Oxford Risk | Behavioural finance. Applied.

Data Security Implementation and Compliance Summary

Version: 1.1

Date: 14/07/2021

Distribution: Internal and External

Classification: Restricted

Registered in England No. 4571309

Date	Version	Changes Incorporated
14/07/2021	1.0	Original Version
20/07/2021	1.1	Added Release Management and Testing

Purpose

An overview of Oxford Risk's security implementation and compliance with IT security policies, standards, and procedures.

Reference

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-12, NIST 800-46, NIST SP 800-48, NIST SP 800-77, NIST SP 800-94, NIST SP 800-97, NIST SP 800-100, NIST SP 800-113, NIST SP 800-114, NIST SP 800-121, NIST SP 800-124, NIST SP 800-164;

Access Control

Reference

NIST SP 800-53a – Access Control (AC),

Summary

1. Oxford Risk employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
2. Oxford Risk Information Owner's authorize explicitly access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.
3. Systems require that users of information system accounts, or roles, with access to administration, security functions or security-relevant information, use non-privileged accounts or roles, when accessing non-security functions. The information system audits the execution of privileged functions
4. Access to production systems is only provisioned temporarily through an exception process/break-glass procedures to the required personnel.
5. Entitlements for accounts with access to production systems are reviewed at a quarterly cadence.
6. Entitlements for Entitlement Administrators, Elevated Access, and Enhanced Entitlements are reviewed quarterly for each applicable individual.
7. Segregation of duties for users who have administrative access, access approval and post access action review is maintained.
8. Restriction of privileged accounts on the information system is implemented by technical operations Role on authorisation of Information Owner.
9. Information systems prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Account Management/Access Control Roles

Information Owner: Information owners are people at the managerial level within an entity who:

1. Delegate account managers to ensure the appropriate level of information access is provided. Delegation can be to individual users, groups and/or third parties (e.g., another entity).
2. Define roles and groups, as well as the corresponding level of access to resources for that role or group.
3. Determining who should have access.
4. Determine the identity assurance level for the application and/or data.

5. Review that accounts and access controls are commensurate with overall business function and that the associated rights have been properly assigned, at a minimum, annually.
6. Require business units with access to protected resources to notify account managers when accounts are no longer required, such as when users are terminated or transferred and when individual access requirements change.

Information Owners: CTO

Account Manager: Account managers maintain accounts. They are the delegated custodians of protected data. Account managers:

1. Maintain appropriate levels of communication with the information owners to determine the level or degree of access granted to an individual.
2. Determine the technical specifications needed to set access privileges.
3. Delegate account management functions to account administrators.
4. Create and maintain procedures used in managing accounts.
5. Perform all account administrator duties as required.

Account Managers: Technical Operations

Account Administrators may:

1. Maintain any necessary information supporting account administration activities, including account management requests and approvals.
2. Enroll new users.
3. Enable/disable user accounts.
4. Create and maintain user roles and groups.
5. Assign rights and privileges to a user or group.
6. Collect data to periodically review user accounts and their associated rights.
7. Assign new authentication tokens (e.g., password resets).
8. Entitlement Administrator: Entitlement administrators are an optional subset of the account manager role. Rights and/or responsibilities are assigned to them by the information owner and generally include:
9. Assign rights and privileges to a user or group.
10. Collect data to periodically review user accounts and their associated rights.
11. Maintain any necessary information supporting account administration activities including account management requests and approvals.

Account Administrators: Technical Operations

Identification and Authentication

Reference

NIST SP 800-53a – Identification and Authentication (IA)

Summary

Oxford Risk shall:

1. Ensure that information systems uniquely identify and authenticate users or processes acting on behalf of users.
2. Ensure that information systems implement multifactor authentication for network access to privileged accounts.
3. Ensure that information systems implement multifactor authentication for network access to non-privileged accounts. Except where authentication is from a tokenised link from email or SMS.
4. Ensure that information systems implement multifactor authentication for local access to privileged accounts.
5. *Ensure that information systems implement replay-resistant authentication mechanisms for network access to privileged accounts using CSRF tokens*
6. Ensure that information systems implement multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device utilizes a cryptographic strength mechanisms that protects the primary authentication token (secret key, private key or one-time password) against compromise by protocol threats including: eavesdropper, replay, online guessing, verifier impersonation and man-in-the-middle attacks.

Oxford Risk shall:

1. Manage information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.
2. Establish initial authenticator content for authenticators defined by the organization.
3. Ensure that authenticators have sufficient strength of mechanism for their intended use.
4. Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
5. Change default content of authenticators prior to information system installation.
6. Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators.
7. Change/refresh authenticators every 90 days.

8. Protect authenticator content from unauthorized disclosure and modification.
9. Require individuals and devices to implement specific security safeguards to protect authenticators.
10. Change authenticators for group/role accounts when membership to those account changes.
11. Ensure that information systems, for password-based authentication enforce minimum password complexity that must not contain the user's entire Account Name value or entire Full Name value
12. Ensure passwords must contain characters from three of the following five categories:
    a. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters);
    b. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters);
    c. Base 10 digits (0 through 9);
    d. Non-alphanumeric characters ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/; and
    e. Any Unicode character that is categorized as an alphabetic character, but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
13. Require passwords to have a minimum length of 8 characters.
14. Enforce at least one changed character when new passwords are created.
15. Store and transmit only cryptographically-protected passwords.
16. Enforce password minimum and maximum lifetime restrictions of one day and 120 days respectively.
17. Allow the use of a temporary password for system logons with an immediate change to a permanent password.
18. Ensure that information system, for PKI-based authentication, validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.
19. Enforce authorized access to the corresponding private key.
20. Map the authenticated identity to the account of the individual or group.
21. Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.
22. Ensure that the information system, for hardware token-based authentication, employs mechanisms that satisfy [external entity defined token quality requirements].

Cryptographic Module Authentication

Reference

NIST Special Publication 800-107, Revision 1, Recommendation for Applications Using Approved Hash Algorithms

Summary

Oxford Risk shall:

1. Ensure that information systems implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, directives, policies, regulations, standards, and guidance for such authentication.

Incident Response

Summary

Incident Response Training

Oxford Risk shall:

- Provide incident response training to information system users consistent with assigned roles and responsibilities:
- Within [entity defined time period] of assuming an incident response role or responsibility.
- When required by information system changes, and [entity defined frequency] thereafter.
- Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.
- Employ automated mechanisms to provide a more thorough and realistic incident response training environment.

Incident Response Testing

Oxford Risk shall:

- Test the incident response capability for the information system to determine the incident response effectiveness and documents the results.
- Coordinate incident response testing with entity contacts responsible for related plans such as Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

Recovery Time Objective and Recovery Point Objective

- In the event of a failure to one availability zone the recovery time objective will be within 5 minutes and the recovery point objective will be within 10 minutes of the failure.
- In the event of a failure to all two or more availability zones the recovery time objective will be within 12 hours and the recovery point objective will be within 24 hours of the failure.

Information Risk Management

a. Systems or process that supports business functions have been appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development life cycle.

b. Information security risk assessments are required for new projects, implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.

c. Entities are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.

d. Risk assessment results, and the decisions made based on these results, has been documented.

Associated Standard: Information Security Risk Management Standard;

Secure System Development Lifecycle (SSDLC) Standard

Information Classification and Handling

a. All information, which is created, acquired or used in support of business activities, will only be used for its intended business purpose.

b. All information assets have an information owner established within the lines of business.

c. Information has been properly managed from its creation, through authorized use, to proper disposal.

d. All information has been classified on an ongoing basis based on its confidentiality, integrity and availability characteristics.

e. An information asset has been classified based on the highest level necessitated by its individual data elements.

f. If the entity is unable to determine the confidentiality classification of information or the information is personal identifying information (PII) the information will have a high confidentiality classification and, therefore, is subject to high confidentiality controls.

g. Merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files)

has been evaluated to determine if a new classification of the merged data is warranted.

h. All reproductions of information in its entirety will carry the same confidentiality classification as the original. Partial reproductions will need to be evaluated to determine if a new classification is warranted.

i. Each classification has an approved set of baseline controls designed to protect these classifications and these controls have been followed.

j. The entity must communicate the requirements for secure handling of information to its workforce.

k. A written or electronic inventory of all information assets is maintained.

l. Content made available to the general public has been reviewed according to a process that will be defined and approved by the entity. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.

m. PPI will not be made available without appropriate safeguards approved by the Oxford Risk.

n. For non-public information to be released outside the entity or shared between other entities, a process have been established that:

    1. evaluates and documents the sensitivity of the information to be released or shared;

    2. identifies the responsibilities of each party for protecting the information;

    3. defines the minimum controls required to transmit and use the information;

    4. records the measures that each party has in place to protect the information;

    5. defines a method for compliance measurement;

    6. provides a signoff procedure for each party to accept responsibilities; and

    7. establishes a schedule and procedure for reviewing the controls.

Associated Standards: Information Classification Standard; Sanitization/Secure Disposal Standard

IT Asset Management

a. All IT hardware and software assets have been assigned to a designated business unit or individual.

b. Entities are required to maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory has been automated where technically feasible.

c. Processes, including regular scanning, has been implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

Associated Standard: Secure Configuration Standard

Personnel Security

a. The workforce has received general security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on specific security procedures, if required, has been completed before access is provided to specific entity sensitive information not covered in the general security training. All security training has been reinforced at least annually and has been tracked by the entity.

b. Oxford Risk has required its workforce to abide by the Acceptable Use of Information Technology Resources Policy, and an auditable process has been in place for users to acknowledge that they agree to abide by the policy's requirements.

c. All job positions have been evaluated by the to determine whether they require access to sensitive information and/or sensitive information technology assets.

d. For those job positions requiring access to sensitive information and sensitive information technology assets, entities must conduct workforce suitability determinations, unless prohibited from doing so by law, regulation or contract. The suitability determination must provide reasonable grounds for the entity to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the entity.

e. HR is responsible for ensuring all issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

Associated Standard: Account Management/Access Control Standard

Cyber Incident Management

a. Oxford Risk have an incident response plan, consistent standards, to effectively respond to security incidents.

b. All observed or suspected information security incidents or weaknesses are reported to appropriate management and the designated security representative as quickly as possible.

Associated Standard: Cyber Incident Response Standard

Physical and Environmental Security

a. Information processing and storage facilities will have a defined security perimeter and appropriate security barriers and access controls.

b. A periodic risk assessment has been performed for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary. These measures have been implemented to mitigate the risks.

c. Information technology equipment has been physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities such as electrical supply and cabling infrastructure.

d. All information technology equipment and information media has been secured to prevent compromise of confidentiality, integrity, or availability in accordance with the classification of information contained therein.

e. Visitors to information processing and storage facilities, including maintenance personnel, has been escorted at all times.

Associated Standard: Information Security Risk Management Standard; Account Management/Access Control Standard; Authentication Tokens Standard; Remote Access Standard; Security Logging Standard

ISO 27001 – Annex A.11: Physical & Environmental Security

Systems Security

Summary

a. Systems include but are not limited to servers, platforms, networks, communications, databases and software applications.

1. An individual or group has been assigned responsibility for maintenance and administration of any system deployed on behalf of the entity. A list of assigned individuals or groups have been centrally maintained.
2. Security has been considered at system inception and documented as part of the decision to create or modify a system.
3. All systems have been developed, maintained and decommissioned in accordance with a secure system development lifecycle (SSDLC).
4. Each system will have a set of controls commensurate with the classification of any data that is stored on or passes through the system.
5. All system clocks must synchronize to a centralized reference time source set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources.
6. Environments and test plans have been established to validate the system works as intended prior to deployment in production.
7. Separation of environments (e.g., development, test, quality assurance, production) is required, either logically or physically, including separate environmental identifications (e.g., desktop background, labels).
8. Formal change control procedures for all systems have been developed, implemented and enforced. At a minimum, any change that may affect the production environment and/or production data has been included.

    a. <u>Databases and Software (including in-house or third party developed and commercial off the shelf (COTS):</u>
        1. All software written for or deployed on systems must incorporate secure coding practices, to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.
        2. Once test data is developed, it has been protected and controlled for the life of the testing in accordance with the classification of the data.
        3. Production data may be used for testing only if a business case is documented and approved in writing by the information owner and the following controls are applied:
            i. All security measures, including but not limited to access controls, system configurations and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed; or
            ii. sensitive data is masked or overwritten with fictional information.

4. Where technically feasible, development software and tools must not be maintained on production systems.
5. Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software.
6. Scripts have been removed from production systems, except those required for the operation and maintenance of the system.
7. Privileged access to production systems by development staff has been restricted.
8. Migration processes have been documented and implemented to govern the transfer of software from the development environment up through the production environment.

b. Network Systems:
   1. Connections between systems have been authorized by the executive management of all relevant entities and protected by the implementation of appropriate controls.
   2. All connections and their configurations have been documented and the documentation has been reviewed by the information owner and the ISO/designated security representative annually, at a minimum, to assure:
      i. the business case for the connection is still valid and the connection is still required; and
      ii. the security controls in place (filters, rules, access control lists, etc.) are appropriate and functioning correctly.
   3. A network architecture has been maintained that includes, at a minimum, tiered network segmentation between:
      i. Internet accessible systems and internal systems;
      ii. systems with high security categorizations (e.g., mission critical, systems containing PII) and other systems; and
      iii. user and server segments.
   4. Network management has been performed from a secure, dedicated network.
   5. Authentication is required for all users connecting to internal systems.
   6. Network authentication is required for all devices connecting to internal networks.
   7. Only authorized individuals or business units may capture or monitor network traffic.
   8. A risk assessment has been performed in consultation with the designated security representative before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.

Associated Standards: Secure System Development Lifecycle Standard; Secure Coding Standard; Security Logging Standard; Secure Configuration Management Standard

Release Management

The purpose of this document is to describe the process of releasing new versions of the application software, patching the virtual machine instances' operating systems, checking and load balancing instances based on their health, with no scheduled downtime. A many colour version of blue-green deployment.

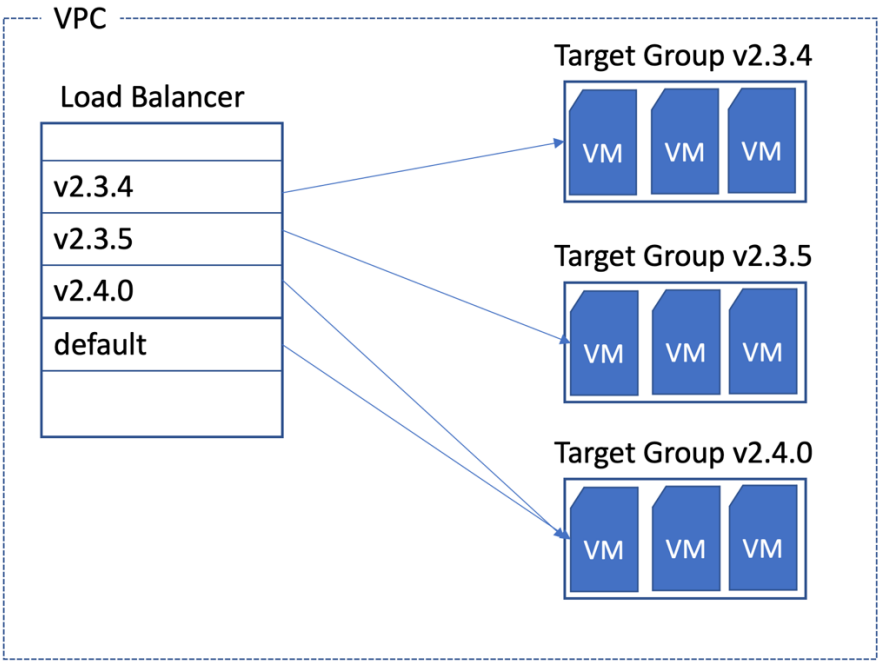
Routing traffic by release version

The diagram below shows the production environment with different versions of the software running. A request to the load balancer with a version header included will allow the request to be routed to a specific version of the application.

e.g.

```
curl --location --request POST 'https://{api_url}' \
--header 'Content-Type: application/json' \
--header 'x-version: refs-tags-v2.3.4'
```

If no version header is included the request will be routed to the default version of the application.



Target Groups

A target group will consist of **at least** 2 virtual machine instances running the same code release on the same version operating system, but on **separate** availability zones.

Target groups will check health of running virtual machine instances at least every 30 seconds and route traffic accordingly.

If a virtual machine in the target group is found unhealthy twice traffic to that virtual machine will be sent to a healthy virtual machine instance in the same target group and an alert will be sent to OR technical operations and the error will be logged in cloud watch.

A new instance will be built automatically to take the place of the unhealthy virtual machine instance. Once a new healthy instance is running, the unhealthy instance can be manually examined and removed.

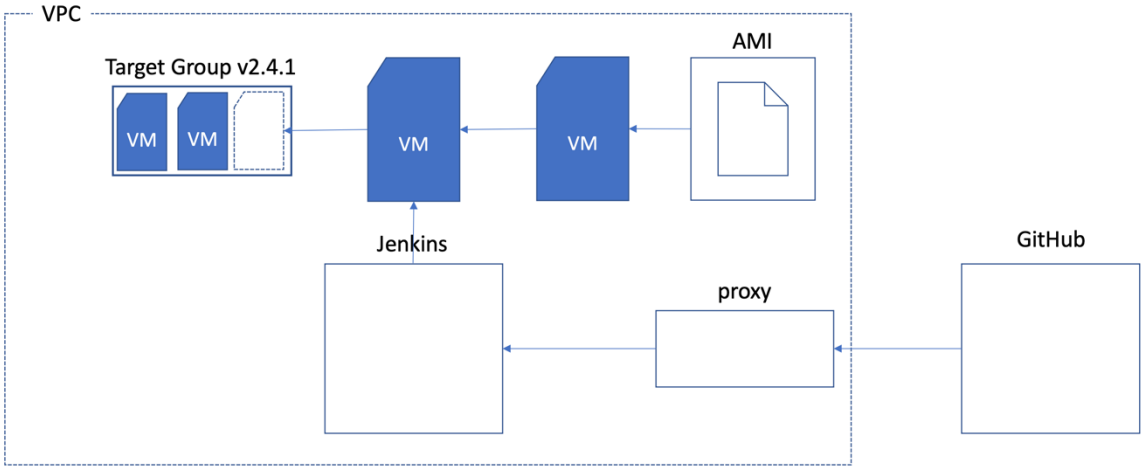
The unhealth virtual machine will be retested every 30 seconds by the target group.

Creation of new releases

This process is automated with Jenkins automation server, Terraform and AWS APIs.

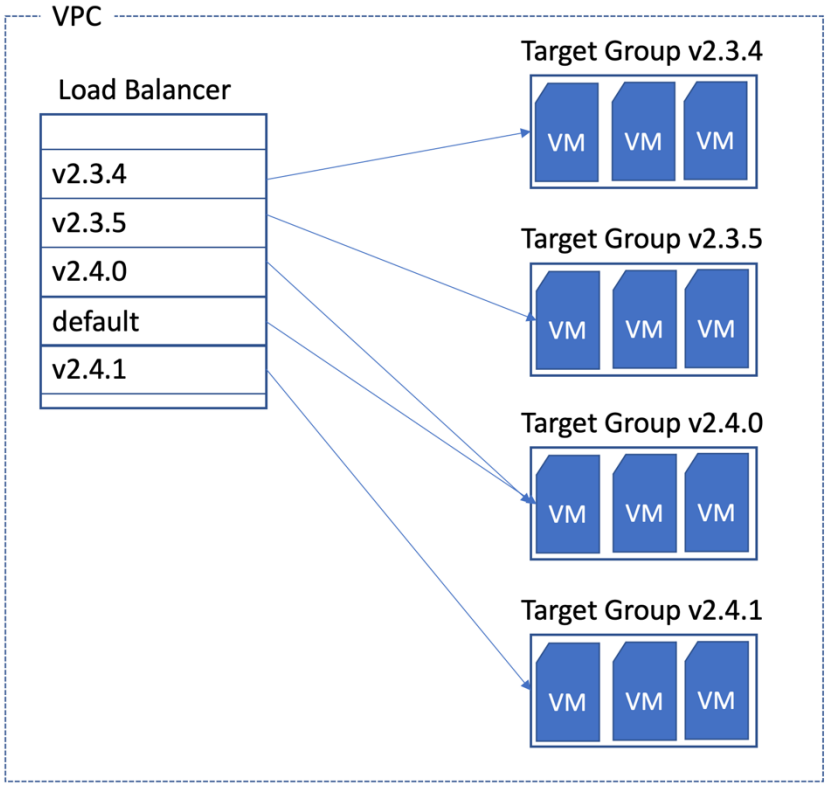
Each virtual machine in the target group will be created from the same AMI (amazon machine image). If there is a patch to the operating system a new AMI will be created and the process will be treated in the same way as a new application release version.

The AMI template will be used to launch at least 2 virtual machine instances. Once the instances are running, Jenkins automation server will build the codebase from GitHub and SCP the build onto the virtual machine instance.
Jenkins will only have access to the `/home/builds` directory of the virtual machine instance and will only have ability to start nginx and start php-fpm, as described in the visudo file.



On successful creation of the instances, the target group will be created with the following naming convention target-{API_name}-v{version_number}.
e.g.
target-live-doc-gen-v2-4-1
target-live-survey-v2-4-1

On successful creation of the target group, the virtual machine instances will be added to target group and a new rule will be added to the load balancer.

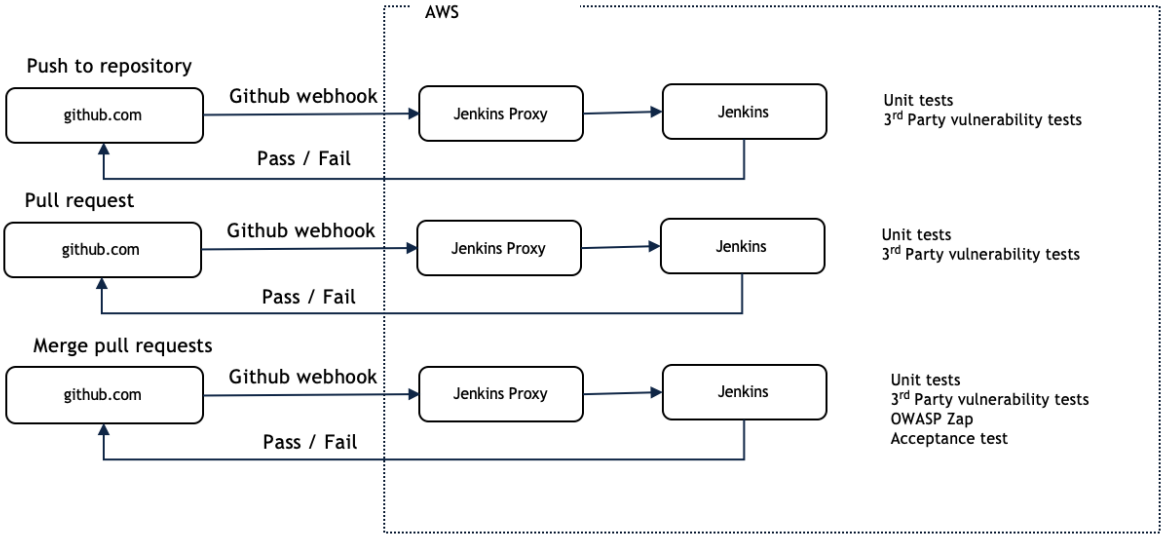


The new code release can be called using the version header e.g.

```
curl --location --request POST 'https://{api_url}' \
--header 'Content-Type: application/json' \
--header 'x-version: refs-tags-v2.4.1'
```

Testing / Continuous integration

Summary



- Developers code and test their applications in Docker, which also mirrors the production infrastructure and communication between services.
- Developers will write acceptance tests and unit tests as they code (TDD). Git hooks are set up to run all unit tests in the docker environment before committing to a repositor.
- Once committed, a GitHub webhook will trigger more testing and verification of the build which is sent back to GitHub to be displayed next to the commit, this testing occurs in the Jenkins automation server.
- Acceptance tests using mocked API calls are also run on the Jenkins system.
- OWASP zap tests are run on the UAT infrastructure.
- Manual testing is performed by the QA department.
- Third party dependencies are installed via composer dependency manager on the Jenkins box, tested for with OWASP Dependency Check and then built.

The SLA covering production architecture are as follows

Target resolution times

Priority	Urgency	Impact Description	Target Response Time	Target Resolution Time
P1	Urgent	Failure of any IT services that will have an immediate and severe impact on business operations in terms of political / financial / corporate image or accreditation status	1 hour	Less than 4 hours
P2	High	Failure of a major business application or the loss of all IT services to a large numbers of Users causing significant impact to the business and its political, financial or corporate image	2 hours	Less than 1 business day
P3	Medium	Failure that is limited in scope in terms of the number of Users affected or its impact to the on-going business. Some form of temporary operational workaround may also be available.	6 hours	Less than 3 business days
P4	Low	Failure for a single or small of group of Users where they can still continue working with some limited inconvenience and have a suitable temporary workaround. No immediate impact to the business or its political, financial or corporate image.	1 business day	Less than 5 business days
P5	Very Low	Customer's confidence in the information being displayed	2 business days	Less than 20 business days

Target availability metrics

Availability %	Downtime per year	Downtime per month*	Downtime per week
99.9%	8.76 hours / 525.6 minutes	43.2 minutes	10.1 minutes

n.b current availability in the past year has been 100%.