AMR Cyber Security

OVS WHITE PAPER

AUGUST 2023

PUBLIC RELEASE

TABLE OF CONTENTS

1.0 Introduction

AMR CyberSecurity is a CHECK, CREST and STAR approved company with a team of experienced principal consultants that hold the highest technical qualifications. AMR CyberSecurity was founded to deliver the best human-led penetration assessment and security assurance services that reduce security risks for the organisations we partner with.

AMR CyberSecurity works with you to protect your brand, your assets and your reputation against the increasing real-world threat of cyber-attacks and digital security compromise.

AMR CyberSecurity is delighted to announce that we are one of the elite cyber security organisations certified to deliver CREST OWASP Verification Standard (OVS) for Web applications. The CREST OVS program has been designed to align with OWASP's application security standard.

1.1 Background

Organisations around the world are faced with the challenge of an expanding attack surface as a result of increased connectivity, digitisation, cloud migration and API integration.

Increasing sums of money are being spent to try to mitigate the rapidly evolving risks to businesses, however the services are unregulated, vary in quality and consistency and thus present a risk to the buying community. There is a growing move towards legislation and regulation to try and set standards but these tend to be domestically or regionally focused.

The result is an expanding patchwork of frameworks and regulations imposed on increasingly complex international supply chains and cross-border trade.

CREST OVS aims to provide much needed clarity, consistency and assurance for application security, with a framework designed to promote the standards as defined by industry professionals.

1.2 Overview of CREST OVS

CREST OVS accredits companies that provide application security testing services to organisations and the application development industry.

It validates that processes, methodology and deliverables to the end-customer are robust and fit for purpose in correctly testing and auditing the principals and controls of the OWASP applications security standards.

It is based on OWASP's two application security standards:

- Application Security Verification Standard (ASVS)
- Mobile Application Security Verification Standard (MASVS)

CREST OVS aims to set the international standard for application security and provide increased levels of assurance for application security assessments. It is important that the product and process delivered to end customers is via a managed and third-party audited framework such as CREST.

1.3 Overview of OWASP ASVS

The OWASP Application Security Verification Standard (ASVS) is a community-driven effort to establish a framework for security requirements throughout the application development lifecycle and beyond, OWASP ASVS has two main goals:

1. To help organisations develop and maintain secure applications.

2. To allow security service vendors, security tools vendors, and consumers to align their requirements and offerings.

Each ASVS level contains a list of security requirements. Each of these requirements can also be mapped to security-specific features and capabilities that must be built into software by developers.

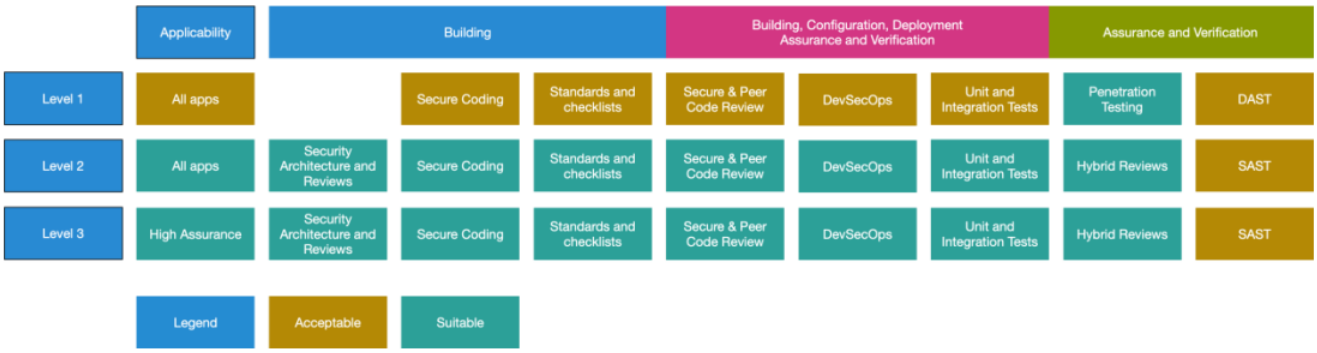


Figure 1 - ASVS matrix of levels and control areas

2.0 Approach

AMR's OVS service line can be applied to any of the application security testing services that we offer:

- Web Application Security Penetration Testing
- Application Programming interface (API) Security Penetration Testing
- Application (Thick Client) Security Penetration Testing
- Mobile Application Security Penetration Testing
- Secure Code Review
- Development, Application and Code Framework auditing

At AMR CyberSecurity, our testing services help you work towards the OWASP ASVS, whatever level you wish to obtain, and are based on the exact requirements of your organisation, as well as the application under consideration.

The ASVS is a multi-level Standard spanning 14 sections and over 260 controls (Fig.1), each assigned a level.

2.1 ASVS Level 1

This is considered the 'bare minimum' security level that all applications should look to achieve. It is useful as the first step of a multi-phase approach, or for when an application does not store or handle sensitive data.

To meet Level 1 standards, applications need to be tested to ensure they defend adequately against easy to exploit vulnerabilities, low effort techniques and vulnerabilities outlined in security checklists such as the OWASP Top 10.

2.2 ASVS Level 2

This is considered the 'standard' security level an application should achieve and ensures that the application under consideration defends against most of the risks associated with software today.

This level should be the baseline for any application that processes sensitive data, such as healthcare data, handles significant business to business transactions or interacts with any critical assets or processes.

2.3 ASVS Level 3

This is the highest level and is designed for critical applications requiring significant security verification. For example, those used within national infrastructure, physical health & safety, or military operations.

Level 3 is also applied if applications perform critical functions, or where the failure of an application could result in a significant impact to an organisation's operations, or even its ability to survive.

2.4 Benefits of OVS Testing

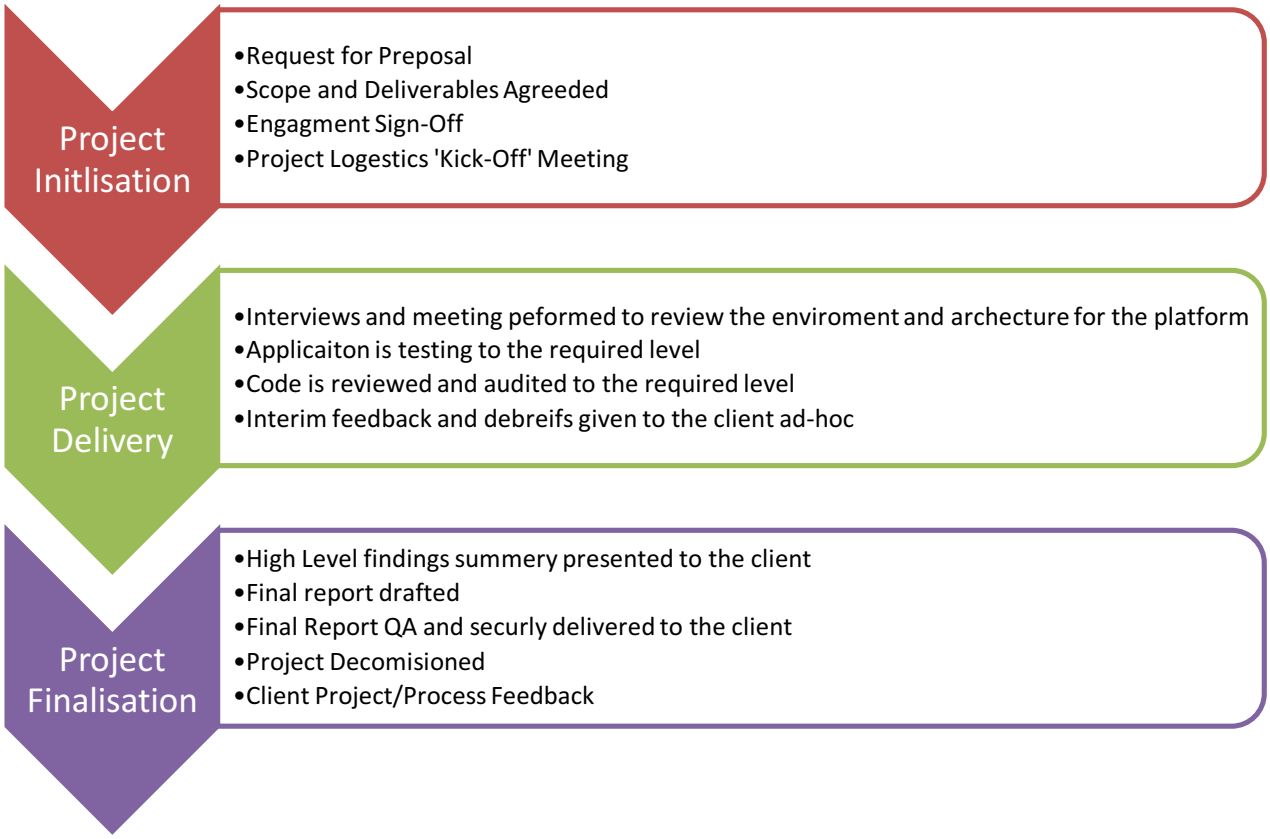
The framework has direct benefits for organisations that rely on secure applications for their business, such as:

- Application testing by a security company to an internationally recognised standard.
- Independent validation that they are getting a quality assured and audited service.
- Potential insurance benefits from using a web developer whose apps have been tested by a CREST OVS-accredited company.
- Marketing benefits for organisations that implement OVS testing for application development across their supply chains.
- Standardised, clear and concise web security reports

3.0 Delivery Approach

AMR Cybersecurity will carry out all testing and auditing in accordance with the *AMR CyberSecurity Application Testing and Security Review Methodology*. This methodology aligns with governmental and cyber-security industry standards that have emerged to focus on key information security requirements and metrics and the following industry best practise procedures and frameworks.

The high level the engagement process is outlined in the diagram below:



The 'Security Verification Standard' level used is based on a defined, proven models shown below. This model can be used to determine the depth of the testing on an organisation's application assessment.

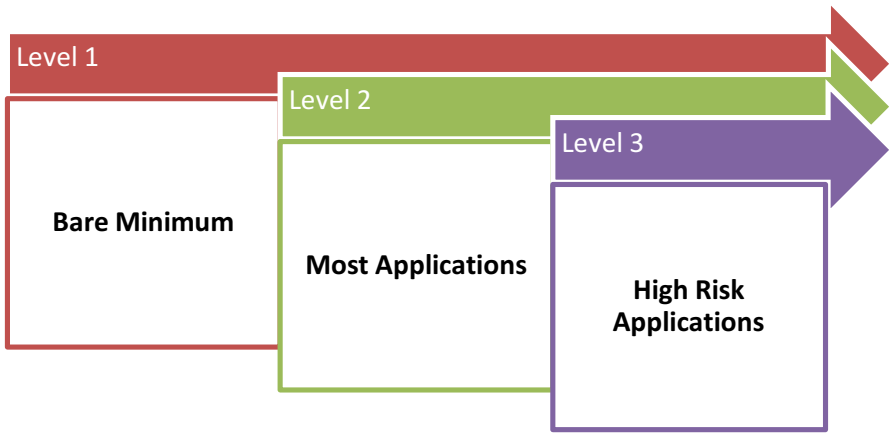


Figure 2 - Application Security Verification Standard (ASVS)

Different types of organisations will require different levels of maturity for their applications deployed. For example, a small company operating a retail business will not have the same requirement for enhanced checks as a major corporate organisation in the finance sector or a government department.

Consequently, the level of maturity should be reviewed in context and compared to the organisation's actual requirements for the application.

For this AMR CyberSecurity uses the table (Table 1) and our expert understanding of the organisation's industry and cyber security controls to rate the level of maturity for the organisation.

Table 1 - Organisation maturity matrix

Level	Maturity	Description
0	Non-existing	Requirement is not selected. We do not believe this is a problem that needs to be solved in our application.
1	Initial	We are aware of the existence of the requirement and the need to study it. However, there is no implementation, and further consideration is needed before going into development.
2	Defined	Implementation has been developed, but relies heavily on individual knowledge, and where a probability of omission exists.
3	Standardised	A standard for implementation and procedures has been documented and communicated across teams, including awareness and training where needed.
4	Verified	Implementation of control has been tested and verified across entire application. The processes are constantly improved and correspond to good practice. Automation and the use of tools are still limited or partial.
5	Automated	The implementation is verified at all times through automated testing and integration with development workflow and has reached the recommended level of best practices.

3.1 Elements Reviewed

AMR Cybersecurity assessment tools have been developed in conjunction with representatives from a broad range of organisations, including industry bodies, consumer organisations, the UK government, and suppliers of expert technical security services.

It delivers an assessment against a methodology model based on various phases and steps that make up the key engagement types:

OWASP AVS – During the assessment up to 14 key areas, outlined below, are assessed using a 3-level structure for progression and development of the implementation to be audited.

- V1: Architecture, Design and Threat Modelling
- V2: Authentication and Verification
- V3: Session Management Verification

- V4: Access Control Verification
- V5: Validation, Sanitation and Encoding Verification
- V6: Stored Cryptography Verification
- V7: Error Handling and Logging Verification
- V8: Data Protection Verification
- V9: Communication Verification
- V10: Malicious Code Verification
- V11: Business Logic Verification
- V12: File and Resources Verification
- V13: API and Web Service Verification
- V14: Configuration and Verification

3.2 Deliverable

There are a number of deliverables as the output of an ASVS or MASVS assessment. Some engagements will have one, some or all of these depending on the client's requirements, at the minimum these will be:

- An overarching management report that contains all the testing technical output and results from the engagement containing:
  - An overview of the engagement
  - Summary of findings, including vulnerability description severity rating (low to critical) and list of affected components.
  - A detailed analysis of each vulnerability.
  - Cross refences details against known vulnerabilities frameworks and category standards
- Summary of Findings in the form of a spreadsheet (Microsoft Excel .xlsx). Separate Tabs included for each area tested as well as a tab detailing any published vulnerabilities.
- OWASPv4_Checklist.xlsx
- OWASP-ASVS.xlsx

Additional deliverables may also be provided depending on the nature of the engagement some of these may include:

- `ASVS-checklist-en.xlsx`
- `Mobile_App_Security_Checklist_en.xlsx`

Based on the responses to the various elements tested and audit questions during the **assessment**, an organisation's level of maturity, and resilience for each of the security controls, steps and phases for the application being assessed is calculated using AMR Cybersecurity assessment tools.
These tools make use of a carefully designed algorithm that consider both the level of response to each test element and the associated weighting factor.

A useful summary of the assessment results is produced automatically and presented both as a table (*Fig 4*) and radar diagram (*Fig 3*) in the **results** tool, which outline the results for an organisation's application.

Security Category	Valid criteria	Total criteria	Validity Percentage	ASVS Level Acquired
Architecture	0	42	0.00	
Authentication	0	57	0.00	
Session Management	0	20	0.00	
Access Control	0	10	0.00	
Input Validation	0	30	0.00	
Cryptography at rest	0	16	0.00	
Error Handling and Logging	0	13	0.00	
Data Protection	0	17	0.00	
Communication Security	0	8	0.00	
Malicious Code	0	10	0.00	
Business Logic	0	8	0.00	
Files and Resources	0	15	0.00	
Web Service	0	15	0.00	
Configuration	0	25	0.00	
Total	0	286	0.00	

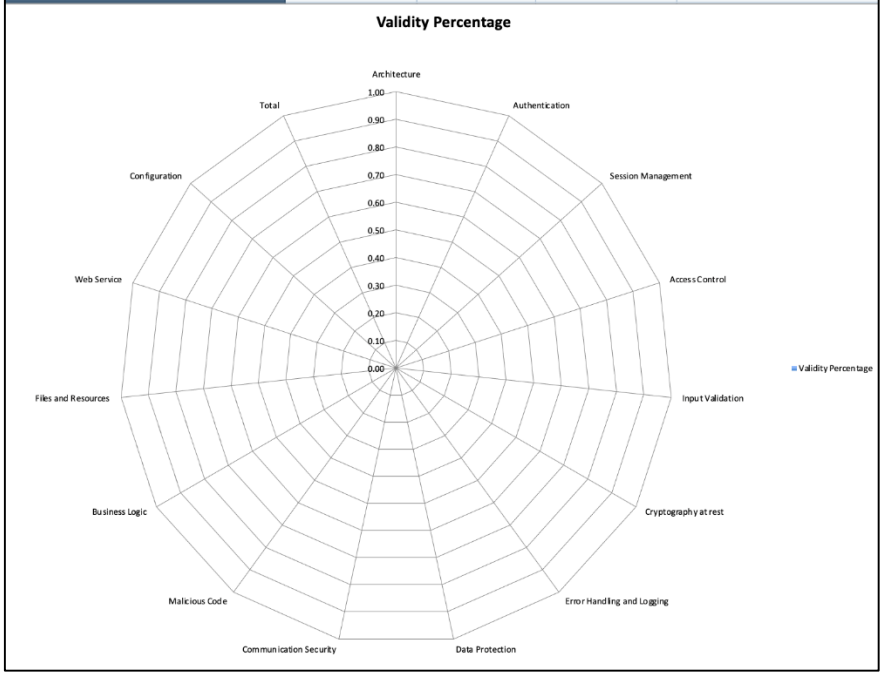
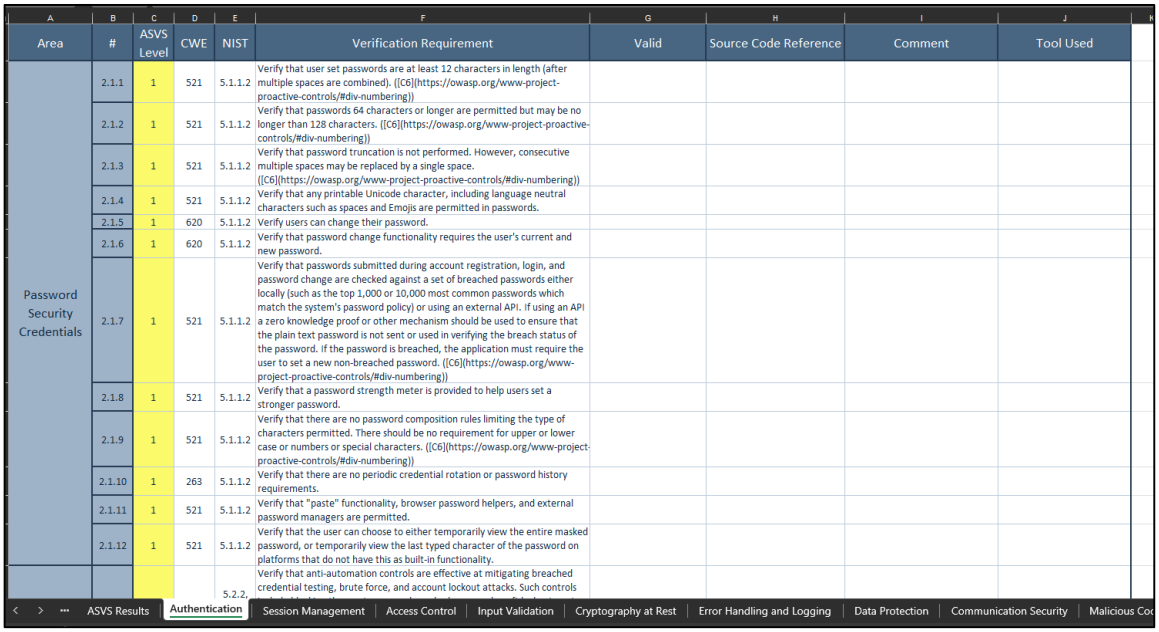


Figure 3 *- Results generated.*



Area	#	ASVS Level	CWE	NIST	Verification Requirement	Valid	Source Code Reference	Comment	Tool Used
Password Security Credentials	2.1.1	1	521	5.1.1.2	Verify that user set passwords are at least 12 characters in length (after multiple spaces are combined). ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering))				
	2.1.2	1	521	5.1.1.2	Verify that passwords 64 characters or longer are permitted but may be no longer than 128 characters. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering))				
	2.1.3	1	521	5.1.1.2	Verify that password truncation is not performed. However, consecutive multiple spaces may be replaced by a single space. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering))				
	2.1.4	1	521	5.1.1.2	Verify that any printable Unicode character, including language neutral characters such as spaces and Emojis are permitted in passwords.				
	2.1.5	1	620	5.1.1.2	Verify users can change their password.				
	2.1.6	1	620	5.1.1.2	Verify that password change functionality requires the user's current and new password.				
	2.1.7	1	521	5.1.1.2	Verify that passwords submitted during account registration, login, and password change are checked against a set of breached passwords either locally (such as the top 1,000 or 10,000 most common passwords which match the system's password policy) or using an external API. If using an API a zero knowledge proof or other mechanism should be used to ensure that the plain text password is not sent or used in verifying the breach status of the password. If the password is breached, the application must require the user to set a new non-breached password. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering))				
	2.1.8	1	521	5.1.1.2	Verify that a password strength meter is provided to help users set a stronger password.				
	2.1.9	1	521	5.1.1.2	Verify that there are no password composition rules limiting the type of characters permitted. There should be no requirement for upper or lower case or numbers or special characters. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering))				
	2.1.10	1	263	5.1.1.2	Verify that there are no periodic credential rotation or password history requirements.				
	2.1.11	1	521	5.1.1.2	Verify that "paste" functionality, browser password helpers, and external password managers are permitted.				
	2.1.12	1	521	5.1.1.2	Verify that the user can choose to either temporarily view the entire masked password, or temporarily view the last typed character of the password on platforms that do not have this as built-in functionality.				
				5.2.2,	Verify that anti-automation controls are effective at mitigating breached credential testing, brute force, and account lockout attacks. Such controls				

ASVS Results | Authentication | Session Management | Access Control | Input Validation | Cryptography at Rest | Error Handling and Logging | Data Protection | Communication Security | Malicious Cod

Figure 4 *- Radar diagram of results*

4.0 Why AMR CyberSecurity

At AMR CyberSecurity we expand and highlight additional controls based on the bespoke requirements of an organisation, as well as testing, benchmarking, and auditing existing controls.

AMR CyberSecurity offers a complete all-round security posture assessment. Our highly experienced consultants have worked across many sectors including Major Corporations, Critical National Infrastructure, Banking and Military. Our consultants understand how to communicate technical issues to both technical and non-technical audiences. We have identified six key security pillars using our combined industry knowledge. This enables us to offer services in the following areas to help organisations improve their protective and control capabilities:

- **Penetration Testing,**
- **Advanced Penetration Testing,**
- **Social Engineering,**
- **Security configuration reviews,**
- **Hardware and IoT security**
- **Secure Source Code Review**

AMR CyberSecurity is a member of leading cybersecurity bodies, including CREST, Cyber Scheme, and IASME Cyber Essentials.

Our senior security consultants hold a minimum of Cyber Scheme CSTL, CREST CCT or TIGER SST (CHECK Team Leader) level qualifications and the highest level of security clearances including Security Clearance (SC) and Developed Vetting (DV).

AMR CyberSecurity is also ISO27001 and ISO9001 certified, assuring that all services that we offer are performed to the highest level of standards.

For more information on any of **AMR Cyber Security** Services please contact **Rachel Bi** on enquiries@amrcybersecurity.com