers. |
| Vulnerability scanning | a process or software tool used to proactively identify network, application and security vulnerabilities. The vulnerability scanner compares details about the scanned environment to a database of known flaws, coding bugs, packet construction anomalies, default configurations and potential paths to sensitive data that can be exploited by hackers.<br>Vulnerability scanning provides immediate feedback on the health and security of a network. Based on the information provided, direct action can be taken to better protect the network. |
| Cyber security or IT security | relates to the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation. |
| Public facing environments | are programs or systems that are not only accessible from within the internal network but are also accessible from the internet. These environments are responsible for either providing services to the public or allowing access to the internal network. |
| Configuration management | focuses on settings specific to infrastructure and architecture that apply across its operation. It may include such things as source code, administrative functionality and authentication methods. |
| Information gathering | focuses on the gathering of public information resources that may reveal the technical specification of the environment. |
| Authentication | focuses on the means to identify any authentication methods in use and to determine if the method is susceptible to account enumeration, dictionary, and brute force attacks. The security of user credentials in transit and storage is also assessed. |