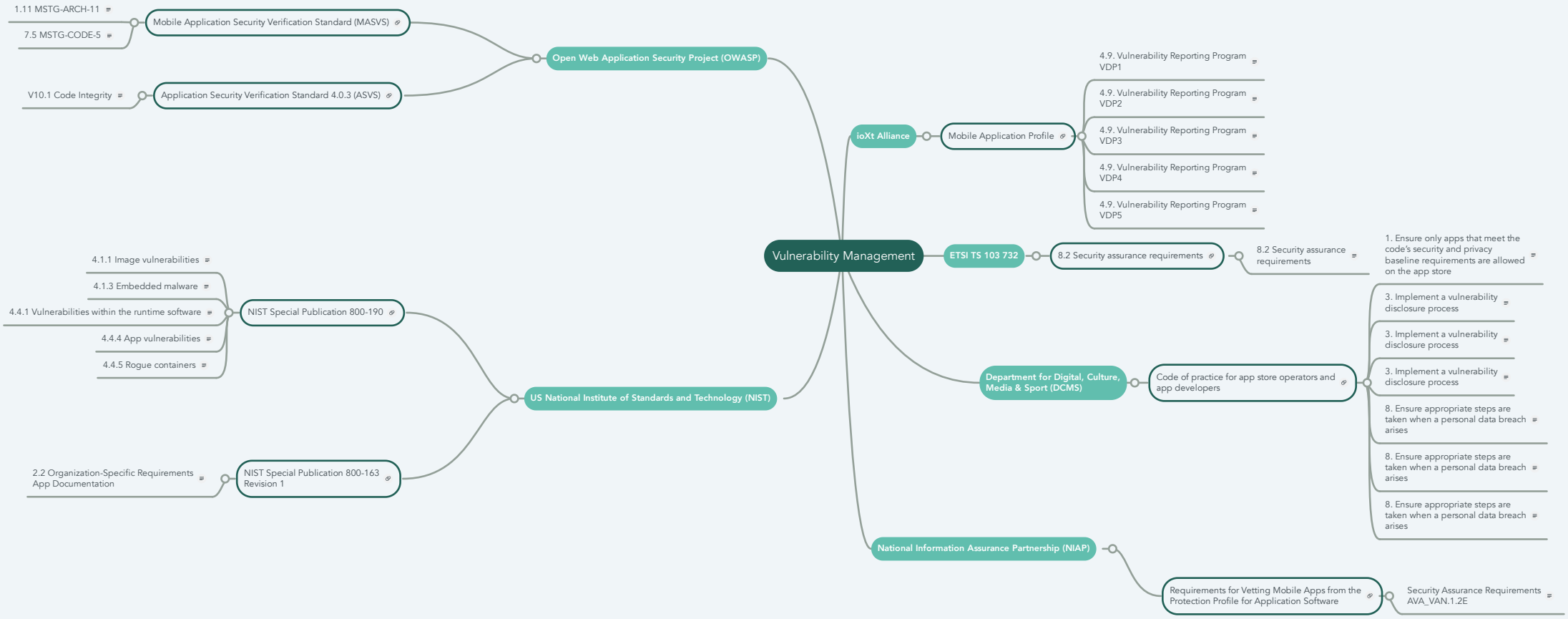
Vulnerability Management
Open Web Application Security Project (OWASP)
Mobile Application Security Verification Standard (MASVS)
1.11 MSTG-ARCH-11
7.5 MSTG-CODE-5
Application Security Verification Standard 4.0.3 (ASVS)
V10.1 Code Integrity
US National Institute of Standards and Technology (NIST)
NIST Special Publication 800-190
4.1.1 Image vulnerabilities
4.1.3 Embedded malware
4.4.1 Vulnerabilities within the runtime software
4.4.4 App vulnerabilities
4.4.5 Rogue containers
NIST Special Publication 800-163 Revision 1
2.2 Organization-Specific Requirements App Documentation
ioXt Alliance
Mobile Application Profile
4.9. Vulnerability Reporting Program VDP1
4.9. Vulnerability Reporting Program VDP2
4.9. Vulnerability Reporting Program VDP3
4.9. Vulnerability Reporting Program VDP4
4.9. Vulnerability Reporting Program VDP5
ETSI TS 103 732
8.2 Security assurance requirements
8.2 Security assurance requirements
1. Ensure only apps that meet the code's security and privacy baseline requirements are allowed on the app store
Department for Digital, Culture, Media & Sport (DCMS)
Code of practice for app store operators and app developers
3. Implement a vulnerability disclosure process
3. Implement a vulnerability disclosure process
3. Implement a vulnerability disclosure process
8. Ensure appropriate steps are taken when a personal data breach arises
8. Ensure appropriate steps are taken when a personal data breach arises
8. Ensure appropriate steps are taken when a personal data breach arises
National Information Assurance Partnership (NIAP)
Requirements for Vetting Mobile Apps from the Protection Profile for Application Software
Security Assurance Requirements AVA_VAN.1.2E

Vulnerability Management

1. ioXt Alliance

1.1. Mobile Application Profile

Link: https://static1.squarespace.com/static/5c6dbac1f8135a29c7fbb621/t/604aa3fa668a8e3b50630433/1615504379349/Mobile_Application_Profile.pdf

1.1.1. 4.9. Vulnerability Reporting Program VDP1

VDP in place

1.1.2. 4.9. Vulnerability Reporting Program VDP2

Accept external submissions

1.1.3. 4.9. Vulnerability Reporting Program VDP3

Monitoring security relevant components.

1.1.4. 4.9. Vulnerability Reporting Program VDP4

Responsible disclosure of defects to impacted parties that must take action.

1.1.5. 4.9. Vulnerability Reporting Program VDP5

Public Researcher Rewards program

2. ETSI TS 103 732

2.1. 8.2 Security assurance requirements

Link: https://www.etsi.org/deliver/etsi_ts/103700_103799/103732/01.01.01_60/ts_103732v010101p.pdf

2.1.1. 8.2 Security assurance requirements

The security assurance requirements consist of EAL2 augmented with ALC_FLR.3 [3], where ALC_FLR.3 is refined as below.
ALC_FLR.3 Systematic flaw remediation
ALC_FLR.3.1D The developer shall document and provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.3.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.3.3D The developer shall provide flaw remediation guidance addressed to TOE users.
ALC_FLR.3.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.3.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.3.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.3.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users. The flaw remediation procedures documentation shall also define the planned minimum length of time after release of the TOE that these methods will be used to maintain the TOE.
ALC_FLR.3.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.
ALC_FLR.3.6C The flaw remediation procedures shall include a procedure requiring timely response and the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.
ALC_FLR.3.7C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.
ALC_FLR.3.8C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.3.9C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.
ALC_FLR.3.10C The flaw remediation guidance shall describe a means by which TOE users can register with the developer, to be eligible to receive security flaw reports and corrections.
ALC_FLR.3.11C The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.
ALC_FLR.3.1E The evaluator shall confirm that the information provided meets all requirements for content and

presentation of evidence.
NOTE: ISO/IEC JTC 1 SC27 WG3 is currently in the process of creating a TR for patch management, but this is not stable yet. Once this is ready, it is suggested to revise the present document to take this TR into account

3. Department for Digital, Culture, Media & Sport (DCMS)

3.1. Code of practice for app store operators and app developers

Link: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers/code-of-practice-for-app-store-operators-and-app-developers

3.1.1. 1. Ensure only apps that meet the code's security and privacy baseline requirements are allowed on the app store

1.4 App stores shall have an app reporting system (such as visible contact details or a contact form), so that users and security researchers can report malicious apps, and Developers can report fraudulent copies of their own apps to the app store.

3.1.2. 3. Implement a vulnerability disclosure process

3.1 Every app shall have a vulnerability disclosure process, such as through contact details or a contact form, which is created and maintained by the Developer.

3.1.3. 3. Implement a vulnerability disclosure process

3.2 Operators shall check that every app on their platform has a vulnerability disclosure process which is accessible and displayed on their app store. This process shall ensure that vulnerabilities can be reported without making them publicly known to malicious actors.

3.1.4. 3. Implement a vulnerability disclosure process

3.3 App Store Operators shall ensure their app store has a vulnerability disclosure process, such as contact details or a contact form, which allows stakeholders to report to the Operator any vulnerabilities found in the app store platform.
3.3.1 App Store Operators should accept vulnerability disclosure reports from stakeholders for apps on their platforms if the Developer has not issued acknowledgement specific to said report after 15 working days. App Store Operators should assess the merit of these reports, and contact the Developer if they are deemed credible.
3.3.2 If App Store Operators don't receive an acknowledgement from the Developer, after a further 15 working days, then they should make the app unavailable on the store.

3.1.5. 8. Ensure appropriate steps are taken when a personal data breach arises

8.1. If a Developer or App Store Operator becomes aware of a security incident in an app which involves a personal data breach, they should inform other relevant stakeholders including App Developers, App Store Operators, and library/SDK Developers.

3.1.6. 8. Ensure appropriate steps are taken when a personal data breach arises

8.2. Developers shall assess the impact of said incident and follow appropriate steps set out under data protection law.

3.1.7. 8. Ensure appropriate steps are taken when a personal data breach arises

8.3. When a personal data breach occurs through an app, the Developer shall inform affected users and signpost instructions for users to protect themselves.

4. National Information Assurance Partnership (NIAP)

4.1. Requirements for Vetting Mobile Apps from the Protection Profile for Application Software

Link: https://www.niap-ccevs.org/MMO/PP/394.R/pp_app_v1.2_table-reqs.htm

4.1.1. Security Assurance Requirements AVA_VAN.1.2E

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
Application Note: Public domain sources include the Common Vulnerabilities and Exposures (CVE) dictionary for publicly known vulnerabilities. Public domain sources also include sites which provide free checking of files for viruses.

5. US National Institute of Standards and Technology (NIST)

5.1. NIST Special Publication 800-190

Link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf

5.1.1. 4.1.1 Image vulnerabilities

There is a need for container technology-specific vulnerability management tools and processes. Traditional vulnerability management tools make many assumptions about host durability and app update mechanisms and frequencies that are fundamentally misaligned with a containerized model. These tools are often unable to detect vulnerabilities within containers, leading to a false sense of safety.

Organizations should use tools that take the pipeline-based build approach and immutable nature of containers and images into their design to provide more actionable and reliable results. Key aspects of effective tools and processes include:
1. Integration with the entire lifecycle of images, from the beginning of the build process, to whatever registries the organization is using, to runtime.
2. Visibility into vulnerabilities at all layers of the image, not just the base layer of the image but also application frameworks and custom software the organization is using. Visibility should be centralized across the organization and provide flexible reporting and monitoring views aligned with organizations' business processes.
3. Policy-driven enforcement; organizations should be able to create "quality gates" at each stage of the build and deployment process to ensure that only images that meet the organization's vulnerability and configuration policies are allowed to progress. For example, organizations should be able to configure a rule in the build process to prevent the progression of images that include vulnerabilities with Common Vulnerability Scoring System (CVSS) [18] ratings above a selected threshold.

5.1.2. 4.1.3 Embedded malware

Organizations should continuously monitor all images for embedded malware. The monitoring processes should include the use of malware signature sets and behavioral detection heuristics based largely on actual "in the wild" attacks.

5.1.3. 4.4.1 Vulnerabilities within the runtime software

The container runtime must be carefully monitored for vulnerabilities, and when problems are detected, they must be remediated quickly. A vulnerable runtime exposes all containers it supports, as well as the host itself, to potentially significant risk. Organizations should use tools to look for Common Vulnerabilities and Exposures (CVEs) vulnerabilities in the runtimes deployed, to upgrade any instances at risk, and to ensure that orchestrators only allow deployments to properly maintained runtimes.

5.1.4. 4.4.4 App vulnerabilities

Existing host-based intrusion detection processes and tools are often unable to detect and prevent attacks within containers due to the differing technical architecture and operational practices previously discussed. Organizations should implement additional tools that are container aware and designed to operate at the scale and change rate typically seen with containers. These tools should be able to automatically profile containerized apps using behavioral learning and build security profiles for them to minimize human interaction. These profiles should then be able to prevent and detect anomalies at runtime, including events such as:
• Invalid or unexpected process execution,
• Invalid or unexpected system calls,
• Changes to protected configuration files and binaries,
• Writes to unexpected locations and file types,
• Creation of unexpected network listeners,
• Traffic sent to unexpected network destinations, and
• Malware storage or execution.

Containers should also be run with their root filesystems in read-only mode. This approach isolates writes to specifically defined directories, which can then be more easily monitored by the aforementioned tools. Furthermore, using read-only filesystems makes the containers more resilient to compromise since any tampering is isolated to these specific locations and can be easily separated from the rest of the app.

5.1.5. 4.4.5 Rogue containers

Organizations should institute separate environments for development, test, production, and other scenarios, each with specific controls to provide role-based access control for container deployment and management activities. All container creation should be associated with individual user identities and logged to provide a clear audit trail of activity. Further, organizations are encouraged to use security tools that can enforce baseline requirements for vulnerability management and compliance prior to allowing an image to be run.

5.2. NIST Special Publication 800-163 Revision 1

Link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163r1.pdf

5.2.1. 2.2 Organization-Specific Requirements App Documentation

Test Results
Code review results and other testing results will indicate which security standards were followed. For example, if an app threat model was created, this standard should be submitted. It will list weaknesses that were identified and should have been addressed during app design and coding.

6. Open Web Application Security Project (OWASP)

6.1. Mobile Application Security Verification Standard (MASVS)

Link: https://github.com/OWASP/owasp-masvs/releases/tag/v1.4.2

6.1.1. 1.11 MSTG-ARCH-11

> A responsible disclosure policy is in place and effectively applied.

6.1.2. 7.5 MSTG-CODE-5

> All third party components used by the mobile app, such as libraries and frameworks, are identified, and checked for known vulnerabilities.

6.2. Application Security Verification Standard 4.0.3 (ASVS)

Link: https://raw.githubusercontent.com/OWASP/ASVS/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-en.pdf

6.2.1. V10.1 Code Integrity

> 10.1.1 Verify that a code analysis tool is in use that can detect potentially malicious code, such as time functions, unsafe file operations and network connections.