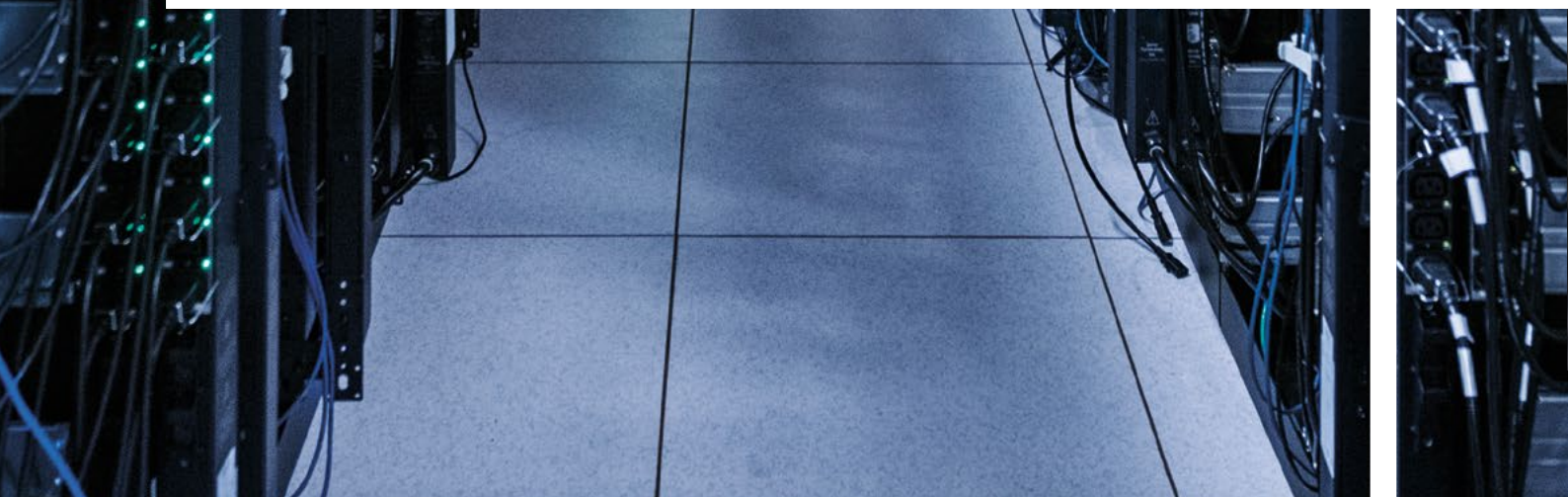
Vulnerability management

Why managing software vulnerabilities is business critical – and how to do it efficiently and effectively

pwc

www.pwc.ch/cybersecurity

Content



1 Introduction

A number of factors are making vulnerability management an increasingly pressing issue. In addition to industry good practice standards such as the NIST Cybersecurity Framework, ISO 27001 and COBIT, which for years have required companies to identify critical vulnerabilities and implement timely remediation measures, various industry regulations are now requiring organisations processing sensitive data such as personal identifiable data (PII), payment cardholder data (PAN) and bank client idendifiable data (CID) to implement risk-based vulnerability management.

Despite the growing awareness, recent cyber and ransomware attacks are proof that many organisations are still failing to address known vulnerabilities with due care and urgency. In the majority of cyber-attacks, it's precisely these vulnerabilities that are exploited to attack corporate and government IT infrastructure.

To fill this gap, regulatory bodies are now requiring corporates that process sensitive data to address vulnerability management. As a result, auditors are also having to verify that organisations are following a risk-based approach and managing vulnerabilities appropriately. But what exactly do 'appropriately' and 'risk based' mean?

As such, as a CISO and compliance officer you should address vulnerability management for IT environments where sensitive data or data with enhanced regulatory requirements are processed in order to remain compliant and to identify and manage your attack surface.

This white paper aims to support an organisation to gain visibility on existing gaps and to manage vulnerabilities in line with industry good practice standards, as well as to comply with financial market regulations such as PCI DSS, Swift, Finance Market Regulation in Switzerland (Finma), Lichtenstein (FMA), Singapore (MAS) and Europe (EBA/GL).

1.1 Vulnerability management scope

Vulnerability management involves far more than merely evaluating, implementing and running a vulnerability scanning tool. Every organisation needs transparency on the known vulnerabilities within its IT assets to manage the risk of the resulting attack surface. This requires a comprehensive set-up with diverse components:

- **IT governance** needs to be in place and mature enough to provide clarity on who's responsible for compliance of the organisation's IT estate and to patch a system within a defined timeframe. If – for whatever reason – this doesn't work or it takes longer than the defined timeframe to patch, compensatory remediation measures must be applied, or the relevant management role must formally accept the residual risk.
- **IT and cyber risk management** helps business and IT leaders understand the potential business impact and take the right actions. When they accept a risk, leaders need to understand the potential threat and the business impact that comes with it.
- **IT service management process integration** is required to integrate vulnerability management in the existing IT service management and IT security management process framework. The focus should be on aligning vulnerability management with IT asset and software life cycle management, monitoring and event management, and incident management. This allows critical vulnerabilities to be handled in due time and if necessary escalated as a security incident.
- **IT and security tool landscape integration** enable vulnerabilities to be assigned to the appropriate peer group, use to be made of orchestration and automation to concentrate on the critical vulnerabilities for the organisation in question, different viewpoints to be consolidated, and the SOC team to be provided with relevant information on the attack surface.

Given these complex and interlocking requirements, many organisations are struggling to bring vulnerability management to the next level – not just to identify vulnerabilities, but also to agree where and within what timeframe remediation measures will be applied and how to handle exceptions where no patch is available or the patch can't be applied.

It's also essential to establish a common understanding of what vulnerability management means for the organisation and what scope it covers. When IT is outsourced, for example, the organisation still needs to take care of vulnerabilities in the outsourced IT environment.

Vulnerability management might have different flavours depending on the organisation's IT footprint. For example, if the organisation develops its own software code or uses partners to develop bespoke software, the scope of vulnerability management might be extended to cover more than just the known and published vulnerabilities for commercial off-the-shelf IT products. Vulnerability management has to cover the entire technology stack, including:

- IT infrastructure: network appliances (switches, routers, load balancers), smart devices (printers, scanners), IoT/OT and building control etc.
- IT platforms: operating systems, databases and storage.
- IT applications: web servers, Java Runtime, middleware and standard tools such as web browsers and Acrobat Reader.

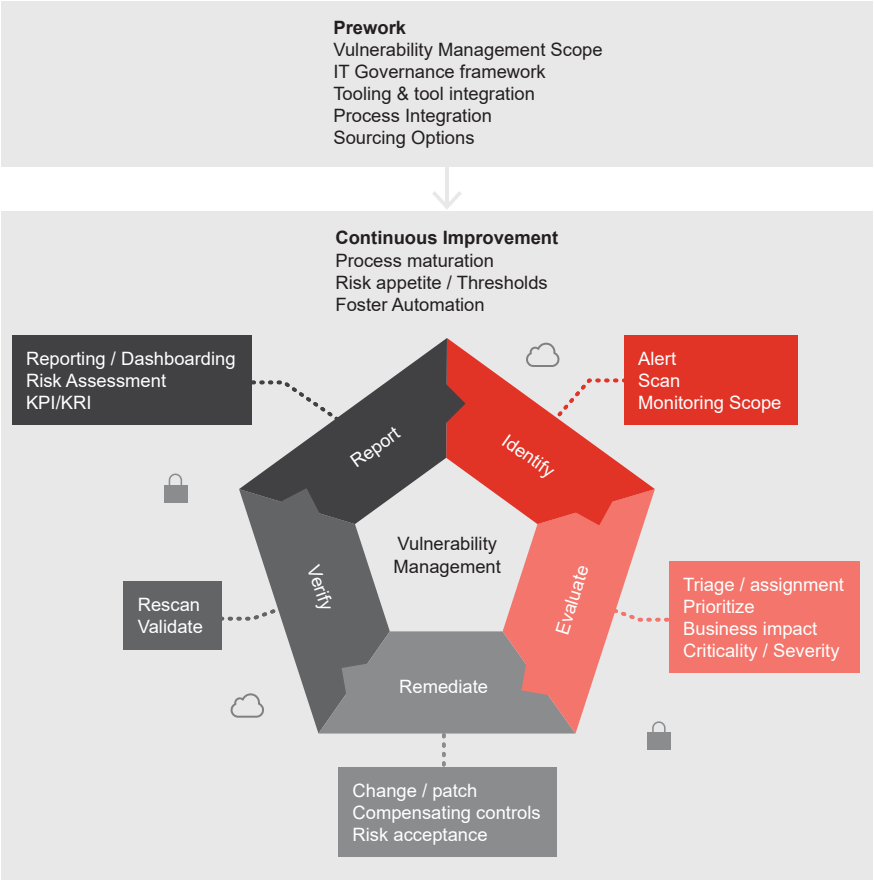
All this means that vulnerability management isn't just an aspect of IT hygiene, but an essential part of IT risk and compliance management, and key to establishing and maintaining trust in IT services. A vulnerability scan verifies whether patches (or other mitigation measures) are applied within the defined timeframe. To apply patches and other remediation measures, change and patch management procedures need to be executed by the relevant teams. The assessment results in an overview of the application landscape and its associated data processing, providing you with a comprehensive picture of your applications, prioritised by operational importance and dependencies (risk based approach). This approach ensures prioritisation of your resources across the organisation's applications, so you can start by addressing the highest risks in relation to data minimisation.

2 Terms and definitions

Term	Definition
CI	Configuration Item
CID	Client Identifiable Data
CMDB	Configuration Management Data Base
COSO	Committee of Sponsoring Organisations of the Treadway Commission (www.coso.org)
IP	Intellectual Property
LOD	Line of Defence in terms of IT governance according to COSO
PAN	Primary Account Number of a debit/credit card
PII	Personal Identifiable Information
SOAR	Security Orchestration, Automation & Response

3 Methodology

Figure 1: The vulnerability management process



1. **Prework:** IT governance as a foundation to identify what IT assets are in scope and to have clearly defined roles and responsibilities to establish and maintain 'compliant data processing'.
2. **Process integration:** Vulnerability management is not a new process, but rather a different angle on IT monitoring, event management and incident response. This includes incident management for handling a critical vulnerability. Consequently, compliance needs to be managed by defining technical standards and systematically monitoring compliance with the IT standards.
3. **Continuous improvement:** Instead of aiming for the 'perfect' solution, start small and quick, and improve over time by expanding scope and fostering automation.

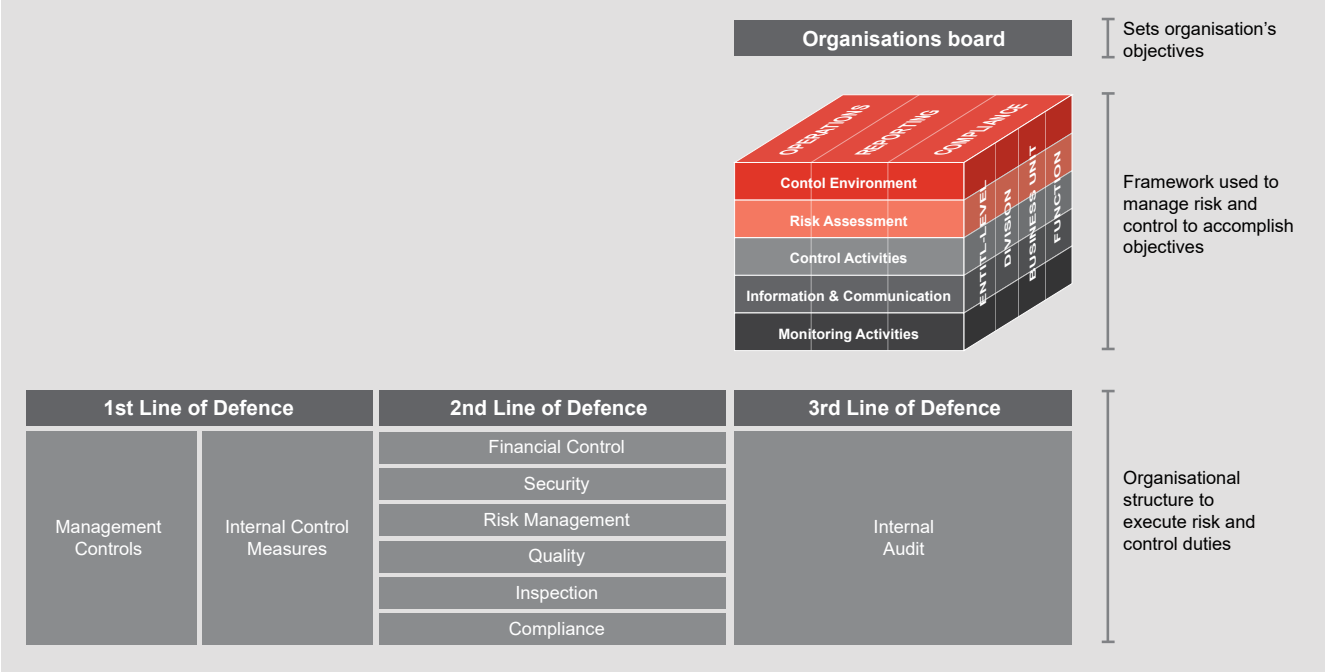
Tooling and tool integration are essential to get the best value and benefit from vulnerability management. For optimum integration, consider combining vulnerability scanning tools with an orchestration solution for seamless integration into the IT service management (IT ticketing) system and the IT asset register/CMDB, and use automation capabilities and playbooks rather than designing workflows in many different tools.

3.1 IT governance and risk management as a foundation

The aim of vulnerability management is to identify known vulnerabilities that would harm the organisation if exploited. Risk management helps to identify the vulnerabilities relevant for the organisation so that it can make best use of the available resources and in a focused way. IT governance according to COSO is a framework for balancing risk and controls to accomplish objectives. COSO therefore introduces the three lines of defence along the following lines:

- Control environment: oversight, structures for authorities, responsibilities and accountability.
- Risk assessment: identifying, assessing and managing risks according to the agreed risk appetite.
- Control activities: implementing and executing controls to comply with regulations and reduce risks to an acceptable level.
- Information and communication: internal/external communication on the objectives.
- Monitoring activities: verifying controls are in place and effective.

Figure 2: The three lines of defence in governance according to COSO



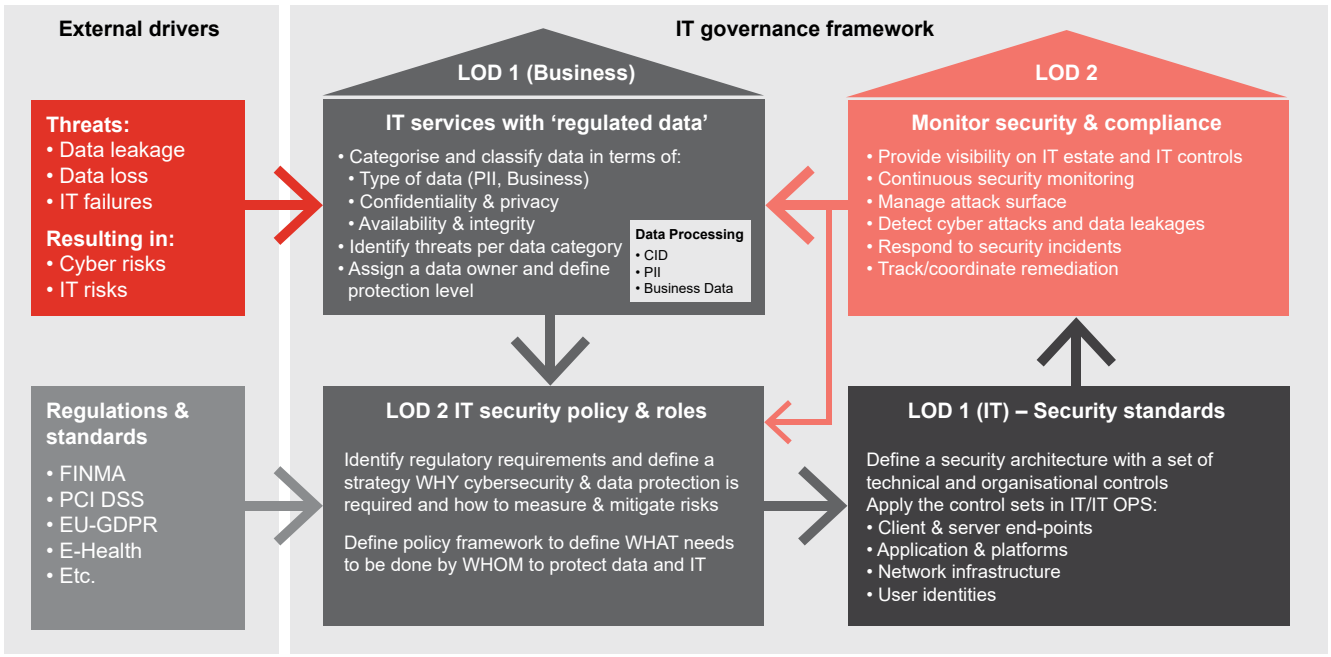
For vulnerability management this means:

- **1st line of defence:**
  - **Management control (LOD1 BU).** The business unit responsible needs to identify data categories processed along the business process, identify applicable laws and regulations to comply with, and bear overall responsibility for compliance.

    The business unit needs to identify whether and which market services process bank client data, PCI cardholder data or SWIFT transactions.
  - **Control measure for IT (LOD1 IT).** Within IT, a dedicated team needs to define the applicable internal control measures for each technology in scope in order to specify the technical standards to comply with the regulatory requirements.

    IT architecture or IT quality assurance defines the set of standard IT products to be used in the IT estate to manage the life cycle and to ensure security patches are applied within a defined timeframe.
- **2nd line of defence (LOD2).** A combination of IT security (defines policy framework and requirements), IT and cyber risk (defines risk metric and methodology) and compliance (helps IT security to translate regulatory, legal and contractual terms into practical requirements for the organisation).
- **3rd line of defence (LOD3).** The internal and external audit, which verifies compliance based on evidence provided and reports deviation from internal and external regulations and standards.

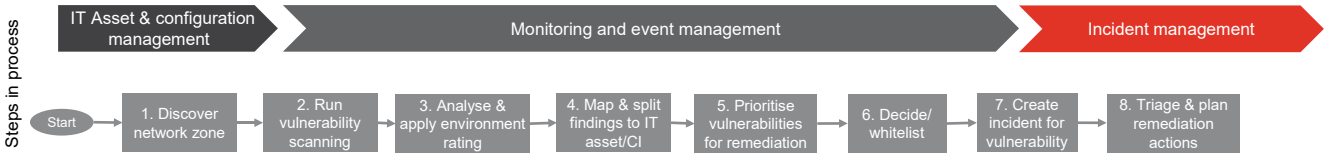
Figure 3: IT and security governance – in a nutshell



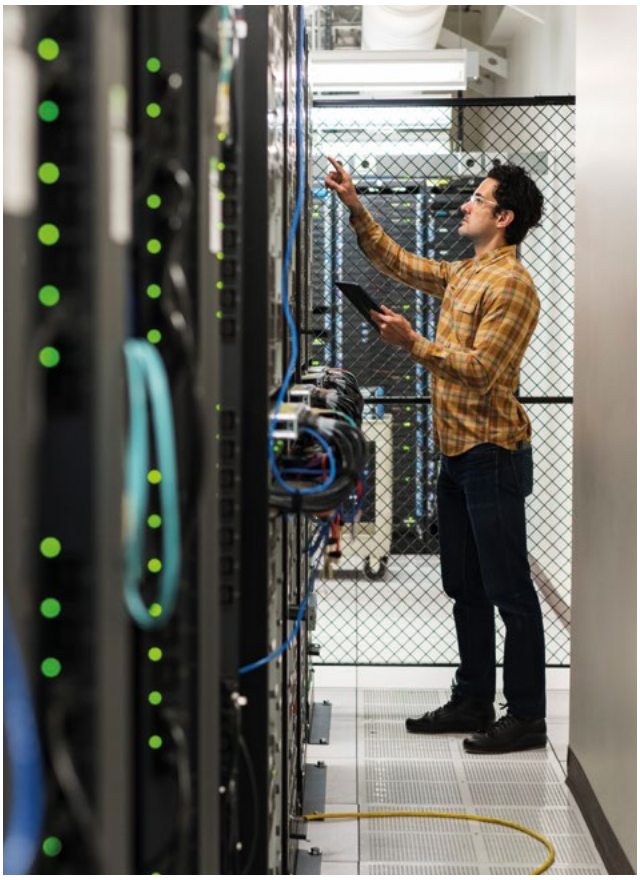
3.2 Process integration

Vulnerability management is not a process on its own. It's a dedicated viewpoint on IT service management and IT security processes.

Figure 4: Process steps of vulnerability management as part of your IT service management process landscape



- **IT asset and configuration management:** In this process the context and scope of vulnerability management are defined. The organisation should start with IT assets where (business) sensitive data and data with enhanced regulatory requirements are processed. This means that clear mapping of IT infrastructure components to IT services is required.
  - If your organisation processes bank client data or PCI cardholder data, it must have an **inventory of IT applications** and application components processing sensitive data.
  - The **IT platform components** (operating system, databases and data storage) and the **IT infrastructure components** (physical data centre, server, storage, firewall and network appliances) underneath the IT application need to be mapped in order to understand what regulatory requirements apply to the IT components. This is usually maintained in a configuration management database (CMDB).
  - The **software packages** used by the organisation should be split into standard SW packages and non-standard SW. For standard SW packages a defined and tested version is provided, and a dedicated operation team is assigned (e.g. Windows Server, Linux Server or Oracle Database). For both standard and non-standard SW, clear responsibilities need to be defined to ensure a process is established to acquire and deploy the latest security patches for all installed SW packages in the organisation.
- **Event management:** On the basis of IT asset discovery and vulnerability scanning, events are created and stored. These events need to be processed in a way that vulnerabilities with potential to cause a high impact to the organisation if exploited are identified. Here the main challenge is to split the identified vulnerabilities between the relevant operation teams and to group them in such a way that a vulnerability can be prioritised in the context of a specific organisation.
- **Incident management:** All events that need a timely reaction must be escalated as a security incident. As an example, the Windows team operating several hundred servers should receive one security incident ticket indicating what server needs to be patched. The ticket should have either a link or information on what vulnerability was discovered and what remediation measures are suggested. Incident management ensures that an incident is processed within a defined timeframe and, if necessary, triaged or escalated to another team or management function.

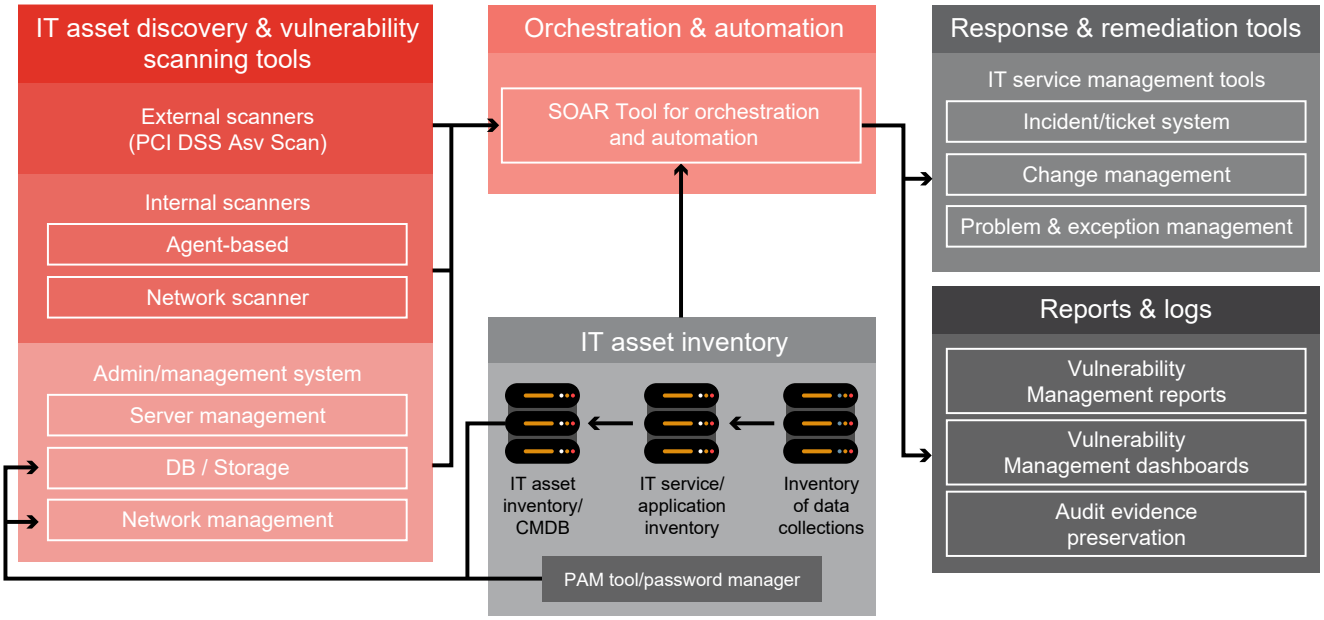


3.3 Tooling and tool integration

Effective and efficient vulnerability management requires an integrated tool landscape. On the basis of our experience, we strongly recommend making use of an orchestration tool rather than trying to integrate each individual security and compliance management tool with the IT service management tools.

The following graphic shows an example of how the relevant tools might be integrated:

Figure 5: Example of architecture building blocks and data flows for vulnerability management



The following building blocks enable optimum integration with the tool landscape and automation of vulnerability management processes:

- **PAM tool:** A privileged access management (PAM) tool allows agentless scanning with credentials, without the credentials of privileged accounts having to be stored in the tool (e.g. CyberArk). This tool is not necessary if agents are used.
- **IT asset inventory**
  - **CMDB:** The CMDB is the (universal) configuration management database, containing all IT assets/ configuration items (CIs) in the system with a unique identifier and a person to contact. This is important to be able to allocate an IP address' vulnerabilities to different support groups (for the operating system, the database and the web application etc.) (e.g. HP ITSM) as an inventory of network segments, the environment rating for each network segment and the IP ranges for each network segment.
  - **Data collections:** This is where the confidentiality rating of the data or IT systems is stored in order to enrich the environment rating with system criticality.
  - **Scanning tool:** Depending on the IT estate an organisation manages, it might be necessary to use more than one scanning tool. Several management suites include functionality to verify whether the managed estate is up to date, or even to roll out the latest patches.
- **SOAR:** This allows the aggregation and enrichment/ grouping of data and is ideally done in a dedicated SOAR tool so that different scanning tools can be combined if needed.
- **Response & remedation tools**
  - **Ticketing tool:** For each vulnerability detected, a security incident is opened and assigned to the corresponding support group. Exceptions can be mapped in the same tool (e.g. as a problem workflow) or in another tool.
  - **Change management tool:** This shows when a patch/update is to be tested and rolled out in the different environments (DEV/TEST/UAT/PROD).

4 Approach

This section describes how the methodology explained in Section 3 is applied to a specific client environment, step by step.

4.1 Step 1: Scope, IT governance and sourcing

The first step is to define the scope, establish the IT governance and select the right sourcing model for the required tools.

- **Scope:** It is best to start with a defined scope where regulatory or contractual provisions require an organisation to implement vulnerability management rather than rolling it out over the entire IT estate. A PII/CID processing application, PCI or SWIFT environment is a good starting point.
- **IT governance:** This is where the roles and responsibilities for defining, implementing and verifying IT security controls are set down. A good way to do this is to define a RACI matrix (see the example below). In this example, the CISO is responsible for defining the requirements and goals. Then the tech teams define how the goals can be achieved, and IT security verifies that time objectives are met. The definitions that need to be covered are as follows:
  - **Patch cycle:** The CISO defines that vulnerabilities that are critical for the organisation in terms of their weighted rating have to be remediated within 10 days, while vulnerabilities rated high need to be remediated within 30 days.
  - **Time objective:** Here it is essential to have a concise definition of what the time objective is and when a timeframe starts. Usually, two options need to be considered, especially for critical vulnerabilities:
    - **Option 1:** The vulnerability is publicly known when a security patch is available.
    - **Option 2:** A vulnerability is communicated either by the CERT team or a vendor mailing list.
  - **Rating of vulnerabilities:** Most vulnerabilities are rated according to a common vulnerability scoring system (CVSS). Versions 2 and 3 are available, and the organisation can also add an environment rating. The definitions of what is 'critical' and 'high' need to be clearly defined for all the parties involved. To avoid miscalculating the criticality of the vulnerability, it's crucial to assess the default CVSS score in relation to the organisation's internal factors (such as network zone, data exposed, business impact and compensating controls in place).
  - **Escalation path:** If everything works as designed, the tech team applies a security patch within the defined patch cycle. Vulnerability management therefore verifies that the time objectives are met and, if not, reminds the tech team to apply the patch. If this is not possible or approved, escalation is initiated.
- **Sourcing for tooling:** If a vulnerability scanning tool is not yet available for all IT environments and IT asset types in scope or is not working as expected, it might be an option to first gather the requirements and map it with the available tool landscape. Many EDR and management tools have vulnerability scanning capabilities integrated already. Besides the evaluation of the appropriate vulnerability scanning tools, it is essential to anticipate that all tools need to be implemented, operated and maintained. As such use of a managed service instead of evaluating and deploying a vulnerability scanning tool might be a good option for your organisation to start quickly.

Table 1: RACI matrix for roles and responsibilities

		LOD 1					LOD 2			LOD 3
Process	Roles / Activities	Security Engineering	Service Owner	IT OPS Team	IT Management	CSIRT	Information Security	CISO	IT Risk	Internal Audit
Prework	Overall responsibility for compliance in terms of data protection and cybersecurity.	C	A	R			C	I	C	
	Overall responsibility for security requirements for IT infrastructure	C	I	I	I		R	A		C
	Maintaining IT Service and application inventory		A	R						
	Defining, planning and implementing measures to counter security vulnerabilities and risks	R	A				C			I
	Defining of Vulnerability KPIs	C			I		R	A	I	
Identify	Operating Vulnerability Scanner	R			A					
	Define / configurate scanning templates	C					R	A		
Evaluate	Analysis, assess vulnerabilities, applying environment rating and deciding on vulnerability rating	C	C	C			R	A	C	
	Analysing and proposing technology-specific remediation measures	R	A			I	C			
Remediate	Applying patches according to the applicable procedure within the defined patch cycle		A	R	I					
	Coordinating remediation action for critical and high vulnerabilities	C	A			R	C			
	Escalating incident if remediation cannot be applied within defined timeframe		A	R			I			
	Deciding how to proceed in the event of escalation	C			A	R	C	A		
	Raising exception if vulnerability is not mitigated within defined timeframe		A/R		A		I		I	
Verify	Track end-to-end Vulnerability Status		I	I	I		R	A	I	
Report	Providing reports (Ad hoc, regularly) including KPIs				I		R	A	I	I

A = Accountable R = Responsible C = Consulted I = Informed

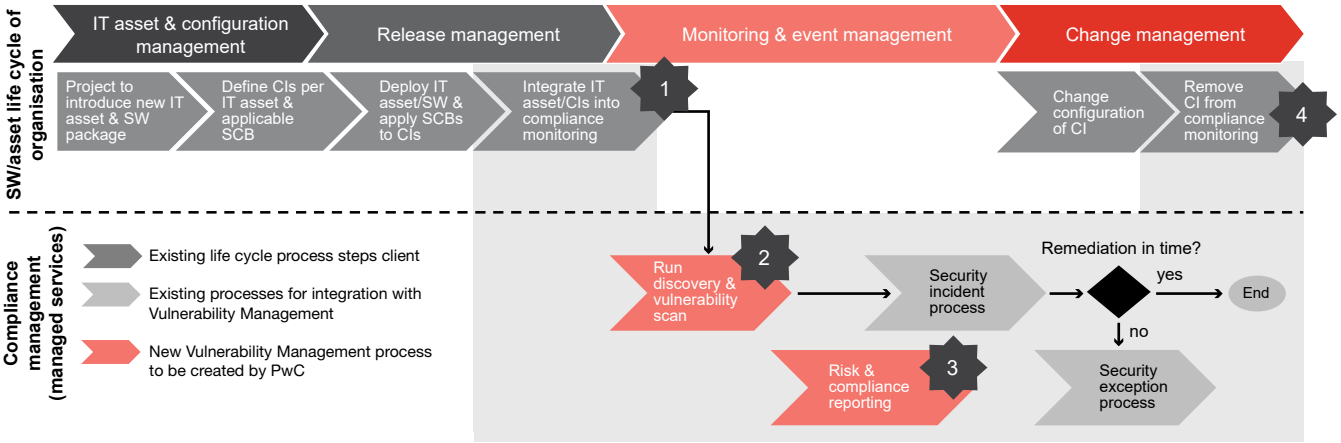
4.2 Step 2: Process integration

Integration into the life cycle of IT assets and software (SW) packages is crucial to the design of the vulnerability management process. This ensures that when an IT asset/software package is deployed, it is formally integrated into compliance monitoring and there is verification that the IT asset fulfils the compliance-relevant security requirements. If the deployment is non-compliant, the unit that initiated the release process is responsible for establishing compliance or approving an exception. After compliance has been established by the project, the operational organisation ensures that compliance is maintained throughout the entire life cycle.

To design the vulnerability management process and align with the existing process framework, we recommend defining use cases, which are triggered by an external event such as:

- A new critical vulnerability is publicly disclosed by a vendor or a national CERT (Computer Emergency Response Team).
- A major SW vendor releases patches (e.g. Microsoft patch Tuesday).
- A new SW/IT asset is introduced in your organisation and needs to be integrated into vulnerability management.
- An IT asset is end of life and is decommissioned.

Figure 6: Example of how the vulnerability management process might be integrated into the ITIL process landscape



We consider the following use cases to be relevant for the vulnerability management process. They should be taken into account in project planning for the introduction of vulnerability management:

1. **Onboard IT asset:** A systematic process (typically release management) ensures that a new IT asset that is put into operation meets the defined security requirements and does not have any vulnerabilities or unnecessary software packages at the time of initial operation.
2. **Discover IT assets in network zone:** The recurring scan (for example weekly, monthly or quarterly) takes place at defined times. For this purpose, the inventory contains a current list of network segments, their risk assessment (for CVSS environment rating) and the IP ranges. An IT asset register or CMDB contains an up-to-date list of the devices expected in a network segment.
3. **Vulnerability scanning:** After the scan is completed, the vulnerabilities are analysed and assessed. To do this, the CVSS score suggested by the vulnerability management system is enriched with an organisation-specific factor on the basis of the network segment and the criticality of the IT system or the data processed with it. In addition to the scan, vulnerabilities can also be submitted for analysis via other sources (PenTest, Vendor Alert, ThreatIntel/OsInt, CSIRT and SOC etc.). A scan is either planned to run periodically such as weekly or executed on specific events. After completion of a scan and the analysis/assessment of the detected vulnerabilities, a report is created. If required, ad-hoc reports can also be created and specific scans can be commissioned.
4. **Decommissioning of the IT asset:** At the end of the life cycle, an IT asset is decommissioned and consequently removed from the compliance monitoring tool.

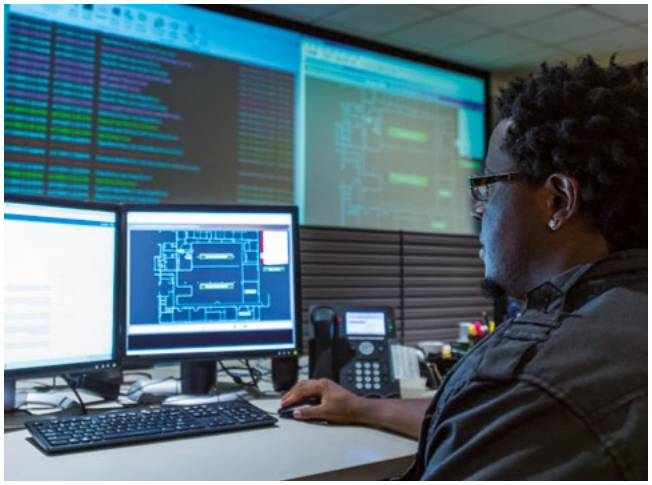
In the design of the vulnerability management process, it's important for assessment and prioritisation, as well as the enrichment of environment-specific parameters of detected vulnerabilities, to take place in one process step. This ensures that a manageable level of relevant vulnerabilities is assigned to the IT organisation for processing.

Depending on the suitability of the security process framework, either a detected and assessed vulnerability can be passed on to the security incident process, or adjustments still have to be made for a new security incident designated as a 'vulnerability'.

It is essential for detected vulnerabilities with a weighted risk rating of 'critical' or 'high' to be handled. For this to happen, an appropriate unit in incident management must regularly track incidents designated as a 'vulnerability' so that they are either triaged to the right units or, if necessary, escalated if no solution is found by the tech teams so that the vulnerability is either eliminated by the next scan, a compensatory measure is taken or an exception is approved by the defined patch standard time objective.

To process the next scan cycle, it's important to be aware of the following questions in advance:

- Should an incident be opened again for a vulnerability that was already recorded in the last scan but is still open?
- Should vulnerabilities lead to an incident in situations where the manufacturer has provided a security patch and this patch is planned in the change management tool but has not yet been applied in all environments?
- How should the different patch cycles/change windows within the IT environment be handled? Do different patch time objectives apply or are exceptions used?
- How long should an exception be valid before a vulnerability that is still open leads to an incident again?
- Is the IT organisation able to meet the time objective for a critical vulnerability (e.g. ten days) for all technologies? How (emergency change)?



4.3 Step 3: Tool integration

As mentioned earlier, vulnerability management requires one or more vulnerability scanning tools, depending on the diversity of the IT landscape. Such tools can be either deployed on premises or acquired on a software-as-a-service (SaaS) basis. Vulnerability scanning can be done:

- with an agent installed on the relevant end point (for servers and clients)
- with a network scanner covering one or several network segments (FW rule needs to allow scanning of multiple network segments if required)
- via a specific management interface to verify that configuration is in accordance with vendor recommendation
- or a combination of the above.

After selecting the right sourcing option for the vulnerability scanner and defining the process landscape for vulnerability management, a solution architecture should be drafted to assign the right tools to the building blocks as defined in Figure 5: Example of architecture building blocks and data flows for integrated vulnerability management. As a result, in the functional building blocks the tools that already exist or are to be acquired are represented together with the anticipated data flows between the tools.

Many vulnerability management tools offer some basic workflow functions to process and triage vulnerabilities. But we suggest integrating the vulnerability scanner into your service management and security operation tool landscape rather than building a new ecosystem to handle vulnerabilities. To do this, we suggest using a security orchestration, automation and response (SOAR) tool for security and compliance monitoring tasks and to gain a consolidated view of your current IT estate – ideally such a tool is already in place in the SOC where the various interfaces can be leveraged.

The advantages of a SOAR versus peer-to-peer integration with all the necessary tools are as follows:

- A SOAR (e.g. Palo Alto Network XSOAR, formally known as Demisto IBM Resilient, Swimlane, or Splunk Phantom) has API integration with most available vulnerability scanners (Qualys, Tenable and Rapid 7 Nexpose) and IT service management tools (ServiceNow, HP ITSM and Remedy etc.).
- A SOAR has built-in playbook templates to adapt and configure for your specific needs. This helps your IT organisation process vulnerabilities by providing the necessary information to the relevant people to decide what to do next or triage to another team.

- A SOAR aims to automate steps in a playbook after humans decide that specific steps do not need to be executed manually and tests have to be done to make sure it works in several iterations.
- A SOAR should provide a ‘single pane of glass’ for security analysts and compliance monitoring by consolidating different views of your IT estate.
- A SOAR allows replacement of a vulnerability scanning tool if it turns out that there are more innovative solutions on the market by merely re-engineering the interface and continuing to use the established playbook. This allows rapid adoption of new technology and tools.
- A SOAR allows you to implement a large portion of the process steps in a tool so that there is accountability on whether steps have been executed and time objectives have been met. This allows you to provide comprehensive reporting and streamline evidence preservation for audits.

Implementing and integrating the process steps into the tools requires a project organisation to roll out vulnerability management and plan the appropriate resources. We suggest a staggered approach where you first onboard the most mature IT platforms. These are usually the operating systems, as these teams are used to receiving and deploying security patches for Windows and Linux systems.

The project organisation needs to enable the technology teams to handle the new vulnerability incidents and support them via ‘early life support’.

Dedicated resources need to be allocated to process the backlog after the first scan. Otherwise, the technology teams are overloaded with old vulnerabilities and get frustrated by the anticipated workload.

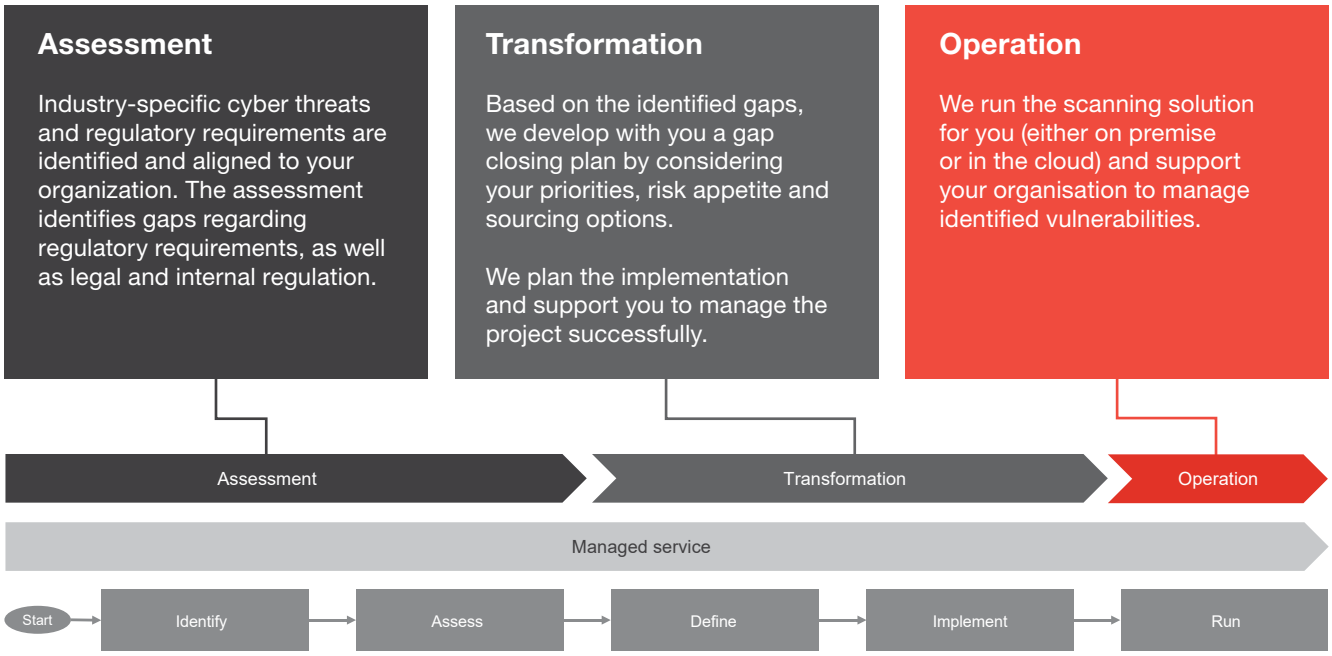
Continuous improvements need to be planned from the beginning to adjust the processes and ratings as needed to generate a digestible workload and to be able to focus on the relevant tasks.

Vulnerability management should also be used to report fact-based data to IT, security and risk management to reprioritise delayed or aborted life cycle projects, and to get rid of legacy infrastructure where no patches are available owing to end-of-support announcements from vendors.

5 How we can support you with vulnerability management

We can support you in three different ways:

Figure 7: PwC's vulnerability management approach



5.1 Assessment

Reviewing your current status by performing a gap analysis.

We recommend analysing the gaps between your current set-up and applicable regulation for you (such as FINMA, PCI DSS, SWIFT) new cyber-risk management requirements and guidelines. This will show what initiatives you have to implement to be compliant, as well as benchmarking your organisation's maturity.

We suggest making a detailed roadmap including priorities for projects and deadlines. To achieve buy-in, it's advisable to submit this roadmap to the executive and board of directors for approval.

5.2 Transformation

We help you define the technical architecture for the tool landscape and the integration of the defined process steps.

A huge part of vulnerability management is remedying the identified vulnerabilities and enhancing the specific solution.

We close the identified gaps and help you comply with the regulatory and security requirements. This includes conceptualising the technical scanning architecture as well as developing and establishing the organisational and procedural requirements for vulnerability scanning.

5.3 Operation

We offer vulnerability management as a managed service. Our Cybersecurity & Privacy team runs the tool either on the client's premises or in the cloud to ensure that recurring scans are carried out.

The managed vulnerability service basically covers:

- scanning IT components
- creating a tailored report
- deriving relevant activities from the scanning report
- triage of remediation tasks to the appropriate OPS team as a security incident.

The following services are also covered:

1. Operation and maintenance/updating vulnerability management tool components and interfaces for a compliance monitoring solution.
2. Running through the discover, analyse, triage and report steps of the defined vulnerability management process so that the vulnerabilities that are relevant for the organisation are identified, evaluated and allotted to the group responsible.

Figure 10: Planned tools mapped to process steps

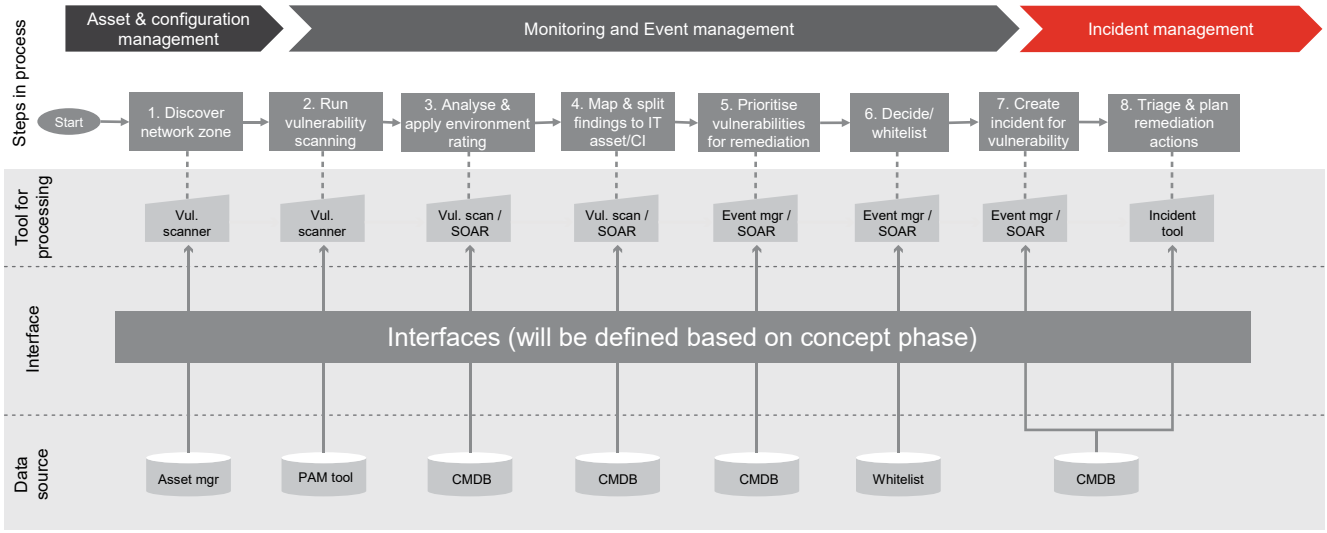
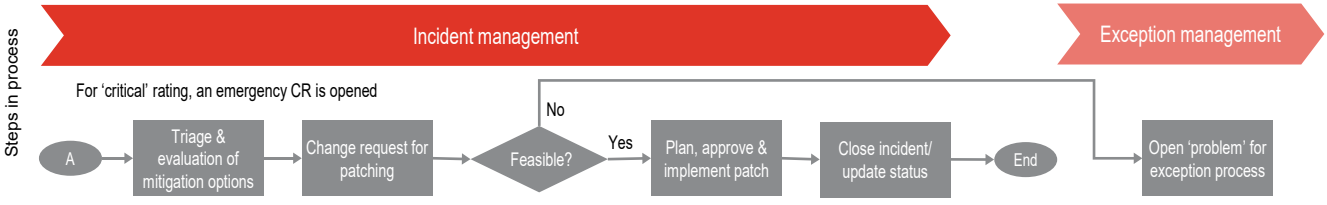


Figure 11: Incident and exception management for relevant vulnerabilities



In the preceding project phases, the tools are set up, configured and integrated into the system landscape.

The OPS team is responsible for operations, maintenance, troubleshooting and continuous improvement and elimination of false positives.

Major customisations and problems are handled in cooperation with professional services at the tool manufacturer.

5.3.1 Identifying relevant vulnerabilities (as-a-service)

The analyst's vulnerability detection tasks are as follows (see Figure 1: The vulnerability management process for more information):

- At defined intervals (e.g. quarterly), the IP ranges defined as scope are discovered for each network segment so that all IPs/devices in the network are listed.
- In the next step, a vulnerability scan is performed for all devices in the network segments.
- The results are processed with automated and manual verifications in such a way that
  - environment-specific criteria are factored in so that the essential vulnerabilities are isolated from the large number of detected vulnerabilities
  - vulnerabilities already being remediated are not reported again
  - the information available from the available inventories is processed.
- Vulnerabilities with a weighted rating of 'critical' are forwarded to the security incident response/CSIRT organisation for coordination and remediation.
- Vulnerabilities with a weighted rating of 'high' for which the patch cycle has already expired are forwarded to the respective IT service/IT asset owner/support team via an incident ticket.
- The vulnerability analyst helps the respective technology teams find a remediation measure acceptable to the organisation (patching and uninstalling the software package etc.).
- Either a change request is opened with the defined remediation measures or an exception process is started.
- For the start of the operational phase, we recommend having the project [team] provide 'early life support' so that the introduction of the new processes is successful and the backlog of older vulnerabilities can be processed systematically.

If required, the analyst can draw on a pool of SMEs.

5.3.2 Support with the elimination of identified vulnerabilities

After the creation and triage of the incident, the back office responsible for vulnerability management regularly checks whether the vulnerabilities have been eliminated within the defined period. For this purpose, the back office employee needs access to the ticket system/change management system in order to track processing.

If no remediation measures can be planned (change request documented) or implemented within the defined period (e.g. 10 days for critical and 30 days for high), the exception process must be started so that the deviation from the security standard and the additional risk are both accepted by the stakeholders responsible.

We provide for monthly scans to be carried out if required to verify that changes reported as completed have actually eliminated the vulnerabilities. If necessary, the service manager initiates escalation.

Summary

As we've seen, vulnerability management isn't just an aspect of IT hygiene, but an essential part of IT risk and compliance management, and key to establishing and maintaining trust in IT services. An effective vulnerability management set-up needs to go further than simply assuring recurring scans of vulnerabilities. It involves the following three aspects:

- process integration
- IT governance
- tooling

Above all, it has to provide an efficient and effective framework to ensure that the results of scans are communicated properly and acted upon by the relevant parts of the organisation, that responsibilities are clearly defined, and that all parts of the system mesh properly to provide the organisation with the desired degree of protection from cyber-attacks via software vulnerabilities. An important part of the process is sourcing the appropriate tools and ensuring that they fit together and into the existing IT set-up.

This is a complex undertaking. The good news is that best practices are available, as well as a choice of modalities to implement the right vulnerability management set-up for any given organisation – a set-up not just matched to its protection needs, but also to its structures, capabilities and resources. A workable solution is within reach. The important thing is to start thinking about it now, be aware of the challenges, and seek expert support if you need it.

For more information please contact our experts

Fabian Faistauer

Director, Cybersecurity
Technology & Transformation
PwC Switzerland

+41 58 792 13 33
fabian.faistauer@pwc.ch

Jannis Louw

Manager, Cybersecurity
Technology & Transformation
PwC Switzerland

+41 58 792 15 92
jannis.louw@pwc.ch

Marius Bleif

Senior Associate, Cybersecurity
Technology & Transformation
PwC Switzerland

+41 79 545 25 38
marius.bleif@pwc.ch

www.pwc.ch/cybersecurity

PwC, Birchstrasse 160, 8050 Zurich, +41 58 792 44 00