@lizfrenz /git

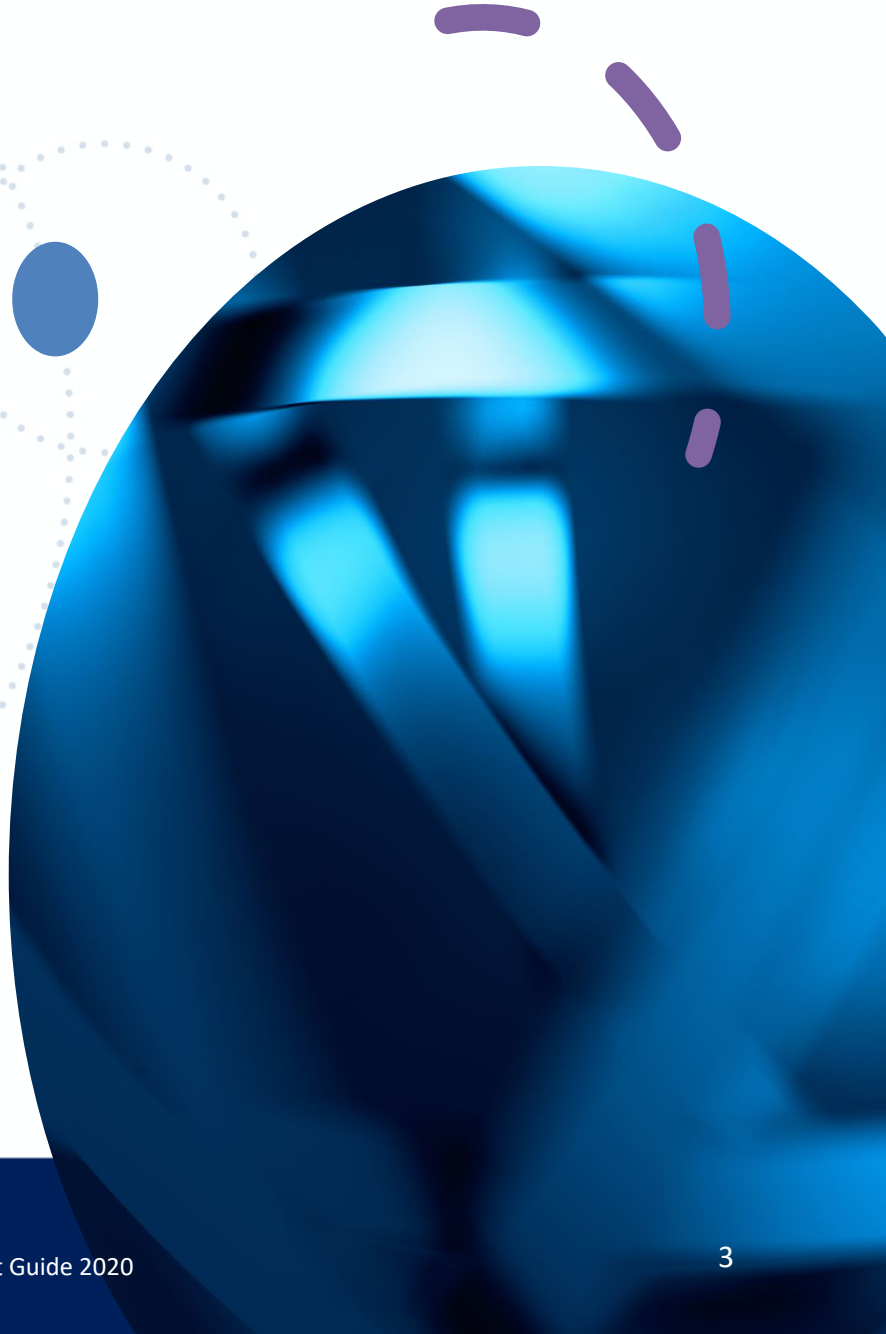
OWASP VULNERABILITY MANAGEMENT GUIDE (OVMG)

$ whoami

- Elizabeth Frenz
- Cyber Security professional
- OWASP volunteer since 2015
- Project leader and author of OWASP Vulnerability Management Guide

What is Vulnerability Management?
(in this context)

- Vulnerability
- potential threats in systems, application, people
- Management
- high-level and low-level governance
- Application of Vulnerability Management
- Preventing cyber attacks
- TJMax, Equifax, Yahoo, Adobe, Mariott, NHS e.g.



Business Impact

- Law & Compliance (PCI DSS)
- Data Breaches & Lawsuits
- Intellectual Property Theft
- Resource Abuse and Hijacking
- Loss of Operations

Why is Vulnerability Management even a project?

OFTEN CONFUSED WITH SOMETHING ELSE (PATCHING, PEN TESTING, A TOOL)

IT'S A COMPLEX PROCESS

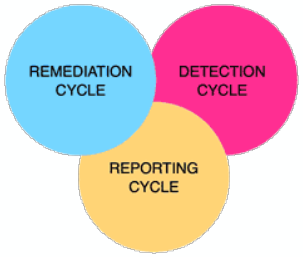
IT IS CHALLENGING TO DEPLOY

THERE IS NO "ONCE AND FOR ALL" SOLUTION

MOST OF THE REFERENCES AND GUIDELINES ARE LENGTHY

OVMG Components

- Three cycles
  - Four Processes
    - Steps
- Cycle – is a domain
- Process – is a task
- Steps – to do list



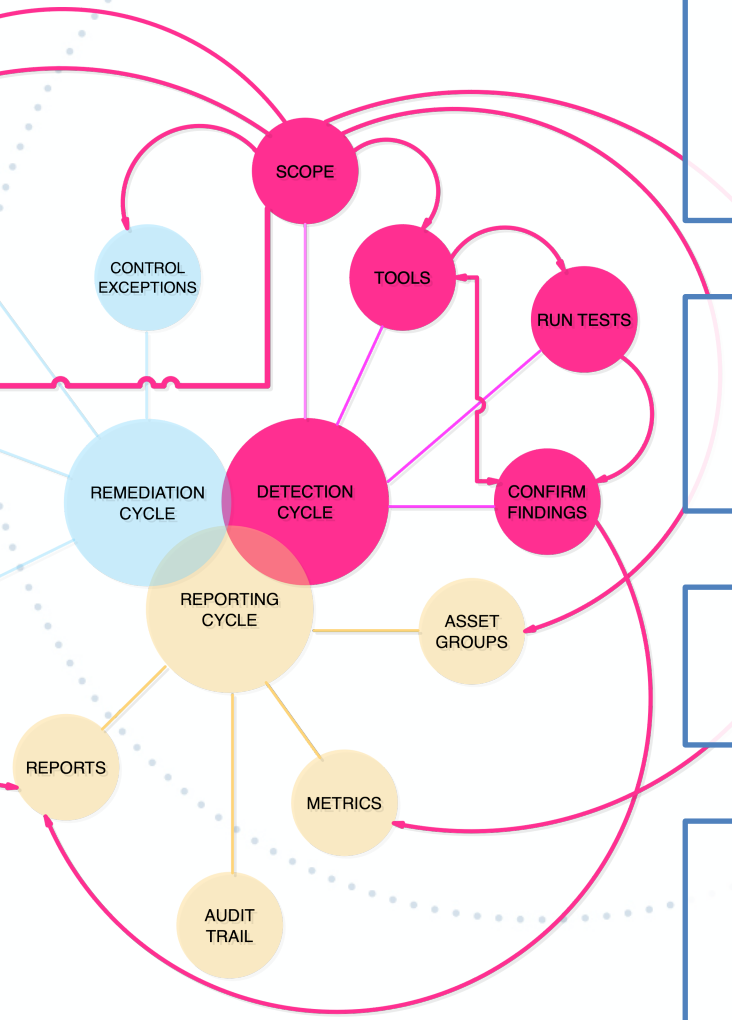
OVMG How2Read

- Cycle – a continuous process; tricycle; color coded
- Task – is actionable item that feeds into other processes
- Input/Output – show how a task is interconnected within the tricycle
- To do – aids to the checklist
- End goal – a short statement of expected result at the end of each task

Tricycle may not be 100 % perfect as you start VM program, but should adhere to continuous improvement as you progress

1.1 TASK		INPUT	OUTPUT
Define/Refine scope		2.4 Reports 3.4 Exceptions	1.2 Tools 2.1 Assets Groups 2.2 Metrics 2.4 Reports 3.1 Prioritize 3.4 Exceptions
#	**TO DO**	**WHY**	
1.1.1	Know the enterprise risks	Whether your organization does or doesn't have risk registry, you have to understand what risks worried your management the most and where are these risks are coming from. Understand a magnitude of monetary losses	

Detection



Scope

- management's sign-off
- objectives of vulnerability tests
- VM policy ready

Tools

- optimize the tools in use to fulfill the objectives of the vulnerability tests

Run Tests

- run vulnerability tests

Confirm Findings

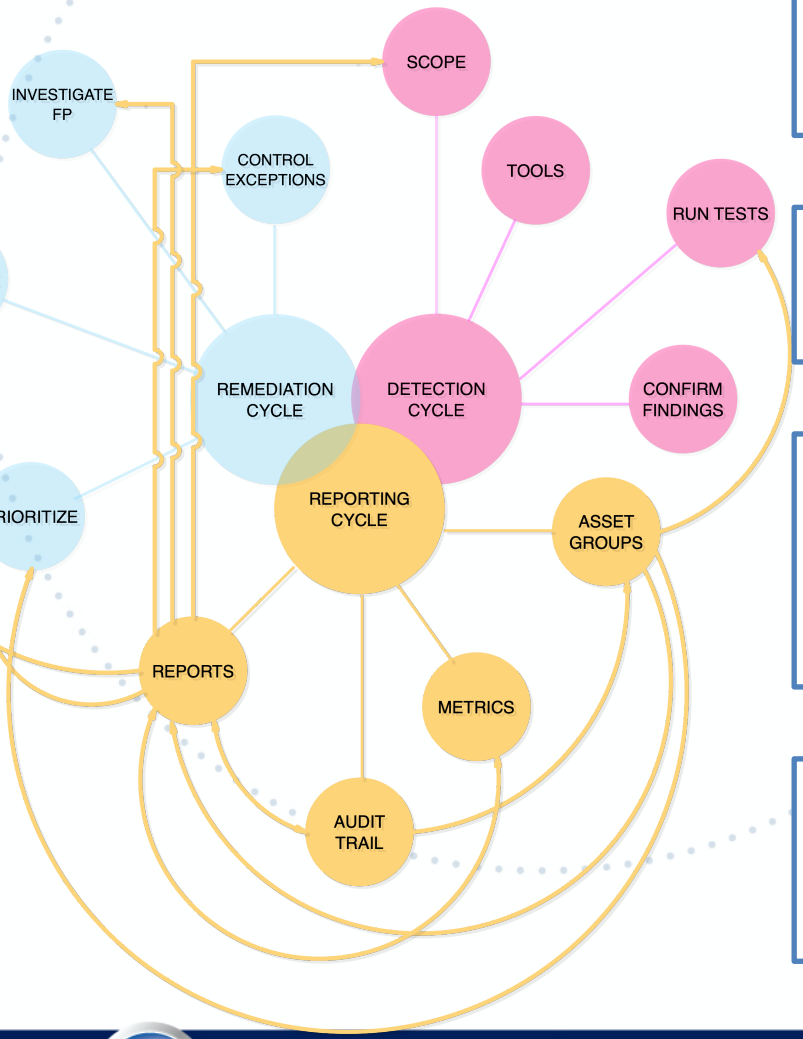
- understand the security test results; have an evidence that your tool doesn't need fine tuning.

Determine the type of tests

- Network scans: credential vs. uncredentialed scans
- Applications scans: static code analysis (SAST) vs. dynamic scans (DAST)
- Business email security or Social Engineering

OVMG is tool agnostic

Reporting



Assets Groups

- create the broad categories for your organization assets

Metrics

- define the metrics you can use in your reports

Audit Trail

- create an audit trail to track a workload for teams or individuals who are responsible for vulnerability remediation

Reports

- summarize security scanning results in a concise form

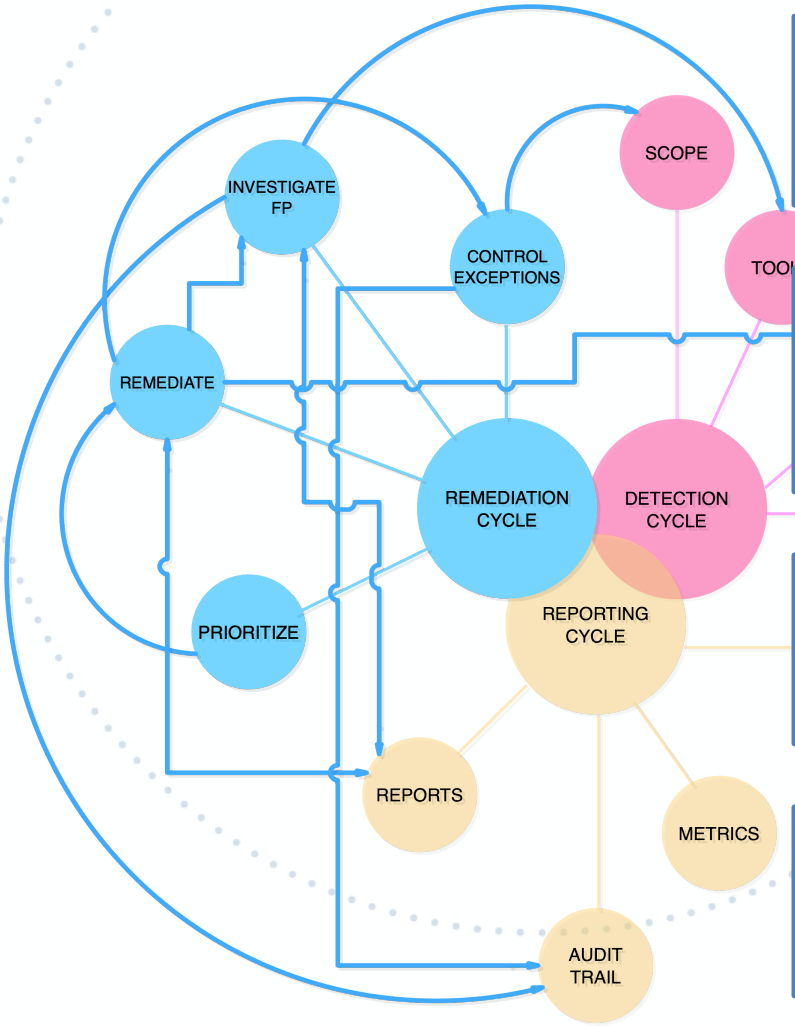
Asset Groups

- Functional
  - Primary | secondary
  - Type
- Type of environment (dev/QA/production)
- Type of OS
- CVE numbering authority
- Type of vulnerability (OWASP Top 10)

Metrics

- Amount and Percentage of vulnerable assets
- Amount and Percentage of vulnerability by severity
- New vulnerability by severity
- New vulnerability by asset groups
- Aging vulnerability by published date
- Aging vulnerability by discovery time

Remediation



Prioritize

- Evidence based reasoning why some vulnerabilities should be remediated asap, in a week, in a month, e.g.

Remediate

- remediation work done by the assigned teams/individuals. Remediation should not be assumed until confirm by the next round of tests.

Investigate FP

- review the evidence that suggests that an instance is not a vulnerability.

Control Exceptions

- ensure that all non-compliance is documented and approved by senior management.

Benefits of OVMG

Who:

- Business folks
- InfoSec folks
- All IT folks!

How:

- Risk reduction
- Process improvement
- Security education

What's to come

- Revisions
- Report Template
- Virtual Discussions


Thank you for attending OVMG presentation! Thank you for attending OVMG presentation! Thank you for attending OVMG presentation! Thank you for attending OVMG presentation! Thank you for attending OVMG presentation! Thank you for attending