

How to build a vulnerability management programme

Pratik Shah

TECHNICAL DIRECTOR (CONSULTING AND RESEARCH)

Jed Kafetz

CYBER SECURITY PRACTICE LEAD

claranet  **cyber security**[®]



Contents

What is vulnerability management?	3
Ingredients required	4
Who actually wants this?	4
Why you should want this	5
How do they calculate risk?.....	8
Strengths	8
Limitations	8
Vulnerability Management Lifecycle	9
Phase 2: Prioritisation of Assets.....	11
Phase 3: Scanning and Security Testing.....	12
Phase 4: Reporting	14
Phase 5: Remediation	15
Phase 6: Verification and Monitoring	16
How to eat an elephant	17

What is vulnerability management?

Vulnerability management is the continuous and routine process of detecting, assessing, reporting, managing, and resolving vulnerabilities across applications, endpoints, networks, and systems. The primary objective of vulnerability management is to **minimise an organisation's risk exposure by addressing a majority of vulnerabilities to reduce the chances of successful cyber attacks leading to data loss or data breach.**

A robust vulnerability management programme relies on understanding your business, your IT estate and the threats you are likely to face, in order to rank risks and address security weaknesses promptly and efficiently. It should enforce accountability, action and continuous improvement, and should enable a risk-based approach to remediating risks.

In most cases, security teams use a combination of tools and offensive security testing to identify vulnerabilities, then implement their own processes to patch and remediate them.





INGREDIENTS REQUIRED

BUDGET e.g., tens or hundreds of thousands of pounds annually.
The cost of your programme will be determined by the size of your organisation, and the number of assets and employees involved

BUY-IN FROM SENIOR LEADERSHIP

SECURITY EXPERTISE

SECURITY TOOLS & PLATFORMS

INPUT FROM LEGAL & COMPLIANCE TEAMS

EFFICIENT PROJECT MANAGEMENT



Who actually wants this?

When they work well, vulnerability management programmes represent the pinnacle of a highly-advanced security posture which is risk-based, proactive, and practical. Who wants to go to all this effort, and why?

One of the key requirements of ISO 27001 is to identify and assess information security risks, which includes the identification and management of vulnerabilities. ISO 27001 requires the implementation of controls to address identified risks, and vulnerability management is an important control for mitigating the risks associated with vulnerabilities.

The General Data Protection Regulation (GDPR) does not specifically require organisations to implement a vulnerability management programme. However, it does emphasise the importance of having appropriate security measures in place to protect personal data. Under GDPR, organisations are required to implement appropriate technical and organisational measures to ensure the security of personal data they process. This includes measures to protect against unauthorised access, accidental or unlawful destruction, alteration, disclosure, or any other unauthorised processing.

Why you should want this

1. Guide, support and justify your security efforts

The overarching purpose of a vulnerability management programme is to strategically guide your security efforts and report on their effectiveness. If you are an IT or security manager, and are required to report to senior leaders that you are aware of the security vulnerabilities affecting your organisation and are working to remediate them, a vulnerability management programme will support these claims and track your progress. It will ultimately guide and justify your security efforts, while providing assurances that risks to the organisation are being management appropriately.

2. Improved security controls

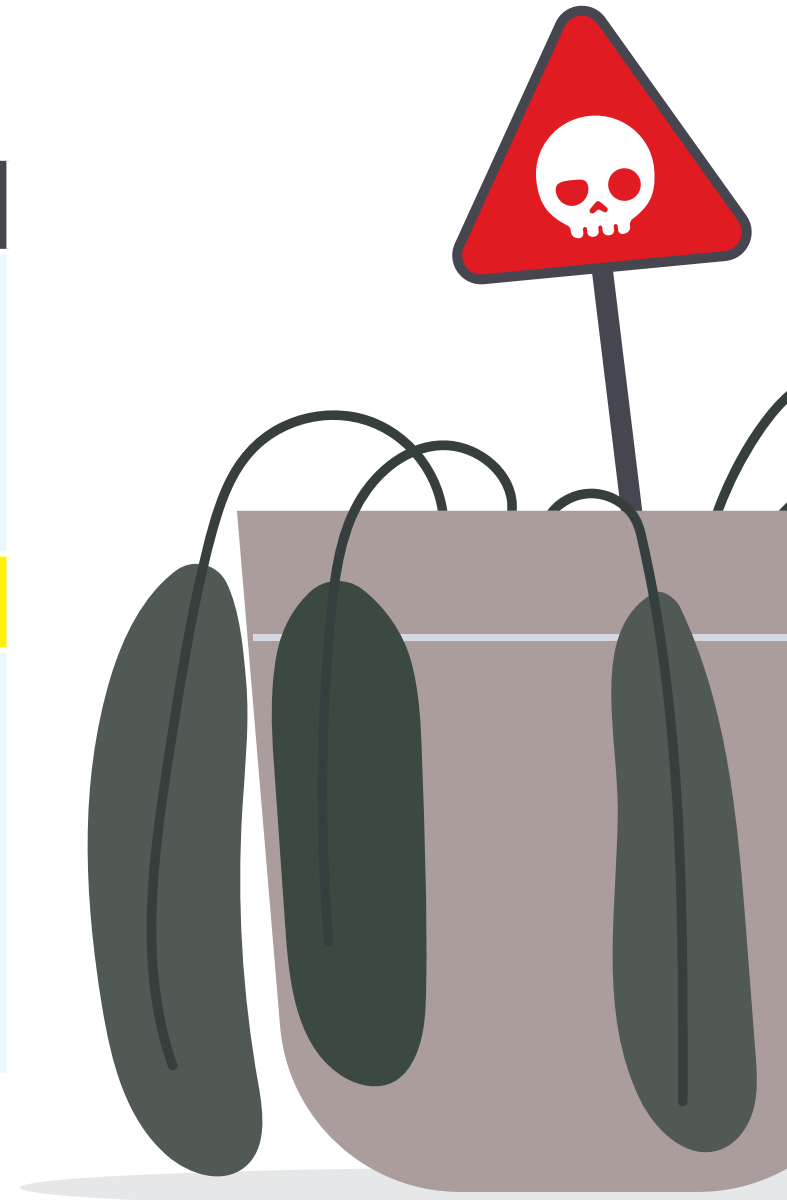
Regularly scanning for vulnerabilities and promptly patching them hardens your security posture, making it more difficult for attackers to compromise, breach, and/or damage your organisation's systems.

3. Visibility and reporting

Vulnerability management provides centralised, accurate, and up-to-date reporting on your organisation's security posture, giving you real-time visibility into potential threats and vulnerabilities. This increased visibility and reporting can help organisations make informed decisions and take proactive measures to mitigate security risks.









4. Resilience against risks

By understanding and mitigating security risks, you can minimise system downtime and safeguard your data in the event of a cyber attack. Carrying out your vulnerability management process can also reduce your time to recover from such incidents, minimising the impact on business operations.



What's in a vulnerability management programme?

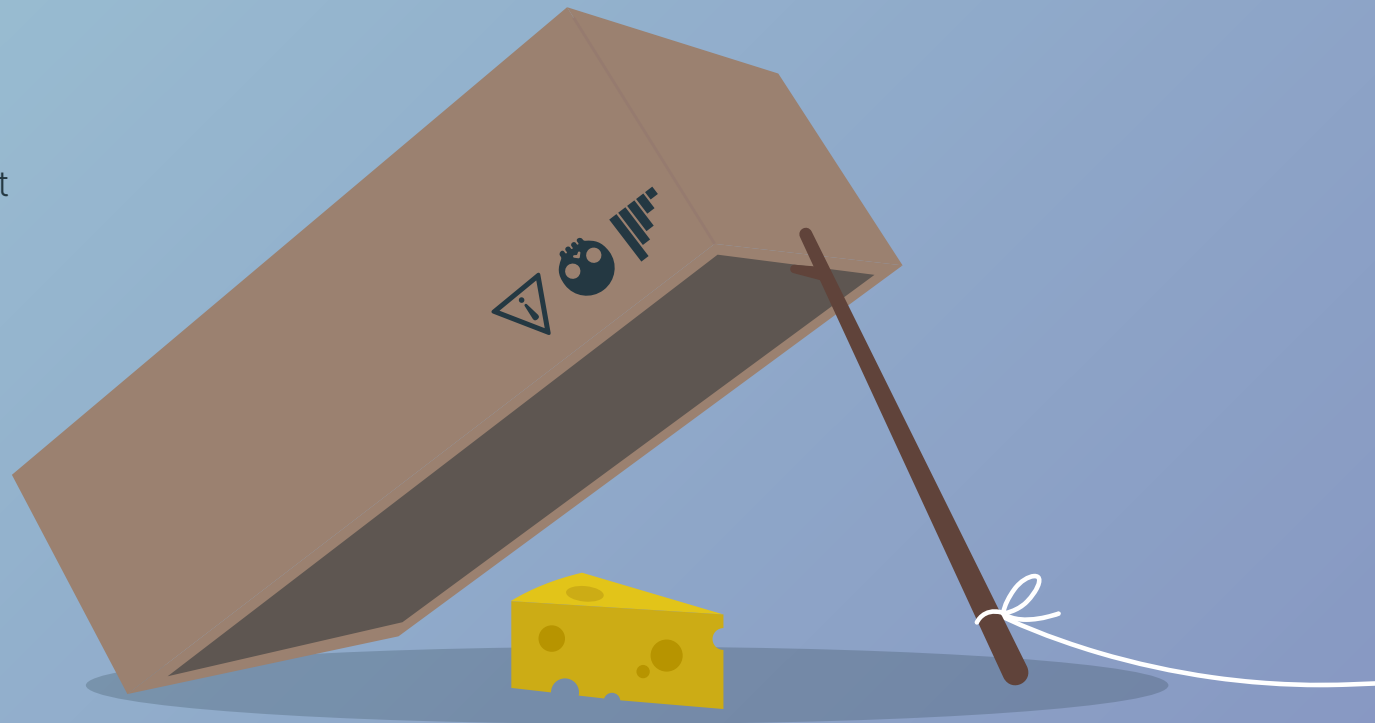
Although specialist vulnerability management tools and solutions exist, you can assemble your vulnerability management programme from the people, processes and technology you have at your disposal. A typical programme would comprise the following components:

	IT ASSET DISCOVERY & INVENTORY	Sometimes known as Attack Surface Management, this activity entails maintaining an up-to-date record of all devices, software, and servers within your digital environment is essential to understand where your risks lie and how you can calculate the success of your programme.
	VULNERABILITY SCANNERS	Vulnerability scanners perform tests against systems and networks, searching for common flaws and weaknesses. These are the most effective when run on a regular basis and when reviewed by experts to verify results, remove any false positives or duplicates, and finally to prioritise the remediations that are needed.
	SIEM (SECURITY INCIDENT & EVENT MANAGEMENT)	SIEM software consolidates an organisation's security information and events in real-time, provides visibility across all digital assets, monitors network traffic, tracks user activity, and identifies unauthorised device connections. By collecting information on indicators of compromise, a SIEM may help indicate that there is a vulnerability.
	PENETRATION TESTING	Penetration testers perform simulated attacks to exploit vulnerabilities and recommend for remediations.
	PATCH MANAGEMENT	Having patch management software helps help you by applying the latest patches automatically across multiple endpoints or systems at once.
	CONFIGURATION MANAGEMENT	Security Configuration Management (SCM) software keeps devices in a secure configuration, tracks changes to device security settings, and ensures that systems are compliant with security policies. SCM tools can scan devices and networks for vulnerabilities, monitor remediation actions, and provide compliance reports.
	THREAT INTELLIGENCE	Threat protection software identifies potential threats, monitors, tracks, and prioritises them for action. These solutions collect data from different sources to indicate security trends and possible security breaches. Threat intelligence can also provide awareness of which vulnerabilities are actively being exploited by threat actors, helping you actively prioritise which vulnerabilities should be remediated first.
	REMEDIATION OF VULNERABILITIES	This process involves prioritising vulnerabilities, developing remediation tickets, identifying the appropriate next steps, and performing remediation tracking to ensure vulnerability or misconfigurations are adequately addressed.

What do vulnerability management tools do?

Vulnerability management tools are designed to identify security gaps across your networks, endpoints, and applications. They search for security vulnerabilities using IP scanners, network and port scanners. Then they assess the risk that those detected vulnerabilities present to the organisation, based on criteria such as the ease and probability of their being exploited by attackers, as well as the value of the IT asset which could be compromised. Many vulnerability management tools then suggest practical remediation measures that need to be taken or automate those remediations themselves.

Buyer beware! Buying a vulnerability management tool is not the same as building and enacting a vulnerability management programme. While there are specialist tools that promise to do it all for you, sadly, additional effort will be required. (Specifically, the time and effort to enact the remediations which will harden your defences and improve your security posture.



How do they calculate risk?

A basic and generic formula is: **Risk = Threat x Probability**

This will be used to calculate a risk score for one vulnerability. Such tools also factor in CVSS score, the location of a vulnerability and the value of the asset it relates to. After you input the assets and score them based on how valuable they are to your organisation. The tool then scans your assets and measures the number of risks or vulnerabilities present across your IT estate, as well as their severity. This is used to calculate an aggregated risk score for your organisation.

Strengths	Limitations
Automated scanning tools discover most basic vulnerabilities fast.	Automated scanners can't discover more complex vulnerabilities that attackers. They cannot detect gaps in physical security or business processes logic which can be exploited.
Dashboards provide a good overview of vulnerabilities at a glance, enabling you to get a real-time understanding of your security posture.	Manual input is always needed, first to configure the tool so it can effectively scan all your assets, and next to verify the results. Verifying the results and removing any duplicates and false positives is essential before the data can be used meaningfully to remediate vulnerabilities. Also, many scanners can't integrate manual verification of the existence of those vulnerabilities.
Scanners categorise vulnerabilities based on the value of the asset to the organisation. Most tools allow you to manually adjust the value of an asset.	Many scanners can't understand the value of an asset to your business, and therefore how an asset (or a specific attack type) will be used in the attack chain.
Some scanners can suggest and even automate remediations for certain vulnerabilities	Some lack the ability to test if that remediation has been effective.
Many scanners have automations and integrations with other tools built in. This means you can easily link them up with other tools used for compliance monitoring (such as PCI DSS for example.)	This cannot be done automatically. Many scanners can't integrate manual verification of the existence of those vulnerabilities. It requires human effort to review the report, map findings to vulnerabilities, and manually input the data into the tool. This can be time-consuming and may introduce human errors during the process.

Vulnerability Management Lifecycle

Whether you are using expensive, specialised tooling or building your vulnerability management programme using what you have already, it should follow the six-phase vulnerability management lifecycle. This serves as a guide, enabling you to make your programme methodical, continuous and repeatable.





PHASE 1: **DISCOVERY**

This stage involves creating an inventory of all the assets across your IT estate and how it is structured, to better understand your attack surface. If you also have a configuration management database (CMDB), this can help map out the interdependencies between these assets.

It is essential to identify, categorise, and evaluate all assets accurately, because you will eventually be placing a risk score next to every asset. As part of this this, you should also identify who in the business is responsible for each asset (and therefore who will be responsible for fixing any vulnerabilities in that asset). Having a full inventory with risk scores next to each will enable you to understand your security posture at a glance. Because your IT estate will change over time, this list will need to be periodically updated.

Begin by conducting vulnerability scans (or contract a third-party security provider to do it for you), to establish a baseline so you know where you are starting from. You can also use the results of any recent security risk assessments or offensive security testing to help calculate your risk scores.



PHASE 2: **PRIORITISATION OF ASSETS**

The aim of this phase is to assess each asset's risk profile, enabling you to identify and mitigate or remediate the most pressing risks first. Assigning a value to each asset based on their importance helps prioritise which assets require more attention, so that you can more efficiently allocate resources.

To gauge the importance of different IT assets, ask yourself, **what are you trying to protect and why?** There are a number of approaches to answering this question:

- Consider where your **sensitive personal data and/or financial data is stored**
- Consider which assets will cause the greatest **disruption to business continuity if they are compromised**
- Consider which assets will cause the greatest **financial risk and cost** to your organisation if they are compromised
- Consider any compliance obligations, such as GDPR, or industry-specific regulations such as HIPAA or PCI DSS
- Consider which assets attackers will use to gain a foothold on your network or escalate their access privileges

Determining which assets are the highest priority will enable you to take a risk-based approach to scanning for vulnerabilities and/or conducting offensive security testing.



PHASE 3: SCANNING AND SECURITY TESTING

Once you have decided which assets to scan and test, you should **identify and evaluate the vulnerabilities present**. You can use automated scanning tools to speed up this process. These will identify potential vulnerabilities and weaknesses across networks and systems. Remember that automated scanners cannot uncover everything, so you will also need the input of penetration testers to uncover what they cannot.

Finding the right tool for the job

Deciding which tools and which kinds of security testing you will use, and how often, will of course be dictated by your budget (for more information on this topic, check out our eBook: ***How to create a bespoke risk-based testing strategy***.) A risk-based approach dictates that you should start with the highest priority and highest risk assets, then expand your coverage over time, with the overall aim of covering your entire IT estate.



PHISHING/SOCIAL ENGINEERING SIMULATIONS



VULNERABILITY SCANNERS



PENETRATION TESTING



CONTINUOUS SECURITY TESTING



RED TEAMING

PURPLE TEAM



WHAT IS IT BEST FOR?

Build the first line of defence

Good for internal infrastructure, but traditionally poor at scanning web applications

Best for external-facing applications and infrastructure

Best for external-facing applications and infrastructure

Only for those with an advanced security posture

Best for testing how your defensive team would respond to a real cyber attack

OBJECTIVES

To identify and measure how resilient your employees are against social engineering attacks, identify which user groups are most susceptible and where additional training is needed.

Identify all possible vulnerabilities that exist in a specific application, system, or scope

Identify all possible vulnerabilities that exist in a specific application, system, or scope; understand these in an organisational context; report on the risk they introduce; define suitable remediations on a continual basis.

Identify all possible vulnerabilities that exist in a specific application, system, or scope; understand these in an organisational context; report on the risk they introduce; define suitable remediations at a single point in time.

Identify weaknesses and strengths in an organisation's security controls; report on the organisation's ability to withstand a targeted real-world attack

Evaluate and report on the effectiveness of your detection and response controls; improve your team's capability to identify and defend against real-world attacks.

OUTCOMES

Targeted training for the most vulnerable user groups.

Present a list of vulnerabilities, ranked by severity and (sometimes) suggest potential remediations.

Remediate vulnerabilities in external infrastructure and applications

Remediate critical vulnerabilities to lower the risk of harm caused by a cyber attack.

Identify weaknesses in your overall ability to withstand real life attacks. Target investment where security controls are not performing

Improve the performance of existing detection and response controls. Invest in controls where there are gaps. Develop training to improve your defensive team's performance.



PHASE 4: REPORTING

Once potential vulnerabilities and misconfigurations have been identified, their risk rating must be evaluated in order to determine how to prioritise your efforts for remediation.

Good, thorough reporting is essential. Expertise is key for this exercise. That means:

- Verifying vulnerabilities
- Removing false positives and duplicates
- **Rank vulnerabilities based on the severity of the risk they present to your organisation, as well as the likelihood of them being exploited.** You can use CVE scores and CVSS scores as guide to understand the severity of the risk, but it is important to factor in your organisation's own unique risk profile, as well as the asset the vulnerability relates to. Document your findings in reports or use those provided by your chosen security provider.

- Writing enough detail in the report so that the owner of the system can effectively fix that vulnerability.

This is essential to create a report which can be used effectively for vulnerability management. All reports must be designed so that you can take action.

Whether you are using your own risk register or a vulnerability management tool, input the findings, and keep them up to date when new reports are delivered. This will enable you to keep track of vulnerability trends across your networks and remain compliant with relevant security standards.

Ensure that all reports are stored securely and can only be accessed by those with admin privileges, so that your reports cannot be used to help someone plan the rest of their cyber attack! (That would be an embarrassing discovery for an incident responder...)



PHASE 5: REMEDIATION

Now you must choose whether to remediate, mitigate, or accept the risks which you have uncovered. Where possible, you should aim to remediate the risk by fixing or patching that vulnerability. However, limited budget and manpower may force you to mitigate the possibility of exploitation or minimise potential damage. Finally, you can choose to accept the vulnerability, although this should only be done when the associated risk is low.

It may seem obvious for a security provider to suggest this but... Just like deciding which assets you will scan and test, **you should remediate the highest priority vulnerabilities first, based on the risk they present to your organisation.** A risk-based approach dictates that you should work from highest to lowest. The risk-based approach is just another way of saying that the purpose of a vulnerability management programme is to enable you to take a methodical and pragmatic approach to allocating resources to mitigating risk.



PHASE 6: VERIFICATION AND MONITORING

Once these vulnerabilities have been remedied or patched, conduct further security testing **to prove that your patches and remediations are effective**. Demonstrating the effectiveness of your remediations is central to running an effective vulnerability management programme.

As well as testing every patch and remediation to ensure their effectiveness at the micro level, you should also monitor the performance of your vulnerability management programme at the macro level. Indeed, such a methodical and comprehensive programme should be designed to allow you to report on the effectiveness of your efforts.

Asset inventory coverage	Overall risk and accepted risk score	Rate of recurrence
Grow your coverage of your IT estate over time. Set time-bound goals for your vulnerability management programme, aiming eventually to include everything.	You can calculate your own risk score, although many vulnerability management tools already do this. Consider how you can reduce your accepted risk as you enact more remediations over time.	Are the same vulnerabilities reoccurring after you have remediated them, or appearing in multiple assets across your estate? Then your remediations aren't effective.
Average vulnerability age/average time to action	Average number of vulnerabilities per asset	Mean time to remediation
A backlog of historic vulnerabilities is likely at the start of your programme. Due to their varying complexity, some vulnerabilities may take longer to fix than others.	This is an imperfect metric for measuring the success of your remediation efforts (which should be focused on the most critical vulnerabilities first), but is useful for reporting on your overall security posture.	This is the king of KPIs (and asset inventory coverage may be the queen). 49 days is the median time it takes organisations to patch vulnerabilities. Aim for lower than that.

How to eat an elephant

Building a vulnerability management programme may be a complex project, but it's not impossible. It requires agreement and alignment from different teams across the organisation. To assemble it all coherently – **the tools, the dashboards, coordinating MSSPs conducting security testing, the reports and monitoring** – requires a dedicated team and effective project management.

Don't expect to be able to do all of this straight away, and don't let the complexity scare you. The value of your achievement will be well worth the effort and you will see incremental positive improvements along the way.

Just remember the age-old wisdom about how you approach eating an elephant: **one bite at a time.**



Why choose us

Claranet Cyber Security is Claranet's dedicated security division committed to helping organisations develop their security posture and build resilience in the face of changing cyber risk. In the never-ending race to keep up with new threats and secure new technologies, we help you make modern happen.

We ask the right questions to uncover the rationale for change behind your security requirements, identifying your business drivers, people and process challenges, and critical threats. This leads us to the solution you really need – something flexible, scalable, and outcome-driven.

Our capabilities span continuous offensive security, SOC-enabled cyber defense, risk consultancy, and training, all of which are underpinned by a 25-year pedigree in penetration testing.



Contact us:
Tel: +44 1924 284 280