



Business Information Security

Week 12:

- Security Maintenance: Security Auditing and Testing

Dr Alex Pudmenzky

Semester 2, 2024

Security Auditing and Testing

- A security audit is a crucial type of evaluation to avoid a data breach
- Auditing a computer system involves checking to see how its operation has met security goals
- Audit tests may be manual or automated
 - Manual tests include interviewing your staff, performing vulnerability scans, reviewing application and OS access controls, analyzing physical access to the systems etc.
 - With automated tests the auditing software creates a report of any changes to important files and settings.
- Before you can determine whether something has worked, you must first define how it's supposed to work, you need to create the policies and procedures that establish the rules and requirements of the system
 - Known as assessing a system



THE UNIVERSITY
OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

Part 1: Security Auditing

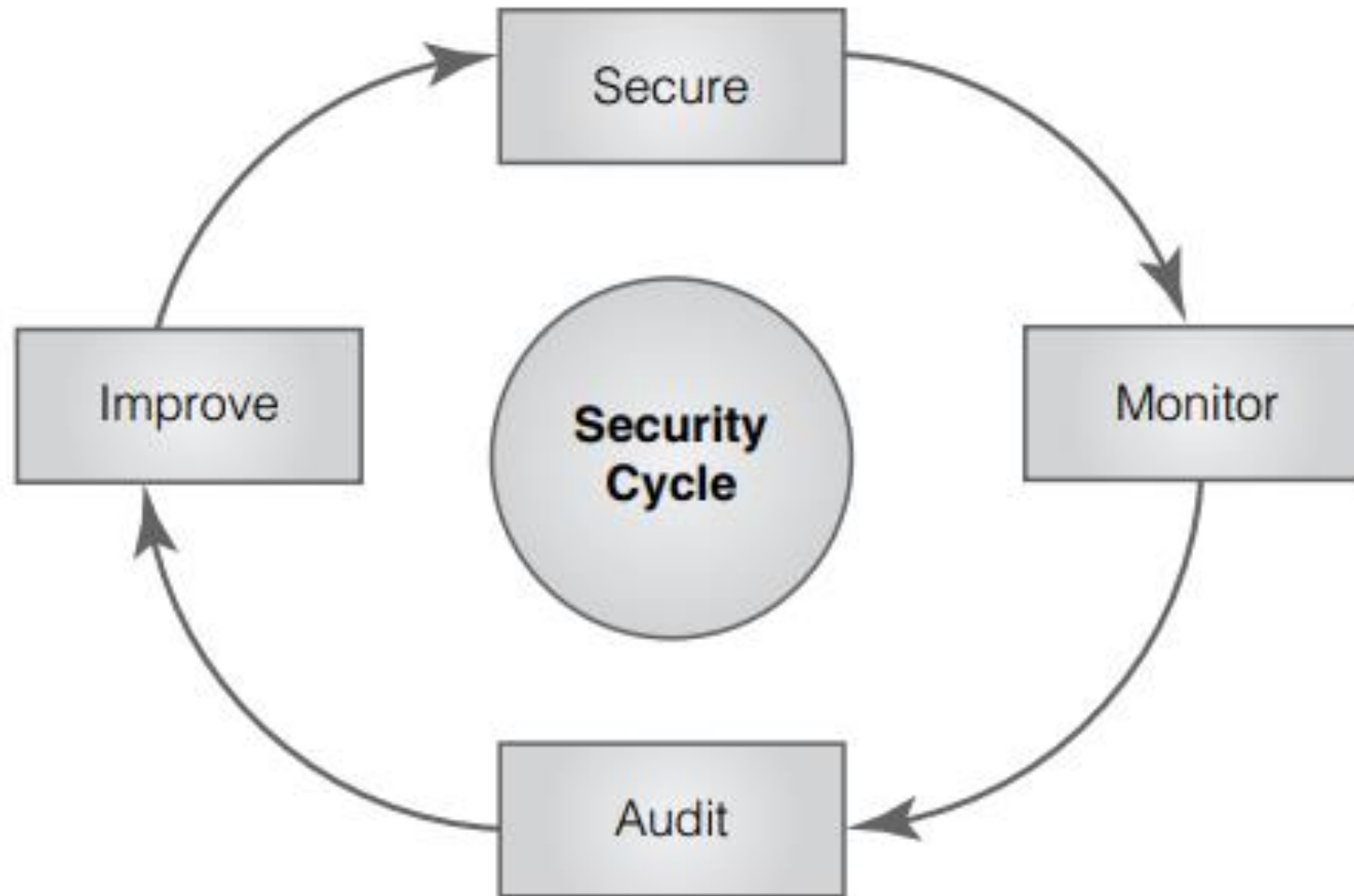
Security Auditing and Analysis

Are security policies
sound and appropriate
for the business or
activity?

Are there controls
supporting your
policies?

Is there effective
implementation and
upkeep of controls?

Security Controls address Risk



Determining What is Acceptable

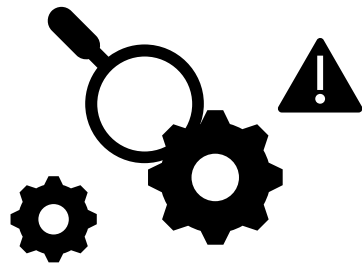
- Define acceptable and unacceptable actions in security policies
- Create standards based on those developed or endorsed by standards bodies
- Communications and other actions **permitted** by a policy document are *acceptable*
- Communications and other actions specifically **banned** in your security policy are *unacceptable*
- *Any action that may reveal confidential information, cause damage to a system's integrity, or make the system unavailable is also unacceptable, even if the policy does not specifically ban it*

Permission Levels

- Promiscuous — Everything is allowed (**home users**)
- Permissive — Anything not specifically prohibited is allowed (**public Internet sites, some schools and libraries, and many training centers**)
- Prudent — A reasonable list of things is permitted; all others are prohibited (**most businesses**)
- Paranoid — Very few things are permitted; all others are prohibited and carefully monitored (**secure facilities**)

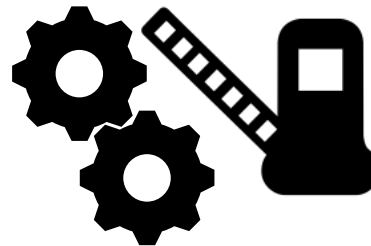
Types of Security Audits

- Large in scope and cover entire departments or business functions
- Narrow and address only one specific system or control



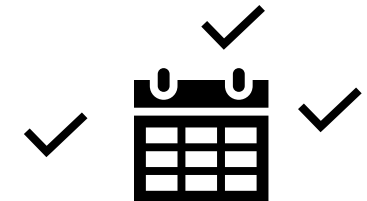
One-Time

For special events like
introducing new software



Tollgate

Give a ,yes' or ,no' to the usage
of a new process



Portfolio

Regularly-scheduled audits to
verify and assess procedures

Purpose of Security Audits

An audit gives you the opportunity to review your risk management program and to confirm that the program has correctly identified and reduced (or otherwise addressed) the risks to your organisation.

Appropriateness of controls

- Is the level of security control suitable for the risk it addresses?

Correct installation of controls

- Is the security control in the right place and working well?

Address purpose of controls

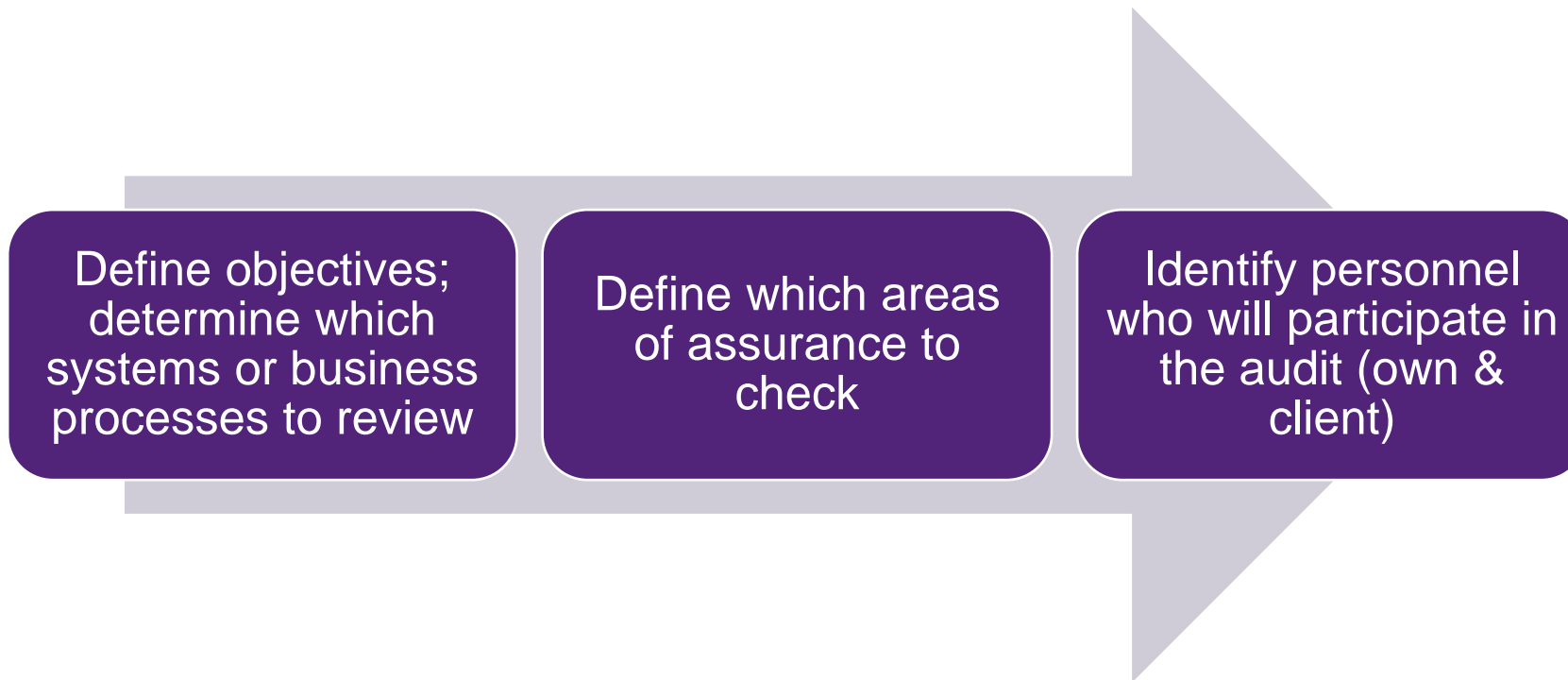
- Is the security control effective in addressing the risk it was designed to address?

Service Organisational Control (SOC) Reports

The *American Institute of Certified Public Accountants* has recognized the increased complexities of service organisations (such as cloud service providers) and created three different levels of audit reporting for service organisations. The Service Organisation Control (SOC) framework defines the scope and contents of three levels of audit reports.

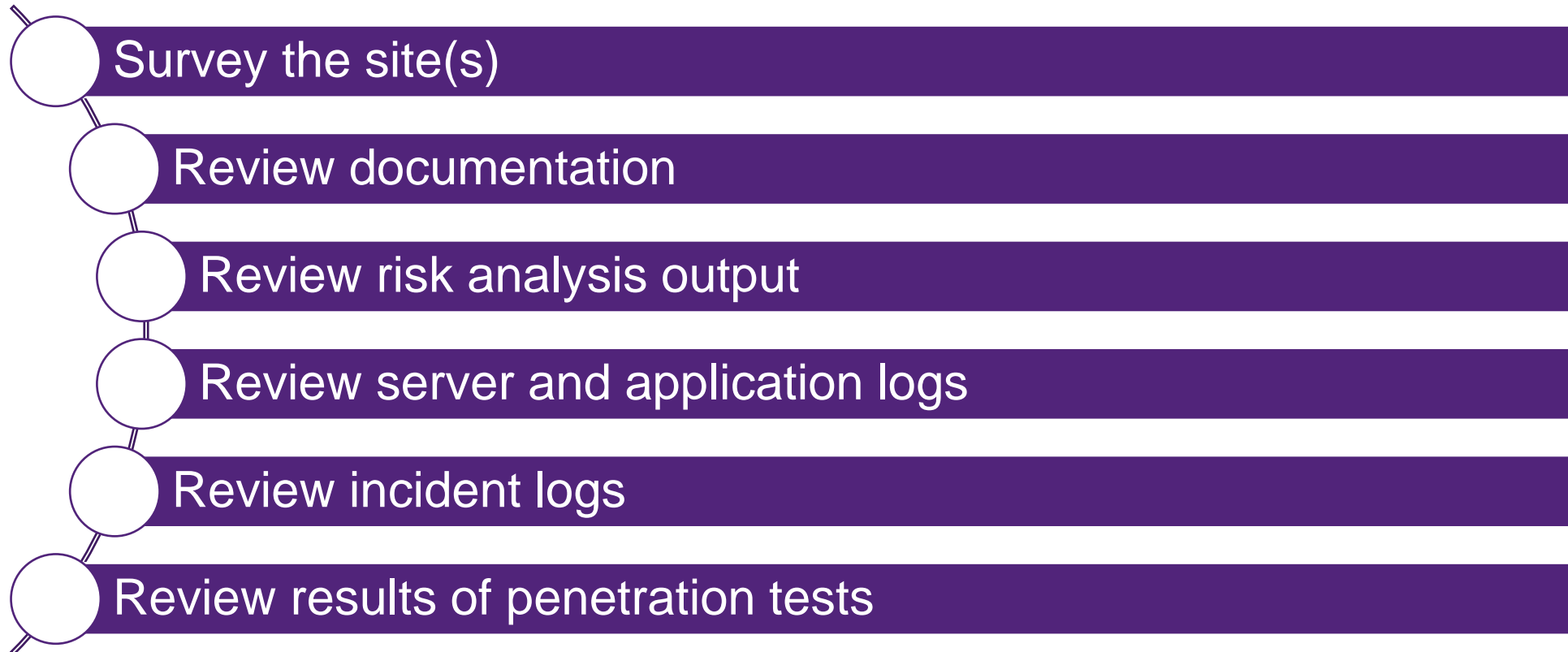
| REPORT TYPE | CONTENTS | AUDIENCE |
|-------------|--|--|
| SOC 1 | Internal controls over financial reporting | <ul style="list-style-type: none">• Users and auditors.• Commonly implemented for organisations that must comply with the Sarbanes Oxley (SOX) Act. The <i>Sarbanes-Oxley Act</i> of 2002 is a United States federal law that mandates certain practices in financial record keeping and reporting for corporations |
| SOC 2 | Security (confidentiality, integrity, availability) and privacy controls | <ul style="list-style-type: none">• Internal• Management, regulators, stakeholders.• Commonly implemented for service providers, hosted data centers, and managed cloud computing providers |
| SOC 3 | Security (confidentiality, integrity, availability) and privacy controls | <ul style="list-style-type: none">• Public• Commonly required for the customers of SOC 2 service providers to verify and validate that the organisation is satisfying customer private data and compliance law requirements |

Planning the Audit



include past
audit results?

Defining the Scope of the Plan



Benchmarks for Audits

Benchmark – The standard to which your system is compared to determine whether it is securely configured

- ISO 27002
- NIST Cybersecurity Framework (CSF)
- ITIL
 - COBIT
 - COSO

ITIL: Information Technology Infrastructure Library

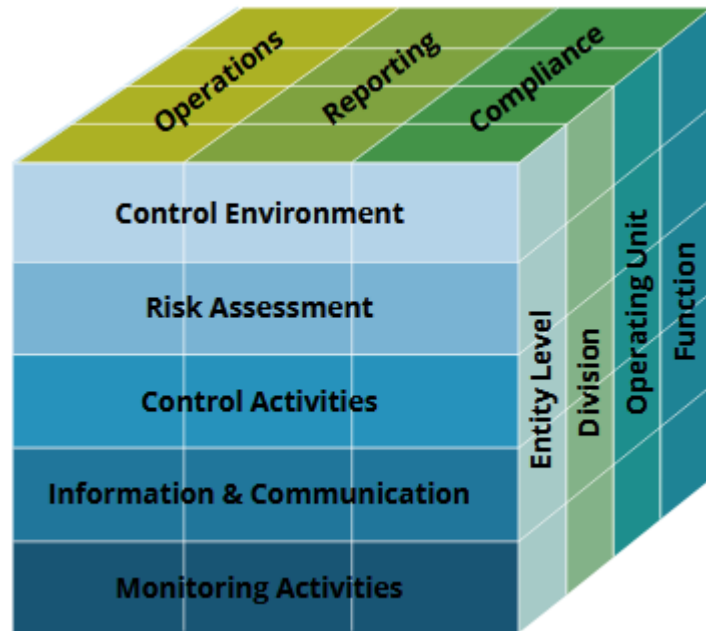
COBIT: Control Objectives for Information and related Technology

COSO: Committee of Sponsoring Organizations of the Treadway Commission

Benchmarks for Audits

- **ISO 27002** — We have run into this one before. ISO 27002 is a best-practices document that gives good guidelines for information security management. For an organisation to claim compliance, it must perform an audit to verify that all provisions are satisfied. ISO 27002 is part of a growing suite of standards, the ISO 27000 series, that defines information security standards.
- **NIST Cybersecurity Framework (CSF)** —NIST CSF, first released in 2014, is a response to a U.S. Presidential Executive Order calling for increased cybersecurity. It focuses on critical infrastructure components but is applicable to many general systems. The road map provides a structured method to securing systems that can help auditors align business drivers and security requirements. NIST also publishes a series of special publications that cover many aspects of information systems. For example, NIST SP 800-37 is a standard that describes best practices, including auditing, for U.S. government information systems.
- **ITIL (Information Technology Infrastructure Library)** —This is a set of concepts and policies for managing IT infrastructure, development, and operations. ITIL is published in a series of books, each covering a separate IT management topic. ITIL gives a detailed description of a number of important IT practices, with comprehensive checklists, tasks, and procedures that any IT organisation can tailor to its needs.

The COSO ERM Framework



The COSO Cube

© 2015 Deloitte & Touche Enterprise Risk Services Pte Ltd

- a) **Control Environment** — Does the board understand the organisation's cyber risk profile and are they informed of how the organisation is managing the evolving cyber risks management faces?
- b) **Risk Assessment** — Has the organisation and its critical stakeholders evaluated its operations, reporting and compliance objectives, and gathered information to understand how cyber risk could impact such objectives?
- c) **Control Activities** — Has the entity developed control activities, including general control activities over technology that enable the organisation to manage cyber risk within the acceptable level of tolerance to the organisation? Have such control activities been deployed through formalized policies and procedures?
- d) **Information and Communication** — Has the organisation identified information requirements to manage internal control over cyber risk? Has the organisation defined internal and external communication channels and protocols that support the functioning of internal control? How will the organisation respond to, manage, and communicate a cyber risk event?
- e) **Monitoring Activities** — How will the organisation select, develop, and perform evaluations to ascertain the design and operating effectiveness of internal controls that address cyber risks? When deficiencies are identified how are these deficiencies communicated and prioritized for corrective action? What is the organisation doing to monitor their cyber risk profile?

Summary: The COSO Enterprise risk management (ERM) framework calls on the Internal Audit Function to assist management and the board of directors and its audit committee by examining, evaluating, reporting on and recommending improvements to the adequacy and effectiveness of the entity's ERM process.

Audit Data Collection Methods

Questionnaires

Interviews

Observation

Checklists

Reviewing
documentation

Reviewing
configurations

Reviewing policy

Performance
security testing

...

Areas included in Audit Plan

| Area | Audit Goal |
|--|---|
| Antivirus software | Up-to-date, universal application |
| System access policies | Current with technology |
| Intrusion detection and event monitoring systems | Log reviews |
| System-hardening policies | Ports, services |
| Cryptographic controls | Key management, usage (network encryption of sensitive data) |
| Contingency planning | Business continuity plan, disaster recovery plan, and continuity of operations plan |

Areas Included in Audit Plan (cont.)

| Area | Audit Goal |
|---|--|
| Hardware and software maintenance | Maintenance agreements, servicing, forecasting of future needs |
| Physical security | Doors locked, power supplies monitored |
| Access control | Need to know, least privilege |
| Change control processes for configuration management | Documented, no unauthorized changes |
| Media protection | Age of media, labeling, storage, transportation |

Example: Control Checks and Identity Management

It is important to ensure that your security controls are effective, reliable, and functioning as you intended. Without monitoring and reviewing, you have no assurance that your information security program is effective or that personnel are exercising due diligence.

When auditing an **identity management system**, you should focus on these key areas:

- **Approval process:** who grants approval for access requests?
- **Authentication mechanisms:** What mechanisms are used for specific security requirements?
- **Password policy and enforcement:** Is there an effective password policy and is it uniformly enforced?
- **Monitoring:** does the organisation have sufficient monitoring systems to detect unauthorized access?
- **Remote access systems:** are all systems properly secured with strong authentication?

Post-Audit activities

- Exit interview
- Data analysis
- Generation of audit report
 - Findings
 - Recommendations
 - Timeline for implementation
 - Level of risk
 - Management response
 - Follow-up
- Presentation of findings
 - Might lead to changes based on regulatory requirements or available budget.

Example Security Audit Report: Passwords

Recommendation 8: Accounts with Non Expiry Passwords

(Priority 2)

Recommendation

A review should be carried out of all accounts whose passwords never expire and controls for these passwords changed to ensure that they are required to change their password in line with best practice.

Should there be an exception where its implementation may affect the operation of the service, this should be documented and its exception authorised by senior management.

Observation

Requiring the use of passwords that meet leading practice standards enhances the integrity and security of the system and changing passwords on a regular basis helps to improve security and minimises the risk of unauthorised access.

There were 148 user accounts defined on the network whose passwords are set to never expire. Although the majority are service or system accounts or group mail boxes, we identified that there were still some individual accounts that were not required to change their passwords in line with system security settings.

Weak password controls can result in a loss of accountability for actions performed, and increases the risk of unauthorised, or inappropriate, access to systems and information resources.

Responsibility

██████ – ICT Team Leader

Management response

Agreed - A policy on exceptions to passwords will be developed. Some exceptions maybe needed for non-expiry accounts in order to run day to day IT operations. For exceptions a business case will need to be signed off by an Assistant Director.

Implementation will be with immediate effect.

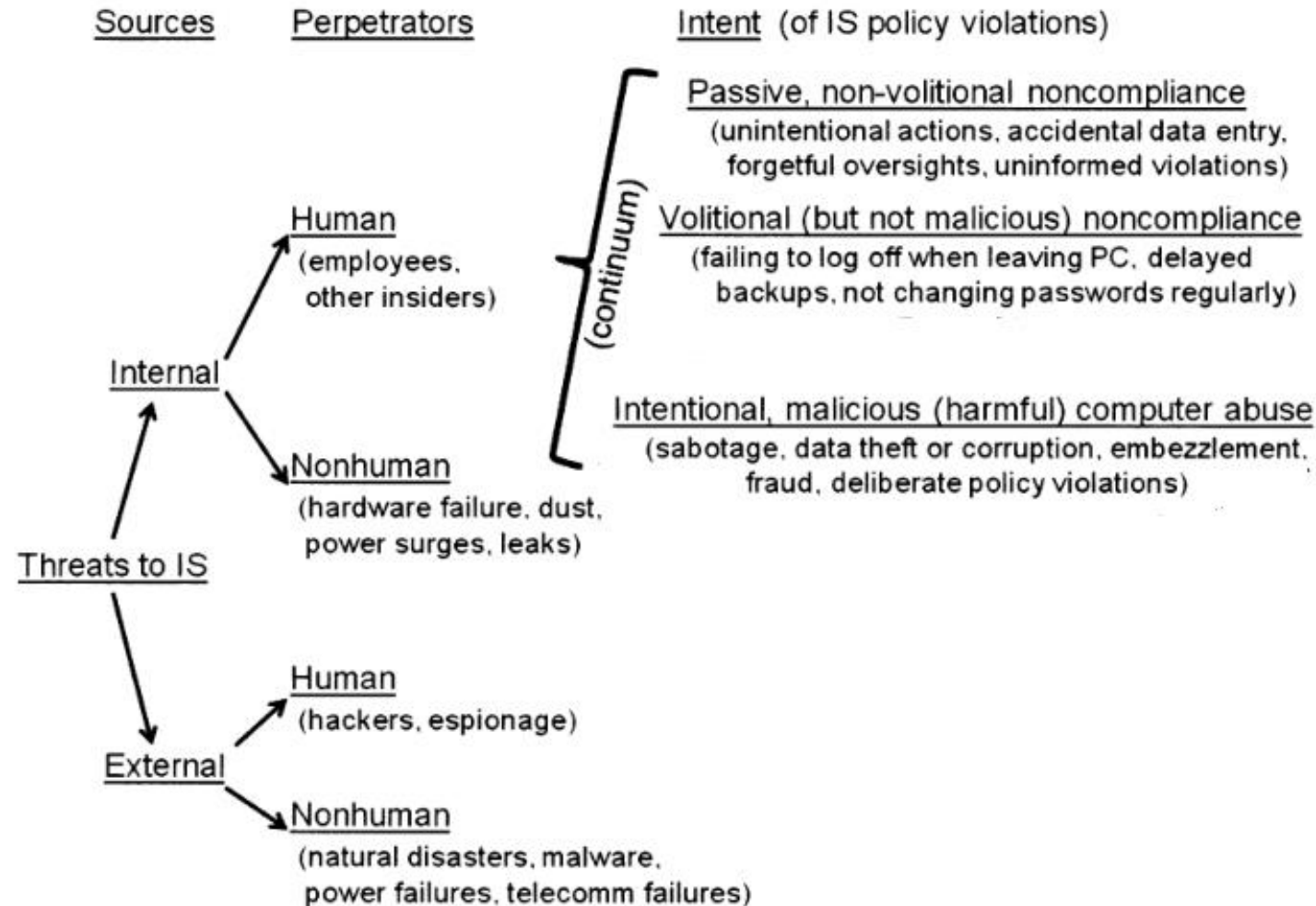


THE UNIVERSITY
OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

Part 2: Security Testing

Threats to Information Security



Security Testing

Before

Data Center Host

Unnecessary services removed
Insecure services removed
System and service are patched
Antivirus / IDS installed
Least privilege on files

Vulnerable service
added to host

After

Data Center Host

Unnecessary services removed
Insecure services removed
System and service needs patch
Antivirus / IDS installed
Least privilege on files

Scans

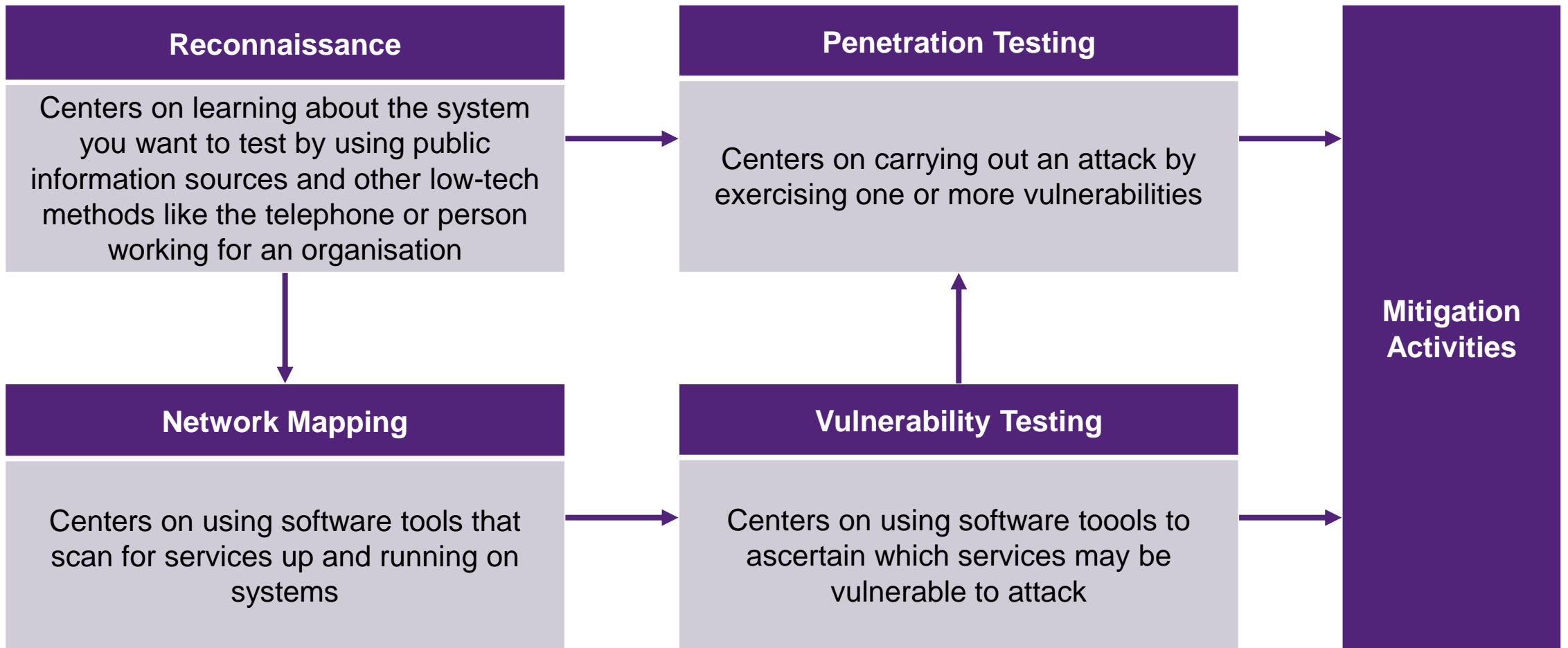
Results

Scan Host

Found 1 unpatched service

The main purpose of any security test is to identify uncorrected vulnerabilities on a system.

Security Testing Road Map



Establishing Testing Goals and Reconnaissance Methods

- **Establish testing goals**
 - Identify vulnerabilities and rank them according to how critical they are to your systems
 - Document a point-in-time (snapshot) test for comparison to other time periods
 - Prepare for auditor review
 - Find the gaps in your security
- **Reconnaissance methods**
 - Social engineering
 - Whois service
 - Zone transfer

Whois Record for UQ

<https://www.whois.com/whois/uq.edu.au>

uq.edu.au

Updated 1 second ago ↻



Domain Information

| | |
|---------------|--|
| Domain: | uq.edu.au |
| Registrar: | Education Services Australia Limited |
| Updated On: | 2024-06-07 |
| Status: | serverRenewProhibited |
| Name Servers: | ns1.dc.uq.edu.au ns2.dc.uq.edu.au ns3.dc.uq.edu.au ns4.dc.uq.edu.au |



Registrant Contact

| | |
|---------------|------------------------------|
| Name: | Director ITS |
| Organization: | The University of Queensland |



Technical Contact

| | |
|-------|-----------|
| Name: | DNS Admin |
|-------|-----------|

Raw Whois Data

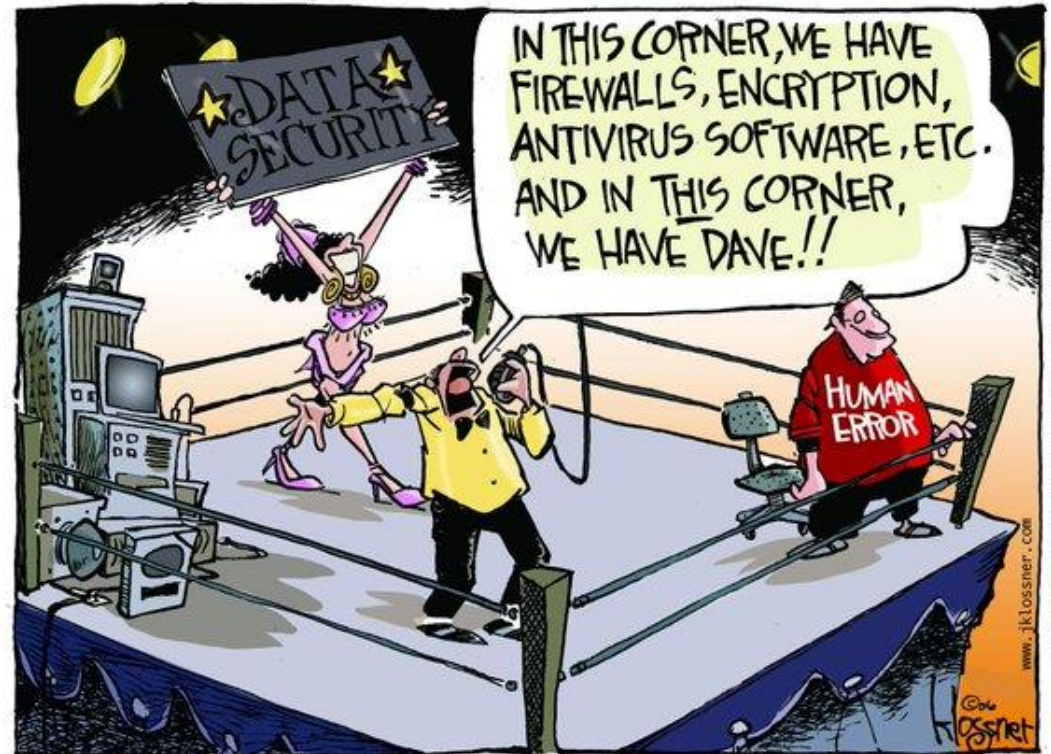
```
Domain Name: uq.edu.au
Registry Domain ID: 6ffc270284f4405aa93314bc3e013efe-AU
Registrar WHOIS Server: https://whois.auda.org.au
Registrar URL: https://www.domainname.edu.au
Last Modified: 2024-06-07T00:18:08Z
Registrar Name: Education Services Australia Limited
Registrar Abuse Contact Email: registrar@esa.edu.au
Registrar Abuse Contact Phone: +61.399109829
Reseller Name:
Status: serverRenewProhibited https://identitydigital.au/get-au/whois-status-codes#serverRenewPro
Status Reason: Not Currently Eligible For Renewal
Registrant Contact ID: 7262c9573d154bbb59ae7866d8d1450-AU
```

Reconnaissance method: Social engineering


95%

"95% of all attacks on enterprise networks are the result of successful spear phishing"

Source: Allan Paller, Director of Research - SANS Institute



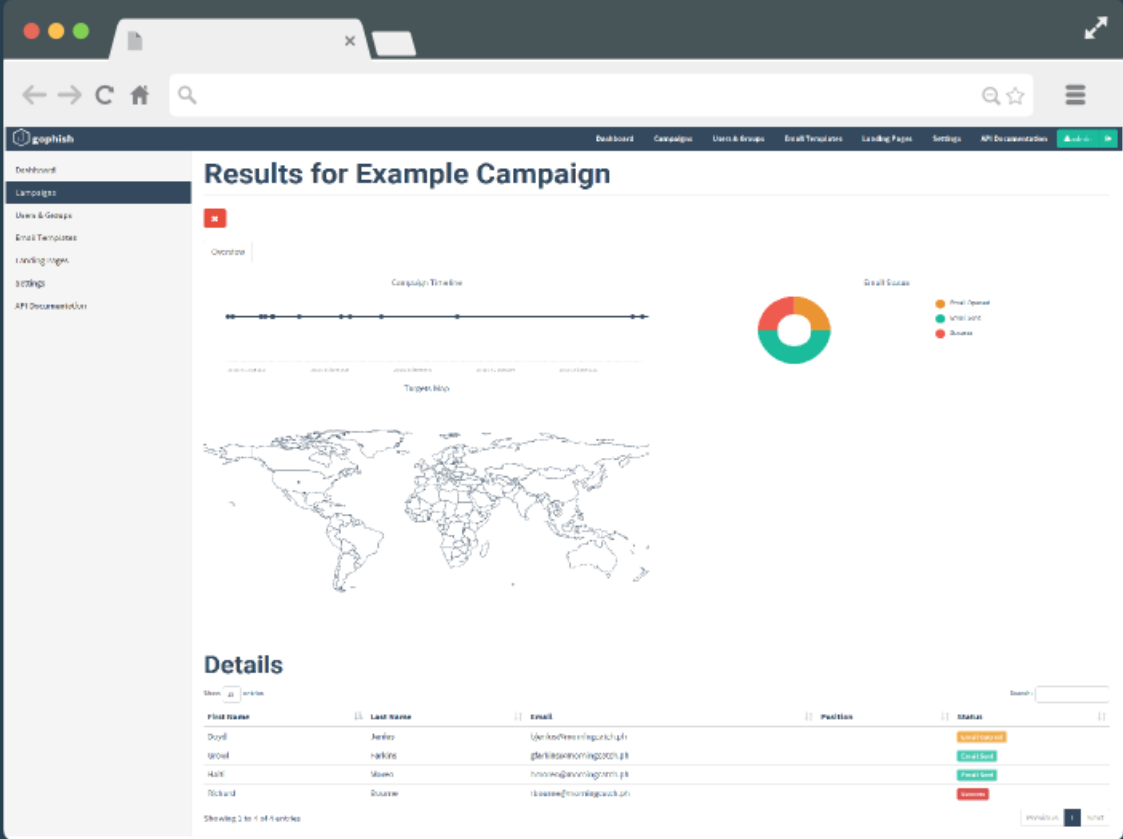
Reconnaissance method: Social engineering



gophish

Open-Source Phishing Framework

[Learn more](#)
[Download](#)



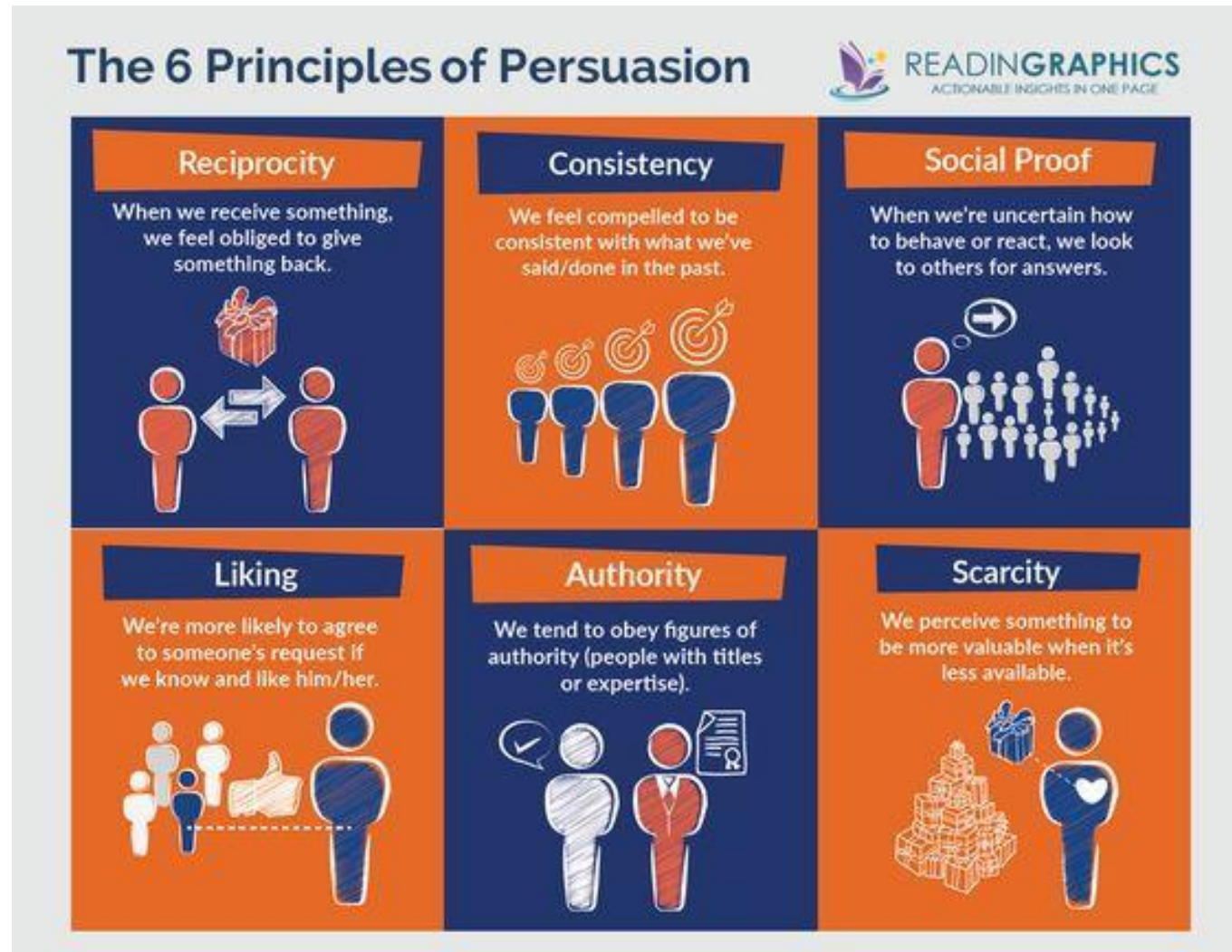
The screenshot shows the Gophish web interface in a browser window. The main heading is "Results for Example Campaign". Below this, there's a "Campaign Timeline" section with a progress bar. To the right is a "Geographical Distribution" donut chart. Below the timeline is a "Target Map" showing a world map. At the bottom, there's a "Details" section with a table of targets.

| First Name | Last Name | Email | Position | Status |
|------------|-----------|------------------------------|----------------------|-----------|
| Dylan | Archer | dylan@archerphishingkit.com | Software Engineer | Completed |
| David | Harris | david@harrisphishingkit.com | Product Manager | Completed |
| Mark | Waters | mark@watersphishingkit.com | Marketing Director | Completed |
| Richard | Quinn | richard@quinnphishingkit.com | Business Development | Completed |

Reconnaissance method: Social engineering

| Table 2. Sources of Adversary Information in a Reconnaissance Campaign | |
|--|--|
| Media Source | Description and Example |
| Personal Social Media | <p>Employees' personal social media are a rich source of information for phishing reconnaissance. Consider the following hypothetical example of simple information triangulation of an individual based on personal social media:</p> <ul style="list-style-type: none"> • John graduated from [University A] and is an athletic supporter – Information gathered from professional networking profile and social media account. • John works at [Company B] – Information gathered from professional networking profile. • John banks at [Bank C] – Information inferred from "liking" or "following" a local bank on social media. • John's banker is [Local Banker D] – Information inferred from "friending" or "following" a local banker on social media. • John uses [Credit Card Company E] – information inferred from a comment about company's service on social media. |
| Organizational Website | <p>Organizational websites are another rich source of information for phishing reconnaissance. Consider the following hypothetical example of simple information triangulation of an individual based on information on an organization's website:</p> <ul style="list-style-type: none"> • Jenny's job title is [Job Title A]. – Information available on company website. • Jenny oversees [Department B] and reports to [Executive C] – Information available on organizational structure chart. • Jenny's previous projects include [Project D] – Information inferred from the "testimonial" section of the website. • Jenny has a relationship with [Supplier E] – Information inferred from list of "corporate partners." |

Reconnaissance method: Social engineering



Which Influence Technique Was Used?

Dear Student,

UQ has now launched its new beta web portal called my.UQ

Please go to [my.UQ](#) and login to activate your new account. You can also access your account directly by going to <https://portal2.my.uq.edu.au>.

You may have to copy and paste the URL into your web browser.

For all the hard work we put into keep your UQ systems working, please return the favor and verify your login for the new beta site.

Jason Benneth

UQ Administrator

[my.UQ](#)

(07) 0113 1271

Influence Techniques

Liking

Reciprocity

Social Proof

Consistency

Authority

Scarcity



Which Influence Technique Was Used?

Dear Student,

UQ has now launched its new beta web portal called my.UQ

Please go to [my.UQ](#) and login to activate your new account. You can also access your account directly by going to <https://portal2.my.uq.edu.au>.

You may have to copy and paste the URL into your web browser.

**We currently have over 85% participation in the beta web portal.
Log on today to be part of this launch with the goal of 100% participation**

Jason Benneth

UQ Administrator

[my.UQ](#)

(07) 0113 1271

Influence Techniques

Liking

Reciprocity

Social Proof

Consistency

Authority

Scarcity



Which Influence Technique Was Used?

Dear Student,

UQ has now launched its new beta web portal called my.UQ

Please go to [my.UQ](#) and login to activate your new account. You can also access your account directly by going to <https://portal2.my.uq.edu.au>.

You may have to copy and paste the URL into your web browser.

If you don't login within the next 48 hours, you will lose access to UQ's web services such as email.

Jason Benneth

UQ Administrator

[my.UQ](#)

(07) 0113 1271

Influence Techniques

Liking

Reciprocity

Social Proof

Consistency

Authority

Scarcity



Which Influence Technique Was Used?

Dear Student,

UQ has now launched its new beta web portal called my.UQ

Please go to [my.UQ](#) and login to activate your new account. You can also access your account directly by going to <https://portal2.my.uq.edu.au>.

You may have to copy and paste the URL into your web browser.

Professor Deborah Terry, UQ Vice-Chancellor and President, hopes to have full participation in this new system this week. Please logon accordingly.

Jason Benneth

UQ Administrator

[my.UQ](#)

(07) 0113 1271

Influence Techniques

Liking

Reciprocity

Social Proof

Consistency

Authority

Scarcity



Which Influence Technique Was Used?

Dear Student,

UQ has now launched its new beta web portal called my.UQ

Please go to [my.UQ](#) and login to activate your new account. You can also access your account directly by going to <https://portal2.my.uq.edu.au>.

You may have to copy and paste the URL into your web browser.

**In using the email and UQ systems, you agreed to keep
confidentials up to date. Please log in to setup your account in the
end system.**

Jason Benneth

UQ Administrator

[my.UQ](#)

(07) 0113 1271

Influence Techniques

Liking

Reciprocity

Social Proof

Consistency

Authority

Scarcity



Which Influence Technique Was Used?

Dear Student,

UQ has now launched its new beta web portal called my.UQ

Please go to [my.UQ](#) and login to activate your new account. You can also access your account directly by going to <https://portal2.my.uq.edu.au>.

You may have to copy and paste the URL into your web browser.

This is an opportunity to help the university by logging into the new system. Your participation will be very much appreciated. Go UQ!

Jason Benneth

UQ Administrator

[my.UQ](#)

(07) 0113 1271

Influence Techniques

Liking

Reciprocity

Social Proof

Consistency

Authority

Scarcity



Testing Methods

Black-box testing

- Uses test methods that aren't based directly on knowledge of a program's architecture or design

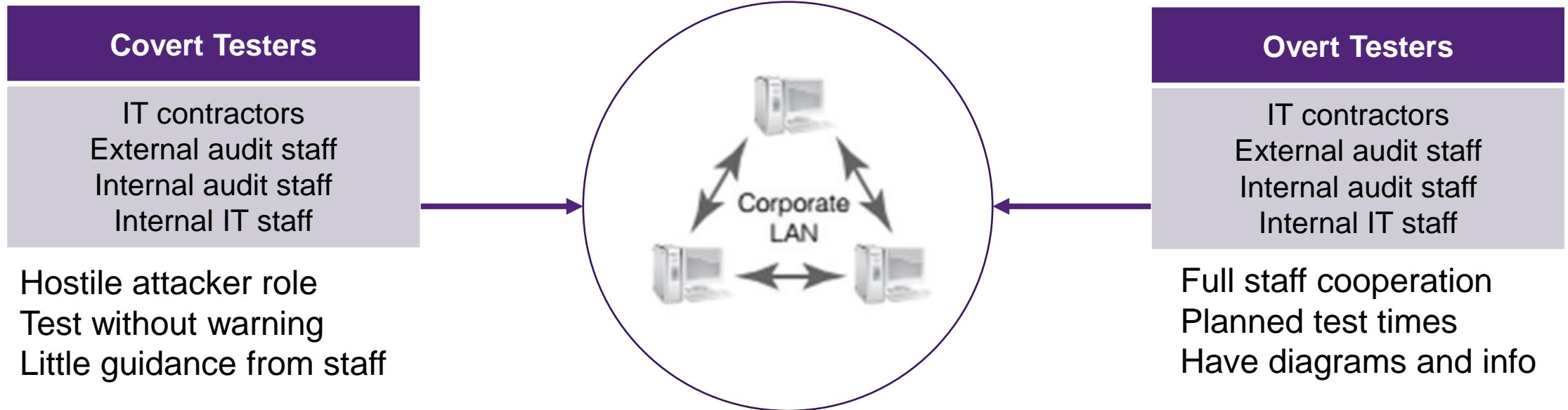
White-box testing

- Is based on knowledge of the application's design and source code

Grey-box testing

- Lies somewhere between black-box testing and white-box testing

Covert vs. Overt Testers



Netsparker Pentest Software (for web applications)

The screenshot displays the Netsparker 4.6.1.11314 interface. The main window shows a vulnerability report titled "Cross-site Scripting Protection Disabled" with an "IMPORTANT" flag. The report details the URL `http://aspnet.testsparker.com/Generics/` and the header `X-XSS-Protection: 0`. It explains that Netsparker detected that cross-site scripting protection is disabled and provides instructions on how to disable Internet Explorer's built-in protection using the `X-XSS-Protection: 0` header.

The "ACTIONS TO TAKE" section suggests "Again BOB, fix this!". The "REMEDY" section provides the command: "Add the X-XSS-Protection header with a value of '1; mode= block'." Below this, a code block shows the remediation: `X-XSS-Protection: 1; mode=block`.

The left sidebar contains a "Site Map" with various endpoints like `ConverterResponse.aspx`, `WS_search.aspx`, and `GuestbookList.aspx`. It also includes a "Knowledge Base" section with links to "Scan Performance", "Out of Scope Links", "Crawling Performance", "Web Pages With Inputs", "MIME Types", "External Scripts", "Cookies", "Comments", "Slowest Pages", "File Extensions", and "JavaScript Files".

The bottom section shows a list of "Issues (64)" including "Boolean Based SQL Injection", "Blind SQL Injection", "SQL Injection", "Cross-site Scripting", "Permanent Cross-site Scripting", "Local File Inclusion", and "Database User Has Admin Privileges". A red line highlights the "Database User Has Admin Privileges" issue.

The interface also features a "Vulnerability" sidebar on the right with options like "Scan", "Request Builder", and "Vulnerability". The bottom status bar shows "Issues (64)", "Encoder", and "Logs (27)".

40

Security Metrics (measuring performance)

| Metrics |
|--|
| Performance and Conformance |
| <ul style="list-style-type: none">• Percentage of business processes that meet defined security requirements• Percentage of security practices that satisfy internal compliance requirements |
| System of Internal Control |
| <ul style="list-style-type: none">• Percentage of processes that satisfy security control requirements• Percentage of controls in which security control requirements are met• Percentage of security controls appropriately monitored and results reported and reviewed |
| Compliance with External Requirements |
| <ul style="list-style-type: none">• Percentage of security practices that satisfy external compliance requirements• Number or percentage of projects initiated by security to implement new external requirements |

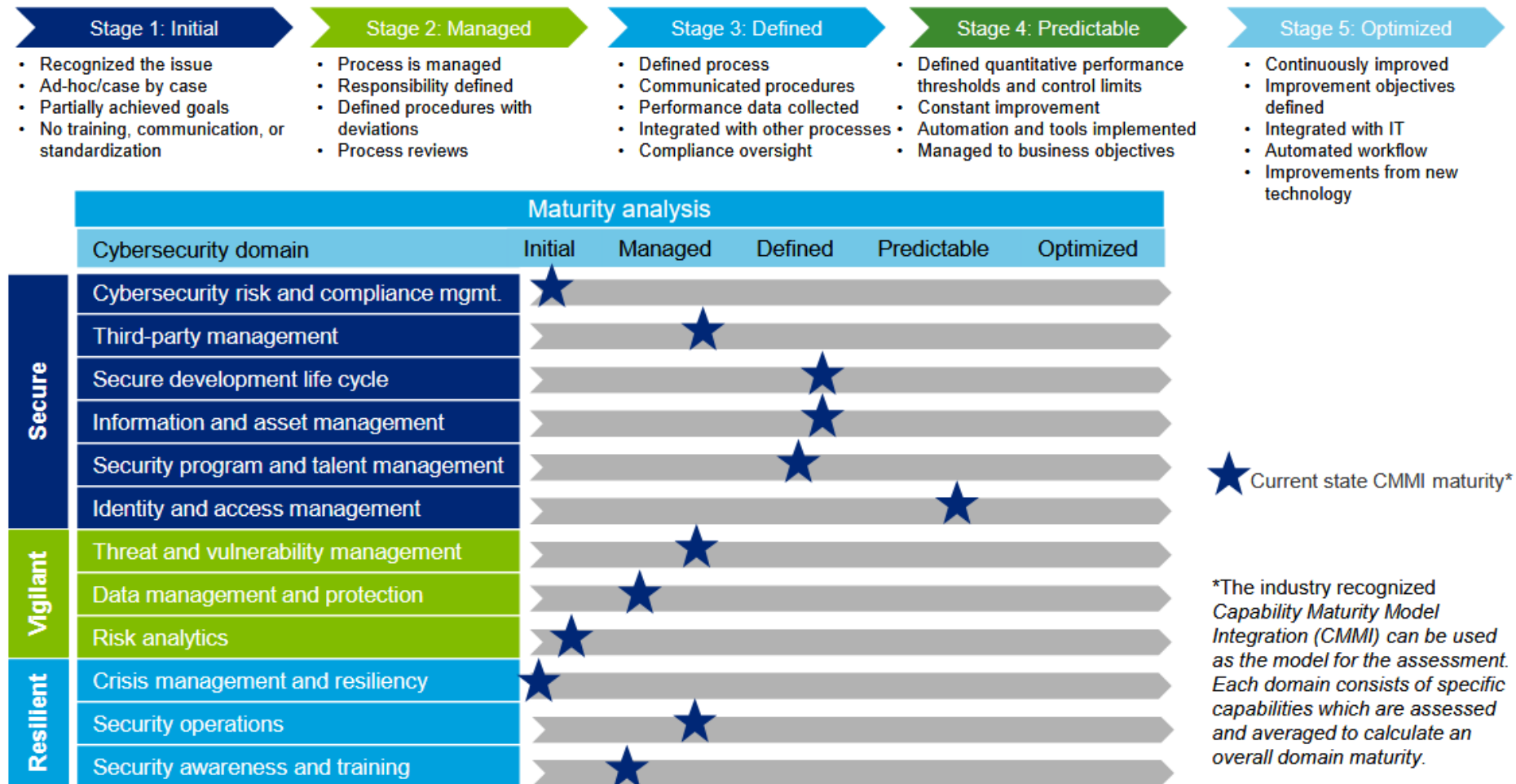
Examples of Security Performance Metrics

- Percentage (%) of system users/security personnel that have received basic awareness training
- Average frequency of audit records review and analyses for inappropriate activity
- Percentage of systems using automated mechanisms to conduct analysis and reporting of inappropriate activities
- Percentage (%) of systems that are compliant with the baseline configuration
- Percentage (%) of systems successfully addressed in the testing of the contingency plan
- Percentage of accounts not associated with specific users
- Percentage (%) of system components that undergo maintenance on schedule
- Cost of information security incidents of unauthorized access to information systems, due to physical security failures
- Percentage (%) of employees who signed acknowledgement that they have read and understood rules of behavior, before being authorized access to the information system
- ...

Example: Deloitte's Cyber Risk Assessment Approach

| Phase | Phase I: Planning and scoping | Phase II: Understand current state | Phase III: Risk assessment | Phase IV: Gap assessment and recommendations |
|----------------|---|---|---|--|
| Key activities | Activities: <ul style="list-style-type: none"> Identify specific internal and external stakeholders: IT, Compliance, Legal, Risk, etc. Understand organization mission and objectives Identify industry requirements and regulatory landscape Perform industry and sector risk profiling (i.e., review industry reports, news, trends, risk vectors) Identify in-scope systems and assets Identify vendors and third-party involvement | Activities: <ul style="list-style-type: none"> Conduct interviews and workshops to understand the current profile Perform walkthroughs of in-scope systems and processes to understand existing controls Understand the use of third-parties, including reviews of applicable reports Review relevant policies and procedures, including security environment, strategic plans, and governance for both internal and external stakeholders Review self assessments Review prior audits | Activities: <ul style="list-style-type: none"> Document list of potential risks across all in-scope capabilities Collaborate with subject matter specialists and management to stratify emerging risks, and document potential impact Evaluate likelihood and impact of risks Prioritize risks based upon organization's objectives, capabilities, and risk appetite Review and validate the risk assessment results with management and identify criticality | Activities: <ul style="list-style-type: none"> Document capability assessment results and develop assessment scorecard Review assessment results with specific stakeholders Identify gaps and evaluate potential severity Map to maturity analysis Document recommendations Develop multiyear cybersecurity/IT audit plan |
| Deliverables | Deliverable: <ul style="list-style-type: none"> Assessment objectives and scope Capability assessment scorecard framework | Deliverable: <ul style="list-style-type: none"> Understanding of environment and current state | Deliverable: <ul style="list-style-type: none"> Prioritized risk ranking Capability assessment findings | Deliverables: <ul style="list-style-type: none"> Maturity analysis Assessment scorecard Remediation recommendations Cybersecurity audit plan |

Example: Deloitte's Cyber Risk Assessment Maturity Analysis



Example: Deloitte's Cyber Risk Assessment Scorecard

| Assessment Scorecard | | | | |
|----------------------|---|--------|---------|------------|
| Cybersecurity domain | | People | Process | Technology |
| Secure | Cybersecurity risk and compliance mgmt. | | | |
| | Third-party management | | | |
| | Secure development life cycle | | | |
| | Information and asset management | | | |
| | Security program and talent management | | | |
| | Identity and access management | | | |
| Vigilant | Threat and vulnerability management | 4 | 2 | 1 |
| | Data management and protection | | | |
| | Risk analytics | | | |
| Resilient | Crisis management and resiliency | | | |
| | Security operations | | | |
| | Security awareness and training | | | |

| Threat and vulnerability management—Penetration testing | | | | |
|---|--|-------|--|-------|
| Area | Findings | Ref. | Recommendations | Ref. |
| People | <ul style="list-style-type: none"> The organization has some resources within the ISOC that can conduct penetration testing, but not on a routine basis due to operational constraints and multiple roles that those resources are fulfilling | 2.6.4 | <ul style="list-style-type: none"> The organization may find it of more value and cost benefit to utilize current resources to conduct internal penetration testing on a routine and dedicated basis since they do have individuals with the necessary skills to perform this duty. | 2.6.4 |
| Process | <ul style="list-style-type: none"> The organization has limited capability to conduct penetration testing in a staged environment or against new and emerging threats | 2.6.5 | <ul style="list-style-type: none"> The organization should expand its penetration testing capability to include more advance testing, more advanced social engineering, and develop greater control over the frequency of testing | 2.6.5 |
| Technology | <ul style="list-style-type: none"> The organization lacks standard tools to perform its own ad-hoc and on-the-spot penetration tests to confirm or support potential vulnerability assessment alerts and/or incident investigation findings. | 2.6.6 | <ul style="list-style-type: none"> Either through agreement with a third-party vendor, or through technology acquisition, develop the technology capability to perform out of cycle penetration testing. | 2.6.6 |

| | | | | |
|------------|------------|------------|----------------|--------------|
| 1: Initial | 2: Managed | 3: Defined | 4: Predictable | 5: Optimized |
|------------|------------|------------|----------------|--------------|

Capability assessment findings and recommendations

Wireshark Demo

Wireshark intro

Malware traffic Analysis with Wireshark, part 1 (4:53m)

<https://www.youtube.com/watch?v=4CbgDFYF9A0>

Malware traffic Analysis with Wireshark, part 2 (13:19m)

https://www.youtube.com/watch?v=T_41vAOHfZ4

Alternatively use the Bb “tutorial slides” for a more extensive explanation and demo...



```
end;
func, std::vector<int>

write(Endtext);
end.
CREATE TABLE product(
class MultinomialNB(object):
def __init__(self):
2))
self.X = None
self.y = None
def __loading(self):
self.list_labels = cl.Counter(s
int acc(std::function<int(int, int)> fun
auto it = operands.begin();
int result = func(*it, *(++it));
if (operands.size() > 2) {
for (++it; it!=operands.end(); ++it)
result = func(result, *it);
}
}
return result;
CDog& operator=(C
```

Thank you