WHITE PAPER

Towards a Unifying **Vulnerability Management** Platform for the **Arab Countries**

2023

Executive Summary

As digital transformation accelerates, governments are relying on third parties such as cloud providers, business management and IoT to drive these initiatives. The ease with which non-IT business units adopt new technologies has led to an increase in shadow IT, making it difficult to assess the organization's risks. While third-party products and services can greatly enhance digital marketing, without third-party/supplier risk management, new risks can be more elusive than results. In fact, the rapid development and application of big data, industrial Internet, cloud computing, artificial intelligence, and other new technologies are driving advancements in convergence and ubiquitous digital services, leading to a prosperous digital economy. However, these new technologies also contribute to the increasing complexity of software architectures and the emergence of new attack methods. As a result, our national cyberspaces are exposed to more security vulnerabilities. In the context of frequent cybersecurity incidents, governments are increasingly aware of cybersecurity risks, and vulnerability management has become an important part of their cybersecurity strategies. Additionally, different countries and regions have legislated to manage cybersecurity vulnerabilities.

This white paper addresses a full-view vulnerability management approach for the Arab countries throughout the product lifecycle across the supply chain, in accordance with the five basic vulnerability management principles as well as industry standards and best practices. This is mainly to support the mitigation of risks on the Arab cyberspace. As stated in the Arab Cybersecurity Strategy, the objective of the proposed holistic vulnerability management framework is to create effective cooperation and better cohesiveness between research, enterprise and government to improve the capacity to assess security and assurance properties throughout the product lifecycle. The region's huge market can be seen as an advantage in the development phase, where a product working at the level of society can be rapidly taken to completion. The most important prerequisite for achieving the strategic goal is ensuring functioning cooperation mechanisms between academia, private business and government institutions, which will ensure that strategic priorities will guide the focus of R&D in academia as well as in the private sector, thus ensuring the existence of key competences for the region.

Contents

1 Background

As digital transformation accelerates, governments are relying on third parties such as cloud providers, business management and IoT to drive these initiatives. The ease with which non-IT business units adopt new technologies has led to an increase in shadow IT, making it difficult to assess the organization's risks. While third-party products and services can greatly enhance digital marketing, without third-party/supplier risk management, new risks can be more elusive than results. In fact, the rapid development and application of big data, industrial Internet, cloud computing, artificial intelligence, and other new technologies are driving advancements in convergence and ubiquitous digital services, leading to a prosperous digital economy. However, these new technologies also contribute to the increasing complexity of software architectures and the emergence of new attack methods. As a result, our national cyberspaces are exposed to more security vulnerabilities.

In the context of frequent cybersecurity incidents, governments are increasingly aware of cybersecurity risks, and vulnerability management has become an important part of their cybersecurity strategies. Additionally, different countries and regions have legislated to manage cybersecurity vulnerabilities.

2 Vulnerability Management Is Crucial to Cyberspace Security

Over the last decades, the evolution of ICT has been governed both by computational technology progress (mainly miniaturization) and the growth in applications. In fact, the continuous uptake of the technologies related to those two aspects has strongly affected guidelines on how to report vulnerabilities without fear of legal repercussions.

Responsible vulnerability disclosure is considered a best practice in the cybersecurity community. It helps to balance the interests of security researchers, who aim to improve the security of systems, with the need for organizations to protect their users and data. This collaborative approach contributes to a safer online environment by allowing organizations to address security flaws before they can be exploited by malicious actors.

1. **Vulnerability reduction and mitigation**

   Establish a full-view and end-to-end vulnerability management mechanism throughout the product lifecycle to rapidly detect, investigate, mitigate, and fix vulnerabilities and support customers in risk mitigation.

   Vulnerability planning and mitigation refer to the processes and strategies that organizations employ to identify, assess, and address vulnerabilities in their systems, networks, and applications. The goal is to proactively manage and reduce the risk of security breaches by preventing or minimizing the impact of potential threats. Here's an overview of these concepts:

   - Vulnerability Planning:
     - Identification: Organizations conduct regular vulnerability assessments to identify potential weaknesses in their IT infrastructure. This involves using tools, scanners, and methodologies to discover vulnerabilities such as software flaws, misconfigurations, or outdated components.
     - Prioritization: Once vulnerabilities are identified, they are often prioritized based on factors such as severity, potential impact, and the likelihood of exploitation. This helps organizations focus on addressing the most critical issues first.
     - Documentation: Documenting identified vulnerabilities, their characteristics, and the affected systems is a crucial part of vulnerability

planning. This information aids in developing mitigation strategies and tracking progress over time.

- Vulnerability Mitigation:
    - Patch Management: Keeping software, operating systems, and applications up to date with the latest security patches is a fundamental aspect of vulnerability mitigation. Regularly applying patches helps address known vulnerabilities and enhances overall system security.
    - Configuration Management: Ensuring that systems are configured securely is essential for reducing vulnerabilities. This includes proper access controls, network segmentation, and adherence to security best practices.
    - Security Controls: Implementing security controls, such as firewalls, intrusion detection systems, and antivirus software, helps prevent and detect security threats. These controls contribute to overall vulnerability mitigation.
    - Education and Training: Educating employees and users about security best practices and potential risks can help prevent common vulnerabilities, such as social engineering attacks or unsafe browsing habits.

Incident Response Planning: Having a well-defined incident response plan in place is critical for effectively addressing vulnerabilities in the event of a security incident. This plan outlines the steps to take when multiple sectors of economy as well as citizens' daily lives. Even though it may appear that technologies and services have evolved independently, a close look to several indicators shows that a tight relation exists between a networked computing architecture and the applications that may be implemented on such infrastructures. During this decade, many efforts have been undertaken to develop technologies and promote standards to integrate the services based on these technologies into a converged user experience. This has been associated with the development of convergent networks and ubiquitous computing that are discussed below.

- Convergent networks: Modern networks consist of aggregations of multiple transmission systems in a manner to form a consistent synergy of technical means. Convergence is getting to a multi-layer concept as illustrated by the following definitions:
    - Convergence of transmission media allowing voice, video, and data to be transmitted over the same networks and integrating them into rich services.
    - Access network convergence, for example fixed mobile convergence (FMC), implies that the user is able to access the same services over different access technologies with the same user experience subject to their bandwidth and latency characteristics.
    - Converged device, implying that the user is able to access a wide range of services over different devices with the same user experience subject to device capability.
    - Convergence of information and communication technology is being driven by the reduction in cost and increase in processing power in general purpose microprocessors and the vigorous industry that has been built around it. For instance, optical networking is being used in the IT industry while many consumer electronics devices are integrating radio technology for accessing networks and connecting to other devices.
- Ubiquitous computing: Recently, human-computer interaction has experienced serious changes in the sense that information processing is being done through a simultaneous usage of multiple computational devices and transmission systems. Basically, all ubiquitous computing models rely on small, inexpensive, robust networked processing devices, distributed at all scales throughout everyday life and generally turned to distinctly common-

place ends. Ubiquitous computing is an interdisciplinary field of research and development that utilizes and integrates pervasive, wireless, embedded, wearable and/or mobile technologies to bridge the gaps between the digital and physical worlds.

Considering that affordable, open, and secure access to communication and information services can bring socio-economic benefits, a joint effort should be developed by Arab representative organisations at national and regional levels to promote the development, deployment, and use of new architectures, protocols, and equipment that support the cyberspace security requirements. In fact, the complexity of the national cyberspaces created a new landscape in which vulnerability management plays a key role.

Henceforth, the number of cyberspace security threats has shot up dramatically. Such threats — which can cause major losses — include cyber ransomware and supply chain security incidents. Vulnerability exploitation remains one of the main causes of security incidents. Building end-to-end supply chain vulnerability management throughout the product lifecycle is an important means to reduce risks on live networks and ensure service continuity.

As the digital transformation of industries around the world deepens, cybersecurity attacks are becoming more and more frequent and automated. The presence of high-risk vulnerabilities and security incidents has given rise to the need for legislation and supervision as well as related technology development. The EU, the UK, China, and the US have released laws and regulations to coordinate vulnerability management, recognizing its significance in national cybersecurity strategies.

The maturity of governments vulnerability management directly reflects their digital governance levels and software engineering capabilities — it is also closely linked to sustainable development of the digital economy. Governments must collaborate with stakeholders to continuously manage vulnerabilities. Failure to do so may result in system breakdown, information leakage, and other risks, compromising business assets and reputation and even hindering long-term development.

3 Alignment with the Arab Cybersecurity Strategy

In 2022, the first draft of the Arab Cybersecurity Strategy (ACSS) has been proposed. The actions defined within these work packages allow an efficient implementation of the ACSS vision while taking into consideration the resiliency of the components of the Arab cyberspace, the digital sovereignty of the member states as well as the sustainability of the underlying controls.

Figure 3-1: The Work Packages of the Arab Cybersecurity Strategy.

The ACSS identifies a common methodology for managing cybersecurity risks. This will ensure efficiency and consistency across all organizations and facilitate the exchange of threat and risk information across inter-dependent systems. A methodology based on international standards should be favored as it may reduce costs and yield better interaction with the private sector. The methodology will provide guidance on assigning roles and responsibilities for various aspects of managing risk, such as assessing the threats, valuing assets, implementing and maintaining mitigating measures, and accepting the residual risk. The methodology should include a certification programme to help assess and eventually improve compliance. Importantly, for the procurement and development of infrastructures or services, the risk-management methodology should provide guidance on minimising risk through secure architecture and design and regular assessments/audits, recognising that security is best achieved when it is an integral part of the design, development, and implementation process of a product, process, or service (security by design).

The objective is to create effective cooperation and better cohesiveness between research, enterprise and government to improve the capacity to take developments in universities to applications in private sector and public services. The region's huge market can be seen as an advantage in the incubator phase, where a product working at the level of society can be rapidly taken to completion. The most important prerequisite for achieving the strategic goal is ensuring functioning cooperation mechanisms between academia, private business and government institutions, which will ensure that strategic priorities will guide the focus of R&D in academia as well as in the private sector, thus ensuring the existence of key competences for the region.

The Arab region lacks a uniform R&D plan that deals with information society and cybersecurity and their technical solutions. The next step in light of the ACSS is to establish a coordination mechanism and define the focus areas for R&D in the field of cybersecurity. Based on priority research issues for the region corresponding to them, guidelines can be provided in future for R&D conducted at universities and companies, for providing substance to support measures for companies and educational projects and scholarships.

To enable effective cooperation between public and private sector for productizing novel solutions commissioned by the regional instances, the regulations on handling of intellectual property need to be updated as well, as today they are focused on products and services in the physical space, without taking into account the essential characteristics of digital environment. In the first phase, it is planned to map in more detail today's situation and the range of problems, considering the current procurement and licensing practices at institutions, best practices and regulations in other countries and specific features of cybersecurity solutions. Based on the analysis performed, an integral regional software intellectual property rights strategy can be developed, one that would support the development of Arab software companies and their competitiveness in the world and introduce the necessary legislative amendments to make it possible. The goal is to create the opportunities flexibly and to commercialize the software commissioned by the regional instances in a manner that promotes the development of enterprise so that the intellectual property rights to the software might be held by private enterprises that developed the software and the Arab licenses the right to use it, while the region is guaranteed the possibility of patching and developing the software further for its purposes.

The ACSS also calls for the establishment of information-sharing mechanisms to enable the exchange of actionable intelligence and threat information between and amongst the public and private sectors. Formal and informal information-sharing programmes can help foster effective coordination and consistent, accurate and appropriate communications during incident response and recovery activities; facilitate rapid sharing of threat and intelligence information among affected parties and other stakeholders; help improve the understanding of how and which sectors have been targeted; disseminate information on the methods that can be used to defend and mitigate damage on the affected assets; and ultimately reduce vulnerabilities and exposure along with their attendant risks. The ACSS will identify one or more institutional structures (i.e., competent authorities) responsible for transmitting accurate and actionable information among the national cybersecurity community, including the public and private sectors. Information-sharing should be a two-way process. If governments are willing to share the information they retain, their actions will

demonstrate to private sector entities that the government is indeed a partner in threat information sharing, and help ensure that responders are focused on and better prepared to respond to essential threats.

4 Vulnerability Management Is a Shared Responsibility and Requires Collaboration

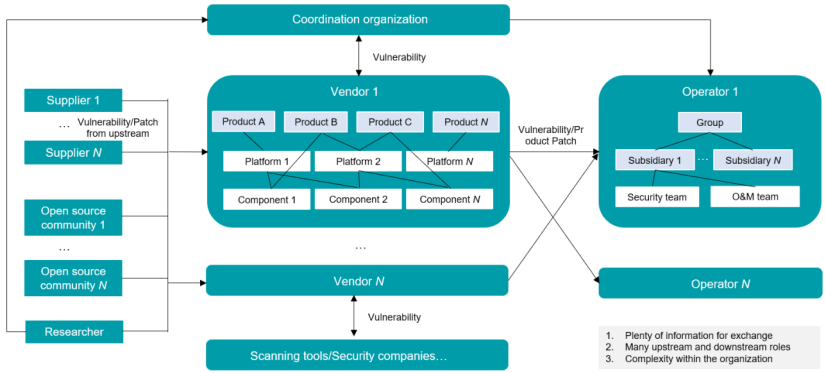
Vulnerability management involves multiple stakeholders across the entire supply chain, for example, suppliers (including open source communities), equipment vendors, carriers, and consumers. It includes vulnerability awareness, verification, remediation, disclosure, and live-network vulnerability risk mitigation throughout the product lifecycle. Ensuring prompt, accurate, and secure exchange of vulnerability information among stakeholders, however, is an industry-wide challenge. The complexity of vulnerability management is further aggravated by large-scale collaborative development of modern software, including software products, platforms, and components, within national cyberspaces.

Vulnerability management requires upstream and downstream collaboration to ensure that all involved parties fulfill their vulnerability management responsibilities. This is to establish a continuous relationship of trust and cooperation throughout the entire supply chain in an open and cooperative manner, enhance trust and capabilities, and collectively mitigate cybersecurity risks arising from vulnerabilities.

Due to the complexity of the vulnerability management process, multiple stakeholders must collaborate to improve the global capabilities in terms of limiting the underlying the cyberattack surface.

- Governments play a complex role in the vulnerability disclosure process. They can act as finders, vendors and coordinators, as well as acquire or maintain vulnerabilities for national security purposes. Governments also develop legislation and regulations that may influence vulnerability disclosure.
- Users of software, hardware and services, and may refer to individuals, organisations or governments.
- Vendors that comprise the developers, manufacturers and suppliers of software, hardware and services. This may also include so-called ‘intermediate vendors’ that make up the supply chain of a specific product or service.
- Finders who make up the community of individuals that identify and report vulnerabilities. Finders are sometimes also referred to as discoverers, reporters or researchers.
- Coordinators are trusted organisations that act as intermediaries between finders and vendors to ensure that vulnerabilities are disclosed and mitigated responsibly.
- Media reports on vulnerabilities and engages in the dissemination of vulnerability information.
- Adversarial actors such as organised criminals or other adversaries may exploit vulnerabilities or engage in the vulnerability disclosure process for nefarious purposes.

Figure 4-1 Collaboration in vulnerability management

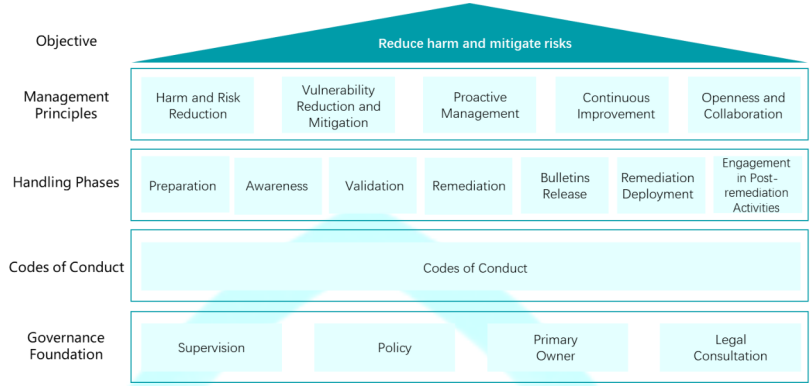


5 Policy and Organizational Framework

Vulnerabilities can arise from a number of factors, including design and engineering flaws, installation errors, inadequate controls or operating procedures, other user errors or changes to the system, and can pose business or environmental threats. In a networked environment, vulnerabilities in popular software, hardware, or services can pose a serious risk to the system and society, and they need to be well controlled and bad to be fixed. Security vulnerabilities that are not detected or disclosed for a long time can further increase these risks and require a process of disclosing the vulnerability.

The key stakeholders mentioned in the foregoing section should create a vulnerability handling process in accordance with this document in order to prepare for investigating and remediating potential vulnerabilities. And it should be periodically assessed to ensure that the process performs as expected and to support process improvements. Vendors should document their vulnerability handling processes in order to ensure that they are repeatable. The following figure is the proposed architecture for vendor vulnerability management.

Figure 5-1 Vulnerability management architecture



The economic impact of vulnerability disclosure refers to the financial and business consequences associated with the process of identifying and reporting security vulnerabilities in software, systems, or networks. Vulnerability disclosure plays a crucial role in the cybersecurity landscape, and its economic implications can be both positive and negative. Here are some aspects to consider:

- Costs of Fixing Vulnerabilities: When security vulnerabilities are responsibly disclosed, companies and organizations need to invest resources in fixing and patching the identified vulnerabilities. This may involve development time, testing, and deployment costs.
- Prevention of Cyber Attacks: Timely and responsible disclosure helps prevent cyber attacks by allowing organizations to address vulnerabilities before they are exploited by malicious actors. The economic benefit here lies in avoiding the potential financial losses and damage to the organization's reputation resulting from a successful cyber attack.
- Reputation and Trust: Rapid and transparent vulnerability disclosure can enhance an organization's reputation for security. This, in turn, can build trust among customers, clients, and partners. The economic impact is often indirect but can influence customer loyalty and business relationships.
- Bug Bounty Programs: Some organizations implement bug bounty programs, where they offer financial rewards to security researchers for responsibly disclosing vulnerabilities. This creates a positive economic incentive for researchers to report issues rather than exploiting them for malicious purposes.
- Regulatory Compliance: In some industries, regulatory requirements mandate the disclosure and mitigation of security vulnerabilities. Non-compliance can result in financial penalties. The economic impact, in this case, is tied to the costs associated with meeting regulatory standards.
- Losses from Exploited Vulnerabilities: On the flip side, if vulnerabilities are not disclosed responsibly, or if they are exploited by malicious actors before being addressed, the economic impact can be severe. This may include financial losses, legal consequences, and damage to the organization's reputation.
- Insurance Considerations: Cybersecurity insurance is becoming more prevalent. The economic impact of vulnerability disclosure may influence insurance premiums and coverage, as organizations that actively manage and disclose vulnerabilities responsibly are often seen as lower risks.

- In summary, the economic impact of vulnerability disclosure involves a complex interplay of costs and benefits. Responsible disclosure practices can contribute to a more secure digital landscape and help organizations avoid potentially devastating financial and reputational consequences associated with cyber threats.

6 Vulnerability Management Objectives

6.1 Holistic vulnerability management

To better support the mitigation of vulnerability risks on live networks of vendors' customers, it is advised to divide vulnerability management objectives into three aspects:

1. **Responsible disclosure**

   According to the industry practice, based on the need-to-know principle, establish a vulnerability disclosure and communication mechanism with customers who purchase vendors' products and solutions to support customers' decision-making on vulnerability risks. Responsible vulnerability disclosure, also known as responsible disclosure or coordinated disclosure, is a process by which security researchers, ethical hackers, or concerned individuals report identified security vulnerabilities to the organization or vendor responsible for the affected system, software, or service. The goal is to give the organization an opportunity to address and fix the vulnerability before it is publicly disclosed or exploited maliciously. Key elements of responsible vulnerability disclosure include:

   - Private Notification: The person discovering the vulnerability privately and confidentially informs the organization or vendor responsible for the software or system. This is often done through a designated contact point, such as a security team or a specific email address.
   - Reasonable Timeframe: The individual reporting the vulnerability typically allows the organization a reasonable amount of time to assess, confirm, and address the issue. The timeframe is usually agreed upon by both parties and can vary depending on the severity of the vulnerability.
   - Collaboration: The process often involves collaboration between the security researcher and the organization. This may include providing additional information about the vulnerability, verifying the effectiveness of the patch or fix, and maintaining communication until the issue is resolved.
   - Non-Disclosure Until Resolution: Responsible disclosure generally entails an agreement not to publicly disclose the vulnerability until the organization has had sufficient time to develop and release a fix. This helps prevent malicious actors from exploiting the vulnerability before a solution is available.
   - Recognition and Rewards: Some organizations implement bug bounty programs or offer recognition to individuals who responsibly disclose vulnerabilities. This provides an incentive for security researchers to report issues rather than exploiting them maliciously.
   - Legal Considerations: Responsible disclosure is often conducted with an understanding of legal considerations. This may include adhering to relevant laws, regulations, and industry norms. Organizations may provide clear guidelines on how to report vulnerabilities without fear of legal repercussions.

   Responsible vulnerability disclosure is considered a best practice in the cybersecurity community. It helps to balance the interests of security researchers, who aim to improve the security of systems, with the need for organizations to protect their users and data. This collaborative approach contributes to a safer online environment by allowing organizations to address security flaws before they can be exploited by malicious actors.

2. **Vulnerability reduction and mitigation**

Establish a full-view and end-to-end vulnerability management mechanism throughout the product lifecycle to rapidly detect, investigate, mitigate, and fix vulnerabilities and support customers in risk mitigation.

Vulnerability planning and mitigation refer to the processes and strategies that organizations employ to identify, assess, and address vulnerabilities in their systems, networks, and applications. The goal is to proactively manage and reduce the risk of security breaches by preventing or minimizing the impact of potential threats. Here's an overview of these concepts:

- Vulnerability Planning:
    - Identification: Organizations conduct regular vulnerability assessments to identify potential weaknesses in their IT infrastructure. This involves using tools, scanners, and methodologies to discover vulnerabilities such as software flaws, misconfigurations, or outdated components.
    - Prioritization: Once vulnerabilities are identified, they are often prioritized based on factors such as severity, potential impact, and the likelihood of exploitation. This helps organizations focus on addressing the most critical issues first.
    - Documentation: Documenting identified vulnerabilities, their characteristics, and the affected systems is a crucial part of vulnerability planning. This information aids in developing mitigation strategies and tracking progress over time.
- Vulnerability Mitigation:
    - Patch Management: Keeping software, operating systems, and applications up to date with the latest security patches is a fundamental aspect of vulnerability mitigation. Regularly applying patches helps address known vulnerabilities and enhances overall system security.
    - Configuration Management: Ensuring that systems are configured securely is essential for reducing vulnerabilities. This includes proper access controls, network segmentation, and adherence to security best practices.
    - Security Controls: Implementing security controls, such as firewalls, intrusion detection systems, and antivirus software, helps prevent and detect security threats. These controls contribute to overall vulnerability mitigation.
    - Education and Training: Educating employees and users about security best practices and potential risks can help prevent common vulnerabilities, such as social engineering attacks or unsafe browsing habits.
    - Incident Response Planning: Having a well-defined incident response plan in place is critical for effectively addressing vulnerabilities in the event of a security incident. This plan outlines the steps to take when a security breach occurs, including containment, eradication, and recovery.
- Continuous Monitoring and Improvement:
    - Continuous Assessment: Security is an ongoing process, and organizations should continuously assess their systems for new vulnerabilities. This involves regularly conducting vulnerability scans, penetration testing, and monitoring for emerging threats.

- Feedback Loops: Establishing feedback loops from incident responses and security incidents helps organizations learn from past experiences and improve their vulnerability planning and mitigation strategies over time.

By incorporating vulnerability planning and mitigation into their cybersecurity practices, Arab Governments can enhance their resilience to potential threats and reduce the likelihood of successful cyberattacks. Regular assessments, proactive measures, and a commitment to ongoing improvement are key elements of an effective vulnerability management program.

3. **Collaborative management**

Organizations specify a collaboration mechanism to mitigate vulnerability risks.

- Collaborative management in vulnerability disclosure refers to the cooperative and coordinated approach taken by security researchers, ethical hackers, and organizations when addressing and resolving security vulnerabilities. This process involves open communication, information sharing, and collaboration to ensure that vulnerabilities are responsibly disclosed and mitigated in a timely manner. The goal is to improve overall cybersecurity while minimizing the risks associated with potential security flaws. Here are key aspects of collaborative management in vulnerability disclosure:
- Open Communication Channels: Establishing open and effective communication channels is crucial. This includes providing clear contact points for security researchers to report vulnerabilities and for organizations to acknowledge and respond to those reports.
- Responsible Disclosure Policies: Organizations often define and publicize their responsible disclosure policies. These policies outline the process for reporting vulnerabilities, the expected timeline for resolution, and any incentives or recognition for security researchers who responsibly disclose issues.
- Coordination of Disclosure Timelines: Coordinating the disclosure timeline is important to ensure that the organization has sufficient time to develop and deploy a fix before the vulnerability is publicly disclosed. This involves mutual agreement between the security researcher and the organization on when the vulnerability details will be made public.
- Collaborative Investigation: Security researchers and organizations may collaborate in investigating the nature and impact of a vulnerability. This collaboration can include sharing technical details, proof-of-concept code, and other relevant information to help the organization understand and address the issue.
- Feedback and Acknowledgment: Organizations should provide timely acknowledgment to the security researchers who report vulnerabilities. Constructive feedback on the quality and relevance of the information provided can contribute to a positive and productive collaboration.
- Bug Bounty Programs: Some organizations implement bug bounty programs as a proactive way to encourage security researchers to discover and report vulnerabilities. These programs offer financial rewards, recognition, or other incentives for responsibly disclosing security issues.
- Community Engagement: Engaging with the broader cybersecurity community is essential. This includes participating in conferences, forums, and industry groups where security researchers and organizations can share insights, best practices, and lessons learned.

- Legal Considerations: Collaborative management takes into account legal considerations, ensuring that the disclosure process adheres to relevant laws and regulations. This may include agreements that protect both the security researcher and the organization during the disclosure process.

By fostering a collaborative environment, organizations can benefit from the expertise of the security community, leading to more effective and efficient vulnerability resolution. Security researchers, in turn, are more likely to engage in responsible disclosure practices when they feel that their efforts are valued and that organizations are committed to addressing security issues.

6.2 Vulnerability Management Principles

Five basic principles are proposed to guide organizations in vulnerability management activities:

1. **Harm and risk reduction**

   The vision for vulnerability management is to reduce the harm and security risks caused by vulnerabilities in vendors' products and services to customers/users. This vision guides the vendors when handling and disclosing vulnerabilities.

2. **Vulnerability reduction and mitigation**

   Although the industry recognizes that vulnerabilities are inevitable, organizations shall strive to: (1) take measures to reduce vulnerabilities in products and services; (2) promptly provide risk mitigations for customers/users once vulnerabilities in products and services are found.

   - Security Controls: Implementing security controls, such as firewalls, intrusion detection/prevention systems, and antivirus solutions, helps prevent and detect security threats. These controls contribute to the mitigation of vulnerabilities.
   - Configuration Management: Ensuring that systems are configured securely is crucial for vulnerability mitigation. This involves following security best practices, limiting unnecessary services, and enforcing the principle of least privilege.
   - Secure Development Practices: Adopting secure coding practices during the software development life cycle helps prevent the introduction of vulnerabilities. This includes code reviews, static analysis, and dynamic testing to identify and eliminate security flaws.
   - Network Segmentation: Segmenting networks can limit the potential impact of a security breach. If an attacker gains access to one segment, the damage can be contained, reducing the overall impact on the organization.
   - User Education and Awareness: Educating employees and users about security best practices can help mitigate vulnerabilities associated with social engineering attacks, phishing attempts, and other user-related risks.
   - Incident Response Planning: Having a well-defined incident response plan is essential for effective vulnerability mitigation. This plan outlines the steps to take in the event of a security incident, including containment, eradication, and recovery.

3. **Proactive management**

   Vulnerability issues shall be resolved through upstream and downstream collaboration in the supply chain. A strategic and systematic approach should be established to identifying, assessing, and mitigating security vulnerabilities before they can be exploited by potential attackers. This approach is crucial for organizations aiming to stay ahead of emerging threats and minimize the risk of security incidents. The stakeholders shall proactively identify and fulfill their responsibilities in vulnerability management and build their management system based on laws, regulations, contracts, and open standards to proactively manage vulnerabilities.

4. **Continuous improvement**

   Cybersecurity is a constantly evolving process where threats and attacks also evolve constantly. As such, defense must be adapted accordingly. Vendors shall continue to learn

from industry standards and best practices in order to drive the maturity of their vulnerability management.

- Monitoring and Assessment: Continuously monitor the organization's systems and networks for new vulnerabilities. This involves ongoing vulnerability scanning, penetration testing, and staying informed about emerging threats.
- Feedback Loops: Establish feedback loops from incident responses and security incidents to continuously improve vulnerability reduction and mitigation strategies. Learning from past experiences helps organizations enhance their security posture over time.

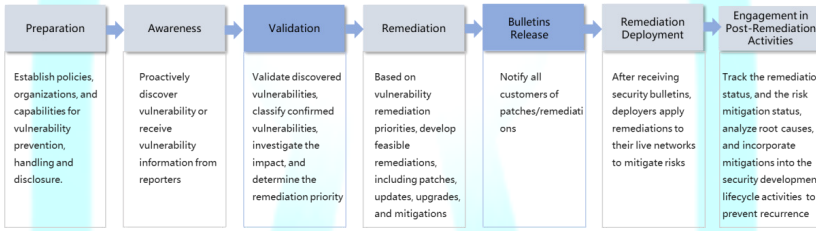
5. **Openness and collaboration**

   The Arab countries should contribute to creating an ecosystem in which all the stakeholders shall continue to adopt an open and cooperative attitude and strengthen the connection with the supply chain and external security ecosystem. They also shall enhance collaboration with stakeholders to build trusted cooperation relationships. The governments should collaborate with external security researchers, industry peers, and relevant communities to share insights, best practices, and threat intelligence. Collaborative efforts can strengthen an organization's ability to address vulnerabilities effectively.

6.3 Key Phases of Vulnerability Handling

Vendors should enhance the security of their products and solutions in order to fully support the secure operations of customers' networks and services. In accordance with ISO/IEC 30111 and ISO/IEC 29147, vendors are suggested to develop a comprehensive vulnerability handling process to safeguard product security. And to jointly address vulnerability risks and challenges, an open, collaborative ecosystem is also required.

Figure 6-1 Seven key phases of vulnerability handling



1. Vulnerability preparation:
   a Develop an effective vulnerability handling process that is transparent to stakeholders, establish organizations to implement the process, present the vulnerability handling framework to stakeholders, and understand the expected behaviors of all parties.
   b Establish and maintain trust relationships with external stakeholders, including but not limited to: (1) complying with industry standards and ensuring information security in the vulnerability handling process; (2) fulfilling commitments.
   c Take measures for vulnerability prevention in product development and build capabilities proactively, so as to ensure product's cybersecurity and resilience.
2. Vulnerability awareness:
   a Establish clear channels to receive reports, including suspected cases, in a smooth and secure manner.

b Confirm vulnerability reports immediately and proactively respond to them.

c Consider all components of a product and their upstream and downstream dependencies of the supply chain in order to better understand the source and impact of vulnerabilities.

3. Vulnerability validation:

a Follow the evidence-based validation principle to check whether vulnerabilities can be exploited. Do not make unsubstantiated assumptions or disseminate unverified information before the validation results are confirmed.

b Build a thorough and comprehensive understanding of verified vulnerabilities in order to better analyze the scope of affected products and services and assist in developing vulnerability mitigations.

c After receiving a vulnerability report, maintain clear communication with the reporter during vulnerability validation to ensure the reporter is aware of the internal progress, and agree on a timeline to avoid any single-point communication failure, so as to prevent irresponsible disclosure by the vulnerability reporter from causing harm to customers.

4. Vulnerability remediation:

a A severity rating for each vulnerability should be assessed to help users assess risk in a faster and more programmatic manner. Existing systems such as the Common Vulnerability Scoring System (CVSS) should be considered during such assessment, but other systems — including self-developed ones — can also be used. A severity rating system should be documented.

b Organizations involved in vulnerability remediation shall respond based on the vulnerability severity and the attack possibility to ensure that the most serious issues are given the highest priorities.

c The vulnerability discovery and remediation processes are dynamic. Therefore, organizations shall reduce vulnerabilities before product release and mitigate known vulnerabilities in the lifecycle phase after product release.

d Organizations involved in vulnerability remediation shall identify and adhere to their responsibilities, including those specified in laws, regulations, contracts, and industry standards, to ensure compliance and dutifulness during vulnerability remediation.

e Organizations shall take feasible measures to minimize the exposure of risks to customers/users during vulnerability remediation.

5. Bulletins release:

a Disclosure organizations shall make feasible efforts to accurately disclose the vulnerabilities only to affected stakeholders with permission control in order to reduce risks.

b Disclosure organizations shall understand that vulnerability disclosure may expose other internal and external organizations affected by the vulnerability to risks. Therefore, they shall ensure thorough coordination with internal teams (of platforms, components, modules, and products) and external parties (vendors, upstream and downstream participants of the supply chain, and the security ecosystem) and negotiate a disclosure timeline.

c Consolidated internal and external coordination during vulnerability disclosure shall aim to reduce harm that may result from vulnerability disclosure and avoid incidents incurred by insufficient collaboration.

d Each disclosure organization shall establish a transparent vulnerability disclosure framework oriented to key stakeholders (customers/users) and disclose known vulnerabilities in a timely and responsible manner based on the framework.

6. Remediation deployment:
    a Deployment organizations shall proactively use security bulletins and communication channels to encourage customers/users to promptly manage patches, including accepting patch suggestions and updating software and hardware components.
    b Deployment organizations shall adopt process and technological means to encourage customers/users to take note of security bulletins and enable the security update function in order to find out about known vulnerabilities and mitigate their risks.
7. Engagement in post-remediation activities:
    a Optimize security activities and improve security engineering based on the review and root cause analysis of known vulnerabilities, so as to minimize possible vulnerabilities in the future.
    b Perform end-to-end measurement on the vulnerability handling process to analyze the effectiveness of the process and make continuous improvement.
    c Continuously foster and raise security awareness among all employees, and help increase the awareness of peer stakeholders during communication, thus driving the security awareness and capability enhancement of the entire industry chain.

6.4 Codes of Conduct for Vulnerability Management

To guide governments more effectively in terms of vulnerability management activities, the following codes of conduct are proposed for vendors regarding key activities in the vulnerability handling process:

1. In the vulnerability handling preparation phase, establish vulnerability handling organizations and processes, specify handling objectives, and establish external communication channels. Researchers should provide detailed information about the vulnerability, its impact, and potential mitigation measures in a manner that is understandable to the organization and its stakeholders.
2. In the vulnerability awareness phase, establish extensive internal and external channels to collect all vulnerability information related to vendors' products, in order to verify and fix vulnerabilities promptly.
3. In the vulnerability validation phase, verify the impact of perceived vulnerabilities on product versions within the lifecycle, and maintain continuous and clear communication with vulnerability reporters. Researchers should conduct their testing in a non-destructive manner. Avoid actions that could harm the organization's systems, disrupt services, or cause data loss.
4. In the vulnerability remediation phase, take proactive actions to mitigate and fix vulnerabilities. In addition, address all vulnerabilities based on their severity and other factors to ensure that they are properly handled.
5. In the security bulletin release phase, disclose vulnerability information only to affected stakeholders, through proper internal and external collaboration. Researchers should refrain from exploiting vulnerabilities for personal gain, malicious purposes, or any activities that could harm individuals or organizations.
6. In the remediation deployment phase, deploy or help customers deploy remediations, proactively communicate with customers about high-risk vulnerabilities, and encourage customers to actively manage patches and stay updated on security bulletins so that they can detect and mitigate vulnerabilities promptly.
7. During engagement in post-remediation activities, product teams should analyze the root causes of vulnerabilities to improve security activities. In addition, product teams should continuously foster and raise security awareness and capabilities among all employees through external communication and through collaboration between upstream and downstream stakeholders in the industry chain. Researchers should engage in continuous learning and improvement, staying informed about evolving cybersecurity best practices, and contributing positively to the cybersecurity community.

6.5 Governance Foundation

The implementation of the Arab vulnerability management platform requires a governance model which enables timely and efficient information sharing. The pillars of this governance model are highlighted below:

1. Supervision

   Vendors should demonstrate leadership and commitment with respect to vulnerability handling by:

   a Establishing a reasonable supervision responsibility system;

   b Creating an overall environment for achieving supervision objectives, for example, establishing a reward and accountability mechanism to ensure that the process is effectively executed;

   c Publicizing and conveying the requirements on vulnerability management, ensuring a wide understanding, and establishing effective feedback channels.

2. Policy

   Vendors should establish a sustainable and trusted vulnerability management system in terms of policies, organizations, processes, technologies, and specifications, and collaborate with external stakeholders to jointly address vulnerability challenges.

3. Primary owner

   Vendors should assign primary owners who take the responsibilities and authority for roles relevant to vulnerability handling. Primary owners should ensure that the vulnerability handling process is correctly executed and the process performance is continuously analyzed and improved.

4. Legal consultation

   Vendors shall have proposed vulnerability remediations and communications reviewed in terms of legality to ensure compliance with internal policies, laws, and existing contracts.

7 Vulnerability Management Practice

A holistic vulnerability management is proposed for the Arab governments as a comprehensive and strategic approach to identifying, assessing, prioritizing, and mitigating security vulnerabilities across an organization's entire IT infrastructure. This approach goes beyond simple vulnerability scanning and patching and involves integrating security practices into various aspects of an organization's processes. The goal is to create a proactive and adaptive security posture that addresses vulnerabilities across people, processes, and technology. Here are key components of holistic vulnerability management:

- Continuous Assessment: Regularly and systematically scan and assess the organization's entire IT environment for vulnerabilities. This includes networks, applications, systems, and other assets. Continuous monitoring allows for the identification of new vulnerabilities and ensures that the security posture remains up-to-date.
- Risk Prioritization: Prioritize vulnerabilities based on factors such as severity, exploitability, and potential impact on the organization. This risk-based approach helps focus resources on addressing the most critical vulnerabilities first.
- Asset Management: Maintain an accurate and up-to-date inventory of all assets within the organization. This includes hardware, software, applications, and other elements. Effective asset management ensures that vulnerabilities are not overlooked, and all systems are accounted for in the vulnerability management process.
- Patch Management: Develop and implement a robust patch management process to promptly address and remediate identified vulnerabilities. This involves testing patches,

prioritizing deployment based on criticality, and ensuring minimal downtime during the patching process.

- Configuration Management: Enforce secure configurations for systems and applications. Misconfigurations can often lead to vulnerabilities, so maintaining a secure baseline and regularly auditing configurations are essential components of holistic vulnerability management.
- Security Training and Awareness: Educate employees and stakeholders about security best practices, the importance of reporting vulnerabilities, and how to use technology securely. A well-informed workforce is a critical component of a holistic approach to vulnerability management.
- Incident Response Planning: Have a well-defined incident response plan in place to respond promptly and effectively when vulnerabilities are exploited or security incidents occur. This plan should outline the steps for detection, containment, eradication, recovery, and lessons learned.
- Collaboration and Communication: Foster collaboration between different teams within the organization, including IT, security, and development teams. Open communication channels between security researchers, vendors, and internal teams contribute to a more effective vulnerability management process.
- Third-Party and Supply Chain Security: Extend vulnerability management practices to third-party vendors and supply chain partners. Assess the security posture of third-party components and ensure they align with the organization's security standards.
- Compliance and Reporting: Align vulnerability management practices with industry regulations and compliance requirements. Regularly report on the status of vulnerabilities, remediation efforts, and overall security posture to relevant stakeholders.

By integrating these elements into a cohesive strategy, the Arab countries can create a resilient and proactive approach to managing vulnerabilities, reducing the risk of security incidents, and improving overall cybersecurity posture.

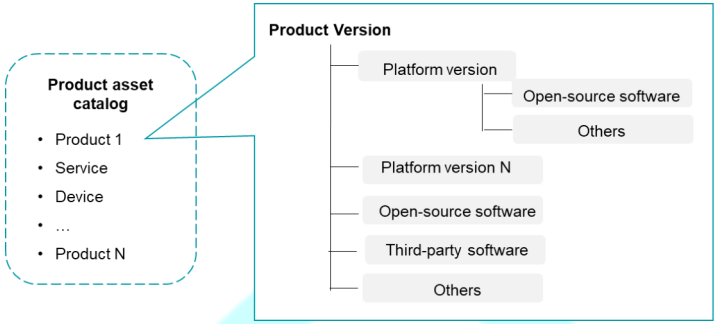
7.1 Product Asset Management

Asset management is the basis of vulnerability management, yet it is an industrywide challenge to ensure the integrity and accuracy of asset information. Furthermore, for the vendor encompassing different types of assets, it is challenging to produce a comprehensive and up-to-date list of assets. In addition, identifying precise information about open-source and third-party software in assets is a common industry challenge.

When a product charter is initiated, assets must be registered to ensure that the asset list is managed from the very beginning. During development, software engineering capabilities (such as full source code build) are set up to ensure that the sources of assets in use (including platforms, open-source software, and third-party software) are managed.

A full picture of vulnerabilities in product versions can be drawn based on all available software asset information. This is helpful for vulnerability verification, remediation, and other management activities.

Figure 7-1 Product Asset Management



7.2 Vulnerability Management Throughout Product Lifecycle

Vendors should adhere to the concept of "building security in design, processes, and operations" throughout the product lifecycle. They should establish processes to ensure that cybersecurity assurance measures are effectively implemented in each phase to improve product security competitiveness.

Vulnerabilities are managed based on product/software version lifecycle milestones. Specifically, vendors should manage vulnerabilities in all product versions yet to reach the End of Service and Support (EOS) and release vulnerability remediations (including mitigation measures, patches, and versions) for versions yet to reach the End of Full Service (EOFS) based on remediation policies in different lifecycle phases to help customers mitigate vulnerability risks on live networks.

7.3 Supply Chain Management

Vulnerabilities in upstream supply chain dependencies can also affect vendors' products and services. Vendors should track all upstream dependencies and vulnerabilities to determine if their products or services are affected. And they should obtain vulnerability information, including remediation advice, from their upstream vendors. In addition, vendors should provide vulnerability information, including remediation advice, to their downstream customers and users. Different roles should be aware of the importance of collaborative supply chain management from different perspectives.

1. As a supplier, a vendor should establish a channel for prompt and accurate vulnerability awareness. Generally, it also needs to develop a vulnerability disclosure website and a proactive communication channel for downstream equipment vendors/integrators, and continuously provides vulnerability remediations to support them in integrating and releasing remediations.
2. As an equipment vendor, it should establish a vulnerability receiving, disclosure, collaboration, and response mechanism with suppliers. In addition, it should operate bug bounty programs to encourage security researchers and organizations to report suspected vulnerabilities in products. It should establish a vulnerability disclosure website and a proactive communication channel to disclose vulnerabilities to customers in Security Advisories (SAs), Security Notices (SNs), and Release Notes (RNs) and support customers in making informed decisions and mitigating vulnerability risks on live networks.
3. As an operator, it should establish a vulnerability receiving, disclosure, collaboration, and response mechanism with equipment vendors and service providers. On the basis of live-network asset management, it needs to perform vulnerability awareness, assessment, remediation, and other activities to control live-network vulnerability risks at an acceptable level.

7.4 Vulnerability Management Platform

To ensure that the key stakeholders fulfill their responsibilities and support customers in vulnerability risk mitigation, organizations should establish a unified vulnerability management platform. This platform collects original data from the vulnerability management activities of the digital assets deployed across the national cyberspaces and generates a full picture of the vulnerability management levels and responsibility fulfillment status of the key stakeholders, enabling visualized and manageable vulnerability management results of the vulnerability management process.

7.5 Bug Bounty Programs

The relationship between discoverers and vendors has evolved over time, but remains complex due to their different objectives and interests. As such, they also often have distinct opinions on the severity of a vulnerability and the necessity to inform the public, as well as how fast this should be done, if at all. One of the main developments in bringing vendors and discoverers closer is the introduction of bug bounty programs, which have become commonplace. A bug bounty program rewards a reporter for discovering and then reporting vulnerabilities.

8 Vulnerability Management Maturity Model (VM3)

In the increasingly complex external environment, governments pay more attention to cybersecurity risks and have higher requirements on product vulnerability management capabilities. Against this backdrop, a vulnerability management maturity model is proposed to help the industry evaluate the E2E vulnerability management maturity, identify gaps, and continuously improve its vulnerability management capabilities.

This model is applicable to complex ecosystems and different product portfolios across domains, and is used to collate other excellent maturity model standards and best practices of leading stakeholders contributing to the protection of the cyberspace. It consists of seven phases: preparation; development; vulnerability identification; vulnerability analysis, verification and remediation; vulnerability disclosure; vulnerability remediation deployment; and vulnerability remediation participation. In each phase, the model is broken down into different focus areas and points.

1. Features of Vulnerability Management Maturity Model
   (1) Extensive versatility:
      a This model is applicable to different countries/governments, enterprises/company, carriers, suppliers, and more.
      b It covers different product types, including devices, IoT terminals, chips, ICT products, and cloud services.
   (2) Greater breadth and depth:
      a This model is built on Intel's PSMM and SANS VMMM models.
      b It expands with additional domains and indicators.
      c It also incorporates reputable international standards, including the standards of the PSIRT SIG, BSIMM, SAMM, CMMI, CMMC from Carnegie Mellon University, and CMM of the University of Oxford.
   (3) Unified language:
      a This model uses a unified language that can be applied across different industries and products. This means that users can use the maturity model without being restricted by their specific industries and products.

      Therefore, the Vulnerability Management Maturity Model **provides a uniform guidebook for vendors to follow**.

2. Seven Phases of the Vulnerability Management Maturity Model

The vulnerability management maturity model consists of seven phases: ***preparation; development; vulnerability identification; vulnerability analysis, verification and remediation; vulnerability disclosure; vulnerability remediation deployment; and vulnerability remediation participation***. In each phase, the model is broken down into different focus areas and points.

Table 8-1 Focus points in different phases.

Vulnerability management Phase	Domain Area	No.	Focus Points
1. Preparation	Policy, Standard and Process	1.01	Policy & Standards
		1.02	Process
	Stakeholder Ecosystem Management	1.03	Internal Stakeholders
		1.04	External stakeholders
	Resources	1.05	Vulnerability Management Tools & Resources
		1.06	Training
	Vulnerability prevention in Product Development	1.07	Secure Product Development Lifecycle
		1.08	Product risk assessment
		1.09	Threat Modeling
		1.10	3rd party and Open source components Security & Vulnerability Management
		1.11	Architecture Design in Vulnerability Prevention System
		1.12	Security Requirements
		1.13	Coding security standards and security practices
		1.14	Vulnerability Scanning and Quality Gate
2. Vulnerability Awareness	Internal Automated	2.1	Vulnerability automation test tools used
		2.2	Vulnerability automation test requirement & configuration
		2.3	Vulnerability automation test Reporting and visibility
	Internal Manual	2.4	Vulnerability Test and Review
		2.5	Internal Bug Bounty
	External Source	2.6	Intake of Reporting

		2.7	Monitoring for Product Component Vulnerabilities
		2.8	External Bug Bounty
3.Vulnerability Validation	Vulnerability Analysis & Validation	3.1	Vulnerability Analysis and Validation
		3.2	Vulnerability Priority
		3.3	Risk Management Process
		3.4	Root Cause Analysis
	Vulnerability Investigation	3.5	Triage and maintain issues, Vulnerability Reproduction
4.Vulnerability Remediation	Remediation & Verification	4.1	Remedy Resolution
		4.2	Verification and Delivery
5.Vulnerability Bulletins Release	Vulnerability Notification	5.1	Vulnerability Notification
	Coordination	5.2	Coordination
	Vulnerability Disclosure	5.3	Vulnerability Disclosure
6.Deploying Vulnerability Remediation (Self-operating business)	Change Management	6.1	Change Management
	Patch Management	6.2	Patches Delivery Method and cadence
	Configuration Management	6.3	Configuration Requirements and Technologies
7. Engagement in post-remediation activities	Customer Follow up & Feedback	7.1	Customer follow up & feedback
	Product Security Incident Operation & Effectiveness	7.2	PSIRT service coverage on different products
		7.3	Operation & Effectiveness
	Lessons Learned	7.4	Review, Retrospective and improvement

3. Five Maturity Levels of Every Focus

Each focus is categorized into five maturity levels.

Level 1: Initial

Level 2: Managed

Level 3: Defined

Level 4: Quantitatively Managed

Level 5: Optimizing

(1) Initial

- No formal vulnerability management policy or standard, and roles and responsibilities not clearly defined
- Undefined risk threat model
- Security review of fragmented architecture design

- Lack of vulnerability scanning and quality check
- Lack of automated and manual vulnerability test
- No internal or external bug bounty program
- No document for internal audit and review of vulnerability management processes

(2) Managed

- Roles and responsibilities defined but not communicated
- Limited number of security and vulnerability-related training sessions provided
- A secure development lifecycle partially defined and adopted
- Vulnerabilities manually identified based on input from technical vendors and general security advice
- Automated vulnerability scanning and verification at least once prior to release
- Documents defining the internal and external bug bounty programs
- Documents defining internal audit and review of vulnerability management processes within the organization

(3) Defined

- Vulnerability management policies and standards, roles and responsibilities clearly defined
- Role-based training, covering security and vulnerability management
- Identification of vulnerabilities and manual prioritizing of vulnerabilities using automated scanners
- Defined risk and threat models and formal security review before release
- Automated test results visible to all relevant team members
- Internal and external bug bounty programs based on industry best practices or international standards
- Review of time to recovery, completeness, and effectiveness

(4) Quantitatively Managed

- Vulnerability management policies and standards, roles and responsibilities clearly defined and well communicated
- Training on technologies, communication, processes and tools in place
- Security product development lifecycle, including security review, automated security access, and measurement criteria for new vulnerabilities in development
- Development team with a security leader who is responsible for reviewing security requirements and results
- Relationships established with researchers who escalate vulnerabilities to enhance communication and data sharing regarding vulnerability management
- At least annual review and update of the response process; assessment of overall vulnerability management improvements

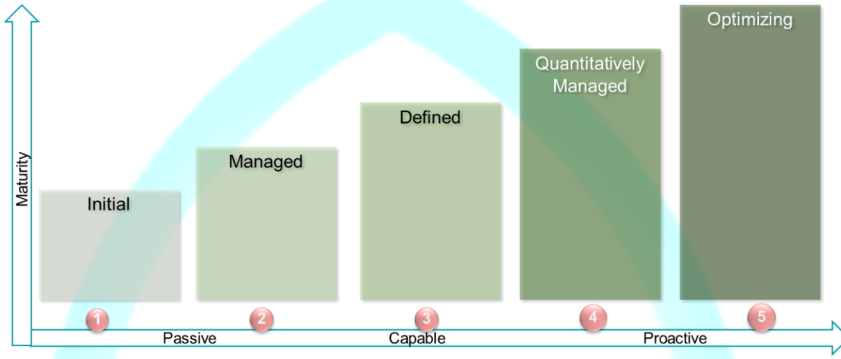
(5) Optimizing

9 Vulnerability management policies and standards, roles and responsibilities clearly defined, well communicated, implemented, and continuously reviewed and updated

- Training on technologies, communication, processes, and tools, with reference to international standards

- Regular checks on the measurement standards of security tests, and enhanced automatic security scanning and testing based on international standards
- Regular reviews and adjustments of the automated vulnerability management process
- Promotion of external bug bounty programs in multiple regions/countries, and regular reviews and updates of the programs
- Vulnerability response performance incorporated into "lessons learned" for improvements to keep pace with industry changes

Figure 9-1 Five levels of vulnerability management maturity



10 Summary

The Arab Governments should be fully aware of how important vulnerability management is to the security of the digital space. Consequently, they should develop full-view vulnerability management throughout the product lifecycle across the supply chain, in accordance with the five basic vulnerability management principles as well as industry standards and best practices. This is to support the mitigation of risks on the network.

As new technologies and threats continue to emerge and evolve, vulnerability management needs to be continuously iterated and optimized. Throughout the holistic Arab regional vulnerability management model proposed in this paper, the stakeholders shall share their experience and practices, build a collaborative and trusted ecosystem with customers and partners, and work together to address cybersecurity risks and challenges posed by vulnerabilities.

11 References and Bibliography

[1] ISO/IEC 29147:2018, ISO

[2] ISO/IEC 30111:2019, ISO

[3] Good practice guide on vulnerability disclosure, ENISA, 2016

[4] Developing National Vulnerability Programmes, ENISA, 2023

[5] Vulnerability Management Maturity Model, SANS

EXECUTIVE SUMMARY

As digital transformation accelerates, governments are relying on third parties such as cloud providers, business management and IoT to drive these initiatives. The ease with which non-IT business units adopt new technologies has led to an increase in shadow IT, making it difficult to assess the organization's risks. While third-party products and services can greatly enhance digital marketing, without third-party/supplier risk management, new risks can be more elusive than results. In fact, the rapid development and application of big data, industrial Internet, cloud computing, artificial intelligence, and other new technologies are driving advancements in convergence and ubiquitous digital services, leading to a prosperous digital economy. However, these new technologies also contribute to the increasing complexity of software architectures and the emergence of new attack methods. As a result, our national cyberspaces are exposed to more security vulnerabilities. In the context of frequent cybersecurity incidents, governments are increasingly aware of cybersecurity risks, and vulnerability management has become an important part of their cybersecurity strategies. Additionally, different countries and regions have legislated to manage cybersecurity vulnerabilities.

This white paper addresses a full-view vulnerability management approach for the Arab countries throughout the product lifecycle across the supply chain, in accordance with the five basic vulnerability management principles as well as industry standards and best practices. This is mainly to support the mitigation of risks on the Arab cyberspace. As stated in the Arab Cybersecurity Strategy, the objective of the proposed holistic vulnerability management framework is to create effective cooperation and better cohesiveness between research, enterprise and government to improve the capacity to assess security and assurance properties throughout the product lifecycle. The region’s huge market can be seen as an advantage in the development phase, where a product working at the level of society can be rapidly taken to completion. The most important prerequisite for achieving the strategic goal is ensuring functioning cooperation mechanisms between academia, private business and government institutions, which will ensure that strategic priorities will guide the focus of R&D in academia as well as in the private sector, thus ensuring the existence of key competences for the region.veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea co mmodo consequat.