Best Practices

Validating Medical Device Cybersecurity Through Penetration Testing

June 2026

MDIC
Medical Device
Innovation Consortium

Contents

Acknowledgments 3

About the Medical Device Innovation Consortium & Cybersecurity Program 4

Executive Summary 6

1. Introduction 7

2. Medical Device Penetration Testing Practices 9

2.1 Scoping Penetration Tests **10**

2.1.1 Determining Assessment Scope 10

2.1.2 Finding the Right Assessment Approach 12

2.1.3 Test Plan Development 13

2.2 Resourcing Penetration Testing **15**

2.2.1 Onboarding: Identifying and Qualifying Penetration Test Service Suppliers 15

2.2.2 Engagement Contracting: Creating Statements of Work 17

2.3 Execute Penetration Testing **18**

2.3.1 Penetration Test Environment & Equipment Preparation 19

2.3.2 Managing Penetration Test Execution 20

2.3.3 Reporting Penetration Test Execution Results 20

2.4 Disposition of Penetration Test Findings **22**

2.4.1 Penetration Testing Across Different Global Jurisdictions 23

2.4.2 Practices for Penetration Test Result Disposition 25

2.5 Communicate Penetration Test Results **28**

2.5.1 Communicating to Regulators 29

2.5.2 Communicating to Customers 30

3. Potential Pitfalls **31**

4. References **33**

5. Glossary **35**

DISCLAIMER

- *FDA employees participate as members of MDIC's Cybersecurity Working Group. The contents of this white paper represent the views of the authors and do not necessarily represent the views of, and are not an endorsement by, U.S. Food and Drug Administration (FDA)/ Department of Health and Human Services (HHS) or the U.S. Government. The views, findings, and interpretations contained in this document do not constitute FDA guidance, position on this matter, or legally enforceable requirements.*
- *The views and opinions expressed in this publication are those of the authors and do not necessarily reflect the views and policies of their respective employers, their management, subsidiaries, affiliates, professionals, or any other agency, organization, or company. The views and opinions in this publication are subject to change and revision.*

Acknowledgments

The following subject matter experts contributed significant time, talents, and expertise to this project. The MDIC (Medical Device Innovation Consortium) Penetration Testing Working Group would like to specifically acknowledge and thank the following individuals for their contributions:

- **Chris Reed (Lead),** Sr. Director of Cybersecurity Policy, Global Regulatory Affairs, *Medtronic*
- **Dirk De Wit,** Head of Product Security Group, *Philips*
- **Jason Herbst,** Principal Product Security Engineer, Product Security Office, *Medtronic*
- **Peter Kapelanski,** Sr. Engineering Manager, Product Security Office, *Medtronic*
- **Inhel Rekik,** Sr. Director, Product Security, *Bracco*
- **Curtis Blythe,** Director, Product Security, *Abbott*
- **Matt Hazelett,** Cybersecurity Policy Analyst, *FDA (Currently at MedSec)*
- **Bob Haack,** Sr. Mgr. MedTech Vulnerability Management, *Johnson & Johnson MedTech*
- **Sanket Kamath,** Sr. Security Engineer, Global Product Cybersecurity, *Boston Scientific*
- **Michelle Jump,** CEO, *MedSec*
- **Ken Hoyme,** Sr. Fellow, Product Security, *Boston Scientific (Retired)*
- **Jessica Wilkerson,** Technical Lead (Cybersecurity), *FDA (Currently at Roche)*
- **Justin Post,** Policy Analyst (Cybersecurity), *FDA*
- **Beau Woods,** Founder, *Stratigos Security*
- **Josh Berry,** Principal Consultant, *MedSec*

About the Medical Device Innovation Consortium

At MDIC, we work together to innovate for better health, transforming lives by accelerating access to medical devices. MDIC advances the scientific and technical disciplines that are fundamental to medical technology throughout the total product life cycle. Founded in 2012, MDIC is the premier public-private partnership convening medical device manufacturers, researchers, regulators, payers, patients, and health care providers as trusted collaborators to solve the industry's complex challenges. MDIC drives advancements in medical technology development, approval, coverage, adoption, and patient access in the core areas of quality design & manufacturing, evidence generation, digital health, and patient engagement. Learn more about our work at MDIC.org.

MDIC Cybersecurity Program

Background

Cyber threats pose risks to patient safety and accessibility. The MDIC cybersecurity program promotes and benchmarks mature risk management practices and nurtures approaches to address system-level risks. Medical devices have grown increasingly complex and connected, improving patient care by integrating advanced features and capabilities. To safeguard these devices and the sector's ability to continue delivering on its promise to improve patient outcomes, ensuring the cybersecurity of medical devices and the systems in which they operate are key. To protect their devices, manufacturers can build risk management programs that span premarket from early design, through the development of devices, and into the post-market.

Mission

Increase and enable sector expertise, collaboration, methodologies, and transparency to support the development and maintenance of safe and secure medical devices throughout the total product life cycle (TPLC).

Vision

By safeguarding patient care and protecting patient safety while advancing cybersecurity maturity and resiliency in medical device technologies, accelerating the secure integration of technologies and processes into healthcare delivery.

Cybersecurity Projects

MDIC's cybersecurity projects address a variety of critical areas, from educating manufacturers on threat modeling to establishing industry-wide benchmarks for cybersecurity maturity. Here are the key medical device cybersecurity projects at MDIC.

- Industry Benchmarking on Cybersecurity Maturity
- Penetration Testing
- Labeling and Transparency
- Threat Modeling
- Coordinated Vulnerability Disclosure Reporting

More information on specific projects, resources available and opportunities for engagement can be found at MDIC website here: https://mdic.org/program/cybersecurity/

Cybersecurity Executive Stewards

The Executive Stewards guide the strategic direction for the cybersecurity program. They support leadership by identifying key projects and facilitating effective communication between key stakeholders and industry engagement.

Adam Lacy, *Stryker*
Chris Reed, *Medtronic*
Curtis Blythe, *Abbott*
Dan Lyon, *Boston Scientific*
Kristen Killheffer, *Siemens Healthineers*
Miguel Crespo, *BD*
Nastassia Tamari, *FDA*
Paul Key, *Smith + Nephew*
Phil Dang, *Johnson & Johnson*
Varum Verma, *Philips*

MDIC Staff

Jithesh Veetil, Head, Center for Digital Health Technology
Pipper White, Sr. Program Manager

- **Contact the MDIC Cybersecurity team at:** cybersecurity@mdic.org

Executive Summary

This document outlines best practices for conducting penetration testing within the context of medical device design control, emphasizing its role as a critical verification and validation activity under the Secure Product Development Framework (SPDF). Penetration testing plays a vital role in ensuring the security and integrity of medical devices, which must meet rigorous regulatory standards to protect patient safety and confidentiality.

Penetration testing is incorporated into the SPDF as a key activity in the post-development phase to assess the security of medical device software and its associated networks. It serves as a proactive measure to identify vulnerabilities, validate system defenses, and support compliance with relevant standards such as FDA guidelines, IEC 62304, and the cybersecurity requirements outlined in IEC 81001-5-1.

By integrating penetration testing within the SPDF, organizations can:

- Verify the Effectiveness of Security Controls: Penetration testing confirms the adequacy of security measures, ensuring that identified risks and vulnerabilities have been appropriately mitigated.
- Validate Software Integrity: Through real-world attack simulations, penetration testing helps validate that medical devices are resilient against potential cyber threats, safeguarding both device functionality and patient data.

By following the outlined best practices, penetration testing becomes an integral part of a robust verification and validation process, enhancing the security and reliability of medical devices while reducing the risk of cybersecurity incidents. This process ultimately provides evidence to support that devices are safe for use, compliant with regulations, and resilient to evolving threats.

1. Introduction

According to the National Institute of Standards and Technology (NIST), penetration testing is defined as:

> *Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual unauthorized actors. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability [NIST SP800-115 – Technical Guide to Information Security Testing and Assessment[1]]*

The UK National Cyber Security Centre (NCSC) defines penetration testing as:

> *"An authorized test of a computer network or system designed to look for security weaknesses. Authorized testers identify publicly known vulnerabilities and common configuration faults in an organizations' IT system using the same tools and techniques as an unauthorized actor. The outcome from an authorized test is a report identifying the vulnerabilities."[2]*

The goal of penetration testing is to build confidence that the security controls designed and implemented in a medical device, hereafter referred to in this document as a device, are adequate. Penetration testing does not prove that an unauthorized actor cannot access a device, as to do so, the penetration tester would have to "prove the negative" – which has long been understood to be impossible. Instead, penetration testing simulates real-world attacks or incidents a device may encounter and determines whether the device can be exploited using those techniques.

Penetration testing focuses on the tactics, techniques, and procedures (TTPs)[3] that an unauthorized actor might use to access the device or its transmitted information to achieve goals that may impact confidentiality, integrity, or availability, especially in any way that could impact safety or effectiveness. The range of potential TTPs is broad, and can include exploiting architectural flaws, software vulnerabilities in the device source code or any third-party software that is used, or social engineering, among others.

In penetration testing, the skills of the tester simulate the capabilities of an unauthorized actor in attempting to access the device or its transmitted information using state-of-the-art TTPs. One may consider scope, resources, execution, disposition, and communicating penetration test characteristics and resulting findings effectively when looking to validate security controls through penetration testing. Given proper penetration test planning and execution within the total product life cycle (TPLC), confidence is built that:

---

[1] https://csrc.nist.gov/publications/detail/sp/800-115/final - See Section 5.2 specifically.

[2] https://www.ncsc.gov.uk/information/check-penetration-testing The UK National Cyber Security Centre (NCSC) defines penetration testing as: "A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might."

[3] https://csrc.nist.gov/glossary/term/Tactics_Techniques_and_Procedures

- An unauthorized actor who focuses their attention on that device may find it difficult to succeed in exploiting it, and may turn their attention to something that is easier to exploit; and
- Vulnerabilities that are known to be exploited by existing malware or to exist commonly in the wild at the time of testing are not easily identified in the device, making it less susceptible to non-targeted malware compromise.[4]

Penetration testing is not:

- An audit against a standard
- A comprehensive search for all potential security issues,
- A rigorous verification of security requirements or controls
- An evergreen set of findings, as new vulnerabilities and methodologies are discovered every day

Verification efforts are performed to confirm that the device correctly implements identified requirements, including security requirements. Validation efforts are performed to demonstrate that the device can consistently fulfill requirements for its intended use. With penetration testing, validation also accounts for the actions of unauthorized actors (e.g., cyber threat actors) that may attempt to exploit device vulnerabilities to manipulate the intended device functionality. A matrix where comparison is made between security verification and validation (V&V) for the normal "intended user," versus what V&V activities are done to increase confidence that the system will resist attempts by "unauthorized users" to penetrate the device and affect its safety and effectiveness, can be useful. Penetration testing can support validation that authorized users can access needed device resources, as well as supporting that unauthorized users may be unable to.

Security	Authorized User	Unauthorized Actor
Verification	• Verify that security requirements are implemented as specified • Verify hardening rules have been implemented correctly	• Verify sufficient input handling through planned boundary testing • Identify and disposition known vulnerabilities
Validation	• Validate that security controls operate as the user expects • Validate that the security controls do not unreasonably interfere with the user completing their workflow	• Validate that security controls successfully resist unauthorized use • Validate the exploitability of identified and known vulnerabilities being "reasonably foreseeable misuse" and the potential impacts the vulnerability could manifest on the device including safety and effectiveness

[4] An example of such a non-targeted malware was WannaCry, a ransomware tool that was generally deployed against vulnerable Microsoft Windows implementation that was not specifically aimed at medical devices but caught some that had not been patched for the underlying vulnerability. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

It can be helpful to ensure that all design security controls have been verified to operate correctly through specific testing traced to requirements. However, full validation of those controls generally warrants exposing the device to real world conditions to ensure the device's design handles common usage and operating environments. Engineers can design security controls that may seem appropriate until they are exposed to real world conditions, where they may fail to perform their objective.[5]

The intent of this document is to address how penetration testing may fit within the Secure Product Development Framework (SPDF) as a verification & validation (V&V) activity. The intended audience is members of medical device manufacturers responsible for quality system management, program management, and R&D management: in other words, those who allocate resources for development activities. Each substantive section of this paper is broken into several sections, which follow the steps organizations can take to accomplish penetration testing. These steps include the following and are detailed in Section 2 (Medical Device Penetration Testing Practices):

1. Scoping Penetration Tests (section 2.1)
2. Resourcing Penetration Testing (section 2.2)
3. Executing Penetration Testing (section 2.3)
4. Disposition of Penetration Test Findings (section 2.4)
5. Communicate Penetration Test Results (section 2.5)

As medical devices and systems become increasingly networked and interconnected, it is important that the impact of cybersecurity threats on safety become part of risk management activities. Validation of security controls is a critical part of the total product life cycle (TPLC). Penetration testing can help accomplish this by using penetration testers that are skilled in the state-of-the-art activities used by cyber threat actors to gain access to target systems. Proper penetration testing scoping, resourcing, execution, and disposition of findings can help validate the security of a medical device effectively resists current cyber threat actor practices.

2. Medical Device Penetration Testing Practices

While a useful tool for medical device cybersecurity risk management, integrating penetration testing into total product life cycles (TPLCs) can be complex. The following sections describe how manufacturers could incorporate penetration testing into their strategies, processes, and procedures.

[5] A simple example often seen in practice is an interface supporting strong transport encryption, but where an unauthorized actor can interact with the device to downgrade or even disable that transport encryption completely due to improper configurations. When manipulated or otherwise misconfigured, the strength of the transport encryption may be downgraded, allowing the unauthorized actor to both expose and manipulate network traffic.

2.1 Scoping Penetration Tests

One of the early activities of penetration testing is scoping; in other words, determining the areas of focus for the penetration test. The test scope includes the approach that will be taken with sharing device information and the overall test plan development. This early scoping work allows for a penetration test that properly validates the device's cybersecurity posture.

2.1.1 Determining Assessment Scope

A properly scoped penetration test can achieve security control validation and overall security risk management objectives. If not scoped properly, the penetration testers may utilize their limited time to focus on activities that may not contribute to understanding whether the device adequately resists the real-world threats that it may face in practice. Poor scoping can lead to increased costs, delays, and ineffective results.

Scoping begins by understanding the system/ecosystem under test and its general purpose and functionality, including each component of the system and related systems, as well as the hardware, firmware, software, mobile apps, web apps, and Application Programming Interfaces (APIs) that the device uses. Each component of the device is then evaluated to determine the system functionality it implements, and the data sensitivity contained within and/or processed by it. Generally, this consists of asking questions about how cyber threat actors may attempt to compromise a component based on its technical characteristics, and what could go wrong if that component were to be compromised.

Prior threat modeling and architectural analysis can be beneficial to the scoping process, as these activities typically help to identify the areas of the system that require security controls, and, thus, are relevant to assess. In addition, system workflows or clinical use cases may be used to identify relevant components.

The following considerations are part of the initial scoping effort:

- **Use of Standard Methodologies –** Industry recognized assessment methodologies can be a starting point to develop test planning, such as Open Worldwide Application Security Project (OWASP) Application Security Verification Standard (ASVS)[6], OWASP Top Ten [7], MITRE ATT&CK [8], MITRE EMB3D [9], or Penetration Testing Execution Standard (PTES) [10]. Methodologies typically articulate categories of common system weaknesses and suggest the type of testing that will evaluate the system's ability to withstand these types of threats. Advantages of using an established methodology include an organization having confidence that certain web application security features were tested, if OWASP's Application Security Verification Standard (ASVS) was used given its methodologies.

[6] https://owasp.org/www-project-application-security-verification-standard/
[7] https://owasp.org/www-project-top-ten/
[8] https://attack.mitre.org/
[9] https://emb3d.mitre.org/
[10] http://pentest-standard.org/

- **Attack Surface Analysis –** According to the National Institute of Standards and Technology (NIST), attack surface is defined as:

  > "The set of points on the boundary of a system, a system component, or an environment where an unauthorized actor can try to enter, cause an effect on, or extract data from, that system, component, or environment." [NIST 800:53]

  Attack surface is a critical consideration in penetration testing, and often drives the level of expertise required to adequately perform the penetration test. Attack surface could include hardware level threats and cover various perspectives, including privileged and unprivileged users. Additionally, attack surface may depend on the use environment of a system. It is best practice that organizations decide how much and which parts of the attack surface are covered during testing, based on the threat model, and resulting cybersecurity risk management documentation. At the same time, it is important that the attack surface in scope for a penetration test not be restricted unnecessarily.

- **Use of Threat Intelligence –** Threat intelligence conducted by the manufacturer, such as specific TTPs that cyber threat actors might potentially use, may be provided to the penetration tester to ensure those known attack patterns are tested. Examples of this may include requesting a penetration tester perform specific types of testing, such as Bluetooth Low Energy (BLE) attacks, given the importance of a BLE connection to a device's safety and effectiveness. While it is important not to limit the penetration tester to specific attacks, it can be very useful to ensure certain threats the device may face in the real world are properly scoped into testing activities. To help ensure adequate coverage of current real-world threats, consider threat intelligence related to the attack surface during scoping of the penetration test.
- **Intended Use Characteristics –** The intended use characteristics of the device will impact the scope of the penetration test. For example, an increased focus on impacts to availability makes sense for therapy devices since failure may cause harm through therapy delays. A diagnostic device may have a greater emphasis on impacts to data integrity given the use of resulting information to inform treatments. Along with sharing any rules of engagement to ensure safety is properly assessed in testing, it may be helpful to share intended use as part of the penetration test scope. At the same time, it is important that intended use not be used as justification to inappropriately limit the scope of a test.
- **Use Environment –** Consider the use environment of the device and the device architecture during the initial scoping effort. For example, if the design of a system assumes network connectivity to a hospital Electronic Health Record (EHR) system, it is reasonable to include that connection as part of the attack surface and/or system scope. Other use environment considerations may also include common threats that operating environments may present, such as:
  - Ransomware propagation in hospital networks
  - Network and/or remote resource availability (or lack thereof), such as cloud
  - Supporting/interacting systems such as EHR APIs or other ecosystem components, including Domain Name System (DNS) and other essential networking infrastructure

2.1.2 Finding the Right Assessment Approach

Penetration testing can be performed by testers with varying levels of system documentation related to the system being tested prior to the start of testing. The degree to which full system information is provided to the penetration tester is usually described as Open Box (i.e., White Box) or Closed Box (i.e., Black box) testing.

Open Box Testing (i.e., White Box Testing): With an Open Box testing approach, the penetration tester is given access to resources (e.g., threat model, architectural documentation, cybersecurity risk assessment, software bill of materials (SBOM), known vulnerabilities and their disposition, source code, etc.) that help them assess and plan valid testing approaches. An Open Box test can provide a deeper look into the defense-in-depth capabilities of the device and may raise the efficiency of the testing engagement.

- **Pros:**
  - Comprehensive test coverage, including the ability to discover exploitable vulnerabilities through source code review.
  - Easier to validate findings through system examination rather than via trial-and-error, leading to fewer false positives.
  - Business logic vulnerabilities may be easier to identify.
  - Post-exploitation flaws (privilege escalation, abuse of functionality) can be discovered sooner.
- **Cons:**
  - Least realistic form of testing as, typically, only an insider would have deep knowledge of the system.
  - Onboarding may take longer given system information is typically collected, securely shared, and reviewed by testers.
  - Testing may identify weaknesses which could be difficult or impossible to exploit by an external cyber threat, leading to wasted time on potentially impacting service and resource intensive remediation.

Closed Box Testing (i.e., Black box testing): With a Closed Box testing approach, only basic information regarding the system is made available to the testers. This represents a real-world scenario where an external cyber threat may use open-source intelligence (OSINT), social engineering, and/or reverse engineering skills to attempt to penetrate system security.

- **Pros:**
  - Most realistic form of testing as this is the position that a real-world cyber threat would most likely be starting from.
  - Can enable creative approaches to testing that are not biased by knowledge of risks already identified and managed.

- **Cons:**
  - Discovery takes time, limiting test coverage during a time-constrained assessment, which could lead to false negatives.
  - Can be difficult for testers to validate if exploitation was successful, leading to more false negatives and possibly false positives.

Approach selection is guided by an organization's validation objectives:

- Finding problems in the business logic/flow of a device warrants knowledge of how the device is intended to function, which takes time and effort to learn before doing any significant testing. For this, **Open Box** testing may be most appropriate so that testers can more quickly understand the system's design and security architecture
- Since penetration tests are often limited by time and resources, while the resources available to cyber threat actors may have no such limitations, **Open Box** testing utilizes the time allocated for the penetration test most efficiently.
- Alternatively, it may be valuable to see how an experienced cyber threat actor would approach a system without any inside knowledge that may bias their approach. In this case, the **Closed Box** approach may be more valuable, especially for more mature devices which have previously been assessed via an Open Box approach.
- Mixed approaches, in which testers are 1. Provided with limited internal information at the outset to focus testers' attention on areas of particular concern, or 2. Provided internal information only after a period of **Closed Box** testing, are also possible. These approaches blend the pros and cons of the two primary approaches.

2.1.3 Test Plan Development

A test plan describes how the testing will be conducted. Common components of a test plan include:

- **Rules of Engagement –** A description of the "rules" the penetration tester is to follow. Often these are items that are specifically out-of-scope or not desired as part of the test execution. Examples may include:
  - **Testing Environment** – Defining a specific environment for testing (e.g., Production, Quality Assurance or Development)
  - **Testing Hours** – Defining the hourly window testing can be performed, to either avoid end-user performance issues or have on-site staff available to troubleshoot resulting issues. This aspect may also give consideration to red/blue team exercises [11], depending on the assessment being performed.
  - **Out-of-Scope Items** – Documenting explicit items that are not to be performed. Examples of these may include: destructive testing of a physical device; denial-of-service attacks; attacks against sensitive devices and/or hosts which could impact critical business operations; social engineering; and removing or changing accounts, among others.

[11] Red team is a term referencing attack simulation such as penetration testing and blue team is a term referencing defensive teams such as security monitoring including vulnerability management and incident response.

- **Documentation of Device Characteristics –** the device characteristics for the penetration test. This may include:
  - Specific versions (or intended versions) of software and hardware, including application, API (application programming interface), and operating system (OS) versions.
  - Specific internal hardware and custom hardware, including processor, radio, and even security chips, leveraged in the design.

  Note: The device characteristics may change between scoping and penetration test execution; regardless, sharing these details with the testers will allow the final report to accurately depict what was tested. Additionally, the device characteristics help ensure that the tester capabilities are accounted for. For example, if hardware is included in testing scope, testers experienced in hardware analysis, such as Printed Circuit Board (PCB) tracing, Joint Technical Action Group (JTAG) port analysis and other debug port analysis, could be useful.

- **Test Dependencies –** Dependencies include the list of items required to perform the planned assessment, the accountable party to provide the item, and the delivery mechanism. This includes a list of physical devices to be provided, environmental considerations (e.g., mobile app on a rooted mobile device), open-box material (source code), or access requirements for limited access testing environments (e.g., VPN (Virtual Private Network)), among others.
- **Timing –** System penetration testing is generally conducted after all other secure product development framework (SPDF) security activities have been performed. Penetration testing on a production-equivalent system with full security features in place may be considered, as testing before all security features are fully implemented may result in issues being reported that a security feature is meant to address. However, testing too late in the SPDF (i.e., just before device launch) may reduce the time available to address any issues found, and the issues may be more costly to fix.

  Penetration testing prior to formal system verification and validation efforts may be most helpful. To help ensure any discovered findings are adequately dispositioned, consider documenting results and dispositioning as part of the formal test anomaly process.

  For systems that are already on-market and are not undergoing continued development efforts, it may be helpful to evaluate the need for penetration testing on a periodic basis. Factors to consider when determining if additional penetration testing may be beneficial include: the time since the last test was performed; new TTPs that have been developed or made possible by advancements in technology (e.g., computational processing power); or the confidence in the scope and testing personnel of the previous penetration test.

- **Duration –** The time necessary to perform a penetration test will be highly dependent on the scope and approach selected. Tests can range from days/weeks to months depending on scope, the approach selected, and resource availability. Starting the planning process for penetration testing early in the device development process, setting milestones, and tracking progress on a regular basis may avoid unnecessary delays.

2.2 Resourcing Penetration Testing

When evaluating how to resource a penetration test there are several factors to consider. To be effective, use qualified and sufficiently independent penetration test resources. This section will detail considerations to support adequate resourcing for penetration tests.

2.2.1 Onboarding: Identifying and Qualifying Penetration Test Service Suppliers

It is important that penetration test service suppliers supporting medical device development be properly vetted, to help ensure the work product will be of sufficient quality. Penetration testing service suppliers vary widely on the levels of proficiency and capability. Some penetration test service suppliers may lack essential skills and may provide only basic and minimum testing. Penetration testing service suppliers often specialize in certain types of testing, such as wireless or mobile applications. Good penetration testing service suppliers are also in high demand and may take time to contract and schedule. Larger organizations may maintain a pool of penetration test service suppliers to choose from to ensure appropriate levels of expertise and availability. A larger organization may even maintain internal expertise that can be used as part of the potential resource pool. At a minimum, one may want to consider performing due diligence to ensure the penetration test service supplier can deliver the level of proficiency and capability needed. A penetration test service may provide evidence of their work that matches the expected scope of an organization's devices. This can be accomplished by reviewing redacted penetration test reports and reviewing penetration testing service staff experience. Ideally, penetration test service suppliers will have experience with regulated devices to ensure their work product will sufficiently support regulatory review and customer expectations.

Factors for Consideration When Selecting a Penetration Test Service Supplier (e.g., Third Party or Internal Test Team)

Organizations may leverage external penetration test service suppliers or internal penetration test service capabilities. Below are factors to consider when selecting a penetration test service supplier:

- **Expertise –** Penetration testing is a specialized discipline, involving unique training and expertise. Penetration testing for medical devices in their environment of use is an even more specialized discipline. Moreover, penetration testing best practices are constantly evolving as cyber threats and digital infrastructure evolve and grow more complex. Organizations may want to ensure that they are identifying and selecting penetration test service suppliers with appropriate expertise. In vetting the potential penetration test service suppliers, look specifically for experience and capability to deliver high quality penetration testing for the portfolio of devices an organization plans to bring and maintain in the market. Asking penetration test service suppliers to provide evidence to back up claims of expertise, including, but not limited to redacted sample reports and the qualifications of specific penetration testers may also be insightful. Consider the following:
  - Expertise with technologies integrated into the devices, such as cloud, wireless, web application, mobile application, firmware, and hardware engineering. A penetration test

with a broad scope may call for more than one person to be assigned to a project to cover the necessary breadth of a device and its supporting ecosystem.

- Experience commensurate to the project complexity. For example, using more junior penetration testers, with appropriate oversight by experienced penetration testers.
- Familiarity with attacker methodologies related to the device architecture. This can be demonstrated through a review of previous work.

  Note: Due to the sensitivity of penetration testing reports, samples of previous work may be limited. Experienced penetration testers often have a public body of work that can also be evaluated to determine whether sufficient experience and expertise can be demonstrated.
- Experience with regulated devices, ideally with medical devices, and success with reports being accepted by regulators.
- With regard to cost, higher skilled resources, especially for specialized expertise such as embedded hardware or wireless BLE testing, may be more expensive. However, some larger firms have high prices that may not reflect their quality of work or capabilities.

- **Volume of Work –** Since penetration testing simulates real world attacks, leveraging a diverse pool of penetration testing service resources over time may provide different perspectives and skills to best identify device security vulnerabilities. In addition, engagement with penetration test service suppliers on a regular basis may help ensure efficient and effective engagement. The volume of penetration tests an organization needs will influence how many penetration tests suppliers are maintained. As noted elsewhere, penetration testing is done on major new device release versions. Repeat testing on a periodic basis commensurate to the risk of the device to help ensure the device is able to remain secure considering new attack techniques may also be necessary. Consider the volume of work needed across the entire portfolio annually along with the other factors discussed in this document when determining how many penetration test service suppliers to maintain as active suppliers.
- **Level of Independence –** A common misconception is that penetration test resources from a third-party organization are the only way to confirm a sufficient level of independence, but internationally, IEC 81001-5-1:2021 specifies the required level of independence for penetration tests as an "independent department or organization" (see Figure 1). The key factor is whether penetration test service resources have sufficient independence from the development team. For smaller organizations with limited staff, it may not be possible to achieve this level of independence without leveraging third-party organizations. Larger organizations may be able to support establishing an internal penetration test service with specialized staff if their independence can be sufficiently established. This can be beneficial to build deeper knowledge on devices, scheduling prioritization, and other efficiencies. When using internal staff for testing, consider the factors as outlined above in addition to ensuring that sufficient independence is demonstrated.

Test Type	Reference	Level of Independence
SECURITY requirements testing	SVV-1 SECURITY requirements testing	Independent department
THREAT mitigation testing	SVV-2 THREAT mitigation testing	Independent department
VULNERABILITY testing	SVV-3 VULNERABILITY testing	Independent person
Static code analysis	SI-1 SECURITY implementation review	None
ATTACK SURFACE analysis	SVV-3 VULNERABILITY testing	Independent person
Known VULNERABILITY scanning	SVV-3 VULNERABILITY testing	Independent person
SOFTWARE COMPOSITION ANALYSIS	SVV-3 VULNERABILITY testing	None
Penetration testing	SVV-4 Penetration testing	Independent department or organization

SOURCE: IEC 62443-4-1:2018[11], SVV-5, 9.6.1.

Figure 1. Required level of independence of testers from developers. ©IEC. This material is reproduced from IEC81001-5-1:2021 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved.

2.2.2 Engagement Contracting: Creating Statements of Work

Every penetration test will create specific documentation prior to the test. A penetration test is not a static work product and depends on the scope of the project which can be captured in specific documentation for each penetration test. This documentation can capture the scope of the test as discussed in section 2.1 above, including the planned duration of the test, and a description of the test environment or test sample, as agreed to between the testing team and the device owners. The content of this document can be retained with the Device's Design History File (DHF) and is often included in the final penetration test report.

For third-party contracted penetration tests, this content is also often reflected in a statement of work (SOW). Consider documenting the overall scope, approach, necessary resources, timing, duration, and any rules of the engagement or reporting expectations of the penetration testing engagement in a contract (usually the SOW) between the manufacturer and the penetration testing organization, whether internal or third-party, for clarity. It may also be helpful to outline any items considered out-of-scope so that testing time can be focused on the in-scope items. If a pool of penetration test suppliers is actively maintained, an organization may be able to perform a bidding process with qualified penetration test service suppliers. As penetration test service suppliers are considered, the following factors may be reviewed:

- **Expertise –** Often penetration test service suppliers specialize in certain types of penetration tests. Similar to vetting of penetration test service suppliers, it is important to consider expertise for specific penetration test engagements. Review "Expertise:" in section 2.2.1 for factors to consider.

- **Cost –** Organizations may have limited budget for resourcing penetration tests. However, a penetration test that is insufficiently resourced risks missing issues and may result in significant consequences. Organizations may wish to identify and compare penetration test supplier costs with the quality of their work to select a vendor that can successfully execute a high-quality penetration test within the target budget.
- **Calendar availability –** There are a limited number of qualified penetration testing service suppliers available. Even internal penetration testing service capabilities will have limited resources that are likely in high demand. Consequently, penetration test service suppliers may have limited availability, and may be unavailable on short notice. It is helpful to identify penetration testing needs early and begin identifying, evaluating, and negotiating with potential penetration test service suppliers early enough to meet timelines. Factors that may influence penetration testing timing include:
  - **Device Development Deadlines:** The organization may have internal device development deadlines. Schedules often shift, but it is easier to shift resources that have already been planned and allocated than waiting until the start of a testing period to finalize specific penetration test service supplier resources.
  - **Regulatory Submission Goals:** The organization may be seeking to submit a marketing application by a certain date.
  - **Engineering SMEs:** Knowing the availability of engineering SMEs to help get testing equipment available and ready for testing, helping testers get testing equipment set up, and answering questions around the testing equipment.
  - **Test Sample, Build, or Environment Availability:** Identifying and making available testing devices, builds, equipment, software, firmware, and anything else that matches the scope of the penetration testing.

Vetting the assigned penetration testers' backgrounds by looking specifically for experience consistent with their experience level and role in the device's architecture or similar devices is also part of engagement. Expertise and experience can be verified through review of previous work in the form of redacted penetration test reports, resumes including examples of penetration testing achievements and even previous organizational experience with the penetration tester. It is important that the specific individuals that performed the test be detailed in the final penetration test report, to ensure penetration test results can be traced to the person or team that performed the work.

2.3 Execute Penetration Testing

Once a penetration test has been successfully scoped and resourced, an organization may move to execute it. Penetration test resources are often scheduled in a dedicated fashion for test execution and therefore it is essential to ensure their time is fully leveraged, given these resources are highly skilled and difficult to reschedule. Generally, this involves three steps to ensure a successful penetration test execution, each of which is discussed in detail in the following subsections:

1. **Preparing Penetration Test Environment & Equipment:** This step is completed prior to the scheduled start date of the test.
2. **Managing Penetration Test Execution:** This step is typically scheduled into a specific time frame so that the penetration test resources can effectively execute the scope of their work during the scheduled time.
3. **Reporting Penetration Test Results:** The draft report results are typically written and provided within a few days of the penetration test being completed. This step reviews the draft results for information accuracy and clarity, as well as adequate communication of the penetration test results.

2.3.1 Penetration Test Environment & Equipment Preparation

The environment(s) and equipment necessary for a given penetration test will be dependent on the test's scope. Ideally, it is helpful to prepare all environments and equipment in advance of the penetration test's planned start.

Types of environments that may be helpful include:

- Cloud services necessary to operate the device
- Internet hosted applications for web-based devices
- Mobile apps/devices with certain features disabled to allow for testing of agreed scope, such as certificate pinning or jailbroken mobile devices

Types of equipment that may be helpful include:

- Mobile devices or other supporting hardware to support devices applications with the proper configuration
- Device hardware
- Specific testing equipment to support testing scope such as Bluetooth Protocol Analyzers or network traffic capture tools

When preparing environments and equipment, organizations may wish to consider:

- Penetration tester tools themselves do not need validation (see rationale in Why Aren't Penetration Tools Validated Typically? sidebar on page 20)
- Non-Production test environments which share resources with production systems are not often leveraged for penetration tests, due to the risk that testing could cause issues for actual users and data. An environment that closely mirrors production and allows for adequate user credentials to be provisioned may be leveraged instead. This often warrants planning and coordination prior to the start of the test.
- Equipment may need to be acquired and received prior to test start: It may be helpful to identify the test equipment needed, such as hardware to complete the test, and arrange access to that equipment at relevant locations. Shipping equipment can have unexpected delays, so taking that into consideration can help ensure equipment arrival prior to the scheduled start of a test.

2.3.2 Managing Penetration Test Execution

Careful management of test execution supports a successful penetration test. Whether leveraging internal or external penetration testing resources, the following practices can improve the odds of a successful test:

- **Oversight and Monitoring –** Effective oversight of testers includes assessing whether 1) the scope is being properly executed, 2) resources are being effectively used, and 3) organizational expectations are being met. This may be more critical with third-party testers, who may not be as familiar with organizational priorities or processes.
- **Communication –** Frequent communication with testers can surface issues for early and efficient resolution. It can also facilitate testers gaining permission, where necessary, to execute certain aspects of the test (e.g., where testing environments may be shared with other resources).
- **Critical Findings –** Briefing critical findings immediately, rather than at the end of the test, can aid in addressing potentially significant and unsafe conditions as soon as possible. Even for unreleased devices, R&D teams will appreciate any additional time they have to begin to assess and respond to any critical findings.

2.3.3 Reporting Penetration Test Execution Results

To be effective, it is important that penetration test results be clearly documented and explained in a way that enables an organization to fully and comprehensively act on the results. Consequently, penetration test reports are one of the most critical aspects of penetration testing.

Why Aren't Penetration Testing Tools Validated Typically?

Since standard device V&V recognizes the need for validated tools, the question arises whether the tools used by a penetration tester need to be validated. There are several reasons why they typically are not.

Penetration testing tools are constantly changing- and validating them would likely require constant and time-consuming revalidation that could impact testing availability or completeness if tool validation were delayed. More importantly, tool validation for penetration testing constrains the tester in ways an unauthorized actor is not. There is only so much time allocated to conduct a penetration test, and if tests need to use only validated tools, testers may be more limited in what they can test, or the test may be delayed while tools are validated. Penetration testers may choose not to use a tool to avoid validation overhead, whereas an unauthorized actor would not be so constrained. To truly simulate the behaviors of an unauthorized actor, it is important that penetration testers have access to the same freedom to explore and utilize tools.

As such, you may consider not subjecting penetration testers to constraints that the unauthorized actor they are trying to simulate would not have. Instead, penetration testers can document all tools, as well as associated version and configuration information, that would be necessary to reproduce the results.

At the end of a penetration testing engagement, the following information is useful for penetration testers to summarize in a report:

- Test scope, minimally what was included in the statement of work or other material used to plan the penetration test engagement
- Duration of testing specifying the dates testing started and was completed, but does not include the time to create and revise reports
- Named individuals performing the tests along with a description of independence, qualifications and technical expertise
- Test methodology including what documentation was provided, what techniques were attempted and how the attack surface of the device was sufficiently tested
- Specifics of devices in their environment of use including but not limited to:
  - serial numbers and associated software build identification, including any supporting software versions provisioned on the devices
  - URLs and supporting environment information such as the cloud hosted APIs
  - any modifications to devices in their environment of use or the environment to enable testing such as removal of software that allows jailbreaking a mobile device or disabling a security control such as antivirus or a web-application firewall
- Penetration test tools used, including:
  - versions
  - specific configurations
  - the sequence of steps that were used to demonstrate each identified vulnerability
- General observations of the overall performance of the system including positive observations of controls that worked effectively
- Any findings identified, including a security risk rating using the penetration test supplier's security risk scoring methodology and appropriate evidence. This may include:
  - recommendations to address identified findings.
  - detailed documentation of findings so that organizations may recreate the findings to determine if and when threats and vulnerabilities have been mitigated.
  - artifacts or evidence of exploited vulnerabilities in the form of screenshots, which may be redacted to protect sensitive information such as encryption keys or passwords[12]

Penetration test findings are typically highly sensitive documents, as findings of risks that are accepted, rather than eliminated or mitigated, could represent instructions for potential exploitation by a threat actor. Even information regarding those findings that are eliminated or mitigated may provide unauthorized actors with information, which could be useful for developing other attacks. As a result, limiting access to the penetration test report to those that have a need to know and proper security mechanisms when sending or storing the report electronically or otherwise are important considerations.

[12] Note that there are certain known vulnerabilities that are not always exploitable in a single attempt but may depend on some randomness (i.e., timing conditions, operational states, etc.) of system behavior. If such vulnerabilities are reported, it is important to communicate an understanding of that randomness to aid in the ability to show whether that vulnerability has been eliminated.

It may be helpful to first provide penetration testing reports as a draft for the customer to review and then finalize the report later after customer feedback is received. Organizations may wish to verify the findings through review by staff that have a deep understanding of the medical device to ensure accuracy. Penetration testing reports generally will include security risk severity ratings for findings that leverage the author's rating scales. Instead of pushing back on the author's ratings, customers may wish to provide feedback to help ensure the nature of the finding is correctly understood and captured. This may lead to the author re-rating the severity of the finding when justified. The customer will generally have the opportunity to evaluate findings using the customer's organizational security risk rating methodology and document their perspective as they disposition penetration test findings within their quality management system.

2.4 Disposition of Penetration Test Findings

Once a penetration test is complete and a final report delivered, organizations may find it helpful to analyze and determine appropriate responses to all risks identified, a process generally known as "disposition," and then document findings in the Design History File (DHF).

Risk responses may take several forms, including:

- Risk Acceptance
- Risk Avoidance
- Risk Sharing or Transfer, and
- Risk Mitigation[13]

The device team can then assess each penetration test finding through their established organizational security [14] and safety risk assessment procedures to determine which response, or combination of responses, is most appropriate for each finding. Both the penetration tester's rating of the finding and the organization's established procedures may contribute to the response to ensure consistent evaluation of risk including potential safety concerns. Consider the following as this process is conducted.

- Security risk control measures (mitigation) for reducing security risks to acceptable levels for all findings and taken when security risks are at unacceptable levels.
- That risk acceptance aligns with the organization's procedurally defined risk tolerance and accurately reflects stakeholder interests.
- Identifying any risk transfer/sharing to be identified within medical device labeling.
- Include risk mitigation actions that are clearly traceable to change requests or other activities done to help reduce the risk. This includes any updates to security requirements added and the testing that supports the penetration test finding was adequately addressed.

Organizations may wish to document the selected risk response(s), traceability to any actions taken, and the associated rationale in the medical device DHF. Penetration test reports can also be attached

[13] See NIST SP 800-39, Section 3.3 for definitions.

[14] Security Risk Management in medical devices should align with ANSI Standard SW96 *Security Risk Management for Device Manufacturers.*

to the associated disposition report to provide clear traceability to disposition of penetration test findings.

The process of analyzing test findings and determining appropriate responses may involve ongoing communication between the device team and the penetration tester, as the penetration tester may be able to improve the device team's understanding of the risks presented by certain vulnerabilities that were identified during testing. The penetration tester may also be able to provide expert advice on the effectiveness of proposed risk responses. At the same time, the development team's detailed knowledge of the medical device may be able to improve the clarity and accuracy of the penetration tester's explanation of a finding.

2.4.1 Penetration Testing Across Different Global Jurisdictions

Penetration test reports, and the dispositions of penetration test findings, may be within the scope of regulations in major geographies, which may require these reports and findings to be included in the medical device DHF or elsewhere. Documentation of penetration test findings and findings disposition may be required by regulation and adequate documentation might be required. Different regulatory bodies may also consider third party penetration testing suppliers to be in scope of purchasing controls within the quality management system in addition to the items below. Examples of some documents with potential regulatory linkages or relevant recommendations are listed below:

- **International Medical Device Regulator's Forum (IMDRF):**
  - IMDRF Principles and Practices for Medical Device Security N60 states in section 5.3 Security Testing, *"Conduct technical security analyses (e.g., penetration testing). These include efforts to identify unknown vulnerabilities through fuzz testing, for example; or checks for alternative entry points, e.g., by reading hidden files, configuration, data streams or hardware registers."*
  - IMDRF Principles and Practices for Medical Device Security N60 states in section 5.6.3 Security Testing Documentation, *"Details of specific testing, such as cross-referencing software components or subsystems with known vulnerability databases, for example, can be found in [N60 Section 5.3], however all testing documents should contain:*
    - *Descriptions of test methods, results, and conclusions;*
    - *A traceability matrix between security risks, security controls, and testing to verify those controls; and*
    - *References to any standards and internal SOPs/documentation used."*
- **Conformance with international consensus standard IEC 81001-5-1 (required in Japan and recognized in other jurisdictions including the U.S.):**
  - IEC 81001-5-1:2021 Section 5.7.4 Penetration Testing
  - IEC 81001-5-1:2021 Section 7.3 Estimation and Evaluation of Security Risk
  - IEC 81001-5-1:2021 Annex B Guidance on Implementation of Secure Lifecycle Activities

- **EU MDR:**
  - The Medical Device Regulations (Regulation (EU) 2017/745) states in Annex I, *"General Safety and Performance Requirements", specifically in Ch 2, Section 17.2 that: "For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation."*
  - The Medical Device Coordination Group document MDCG 2019-16 "Guidance on Cybersecurity for medical devices" elaborates in section 3.7 "Verification/Validation" that: *"The primary means of security verification and validation is testing. Methods can include security feature testing, fuzz testing, vulnerability scanning and penetration testing."*
  - The Medical Device Regulations further state in Annex II, "Technical Documentation," specifically Section 6, that: *"The documentation shall contain the results and critical analyses of all verifications and validation tests and/or studies undertaken to demonstrate conformity of the device with the requirements of this Regulation and in particular the applicable general safety and performance requirements."*
- **US FDA:**
  - Section V.C (Cybersecurity Testing) of FDA's guidance titled "Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions" elaborates on the US FDA's recommendations regarding the following types of cybersecurity testing documentation to be included in a premarket submission: security requirements testing, threat mitigation testing, vulnerability testing and penetration testing.
  - With respect to penetration testing specifically, the guidance states that the manufacturer: *"should identify and characterize security-related issues via tests that focus on discovering and exploiting security vulnerabilities in the product."* Specific elements to include in penetration test reports are: *"Independence and technical expertise of testers; scope of testing; duration of testing; testing methods employed; and test results, findings, and observations."*
  - Note if a third party is leveraged for testing that guidance states: "For any third party test reports, manufacturers should provide the original third-party report."
  - The guidance recommends that manufacturers assess any:
    - *"findings including rationales for not implementing or deferring any findings to future releases."*
    - *vulnerabilities and anomalies identified during testing for their "security impacts as part of the security risk management process."*

2.4.2 Practices for Penetration Test Result Disposition

Typically, once penetration testing has been completed, and the report delivered, the organization would conduct an in-depth analysis of the test results to adequately disposition the findings, through a methodical process captured in their Quality Management System (QMS).

This section explains some practices that the organization may employ in their analysis and disposition.

2.4.2.1 Risk Assessment, Rating, and Management

When performing risk assessments on penetration testing findings, organizations may wish to:

- **Assess in Context –** The same technical vulnerability, present in two different medical devices, may have a completely different effect, depending on the characteristics and intended use of each device.
- **Assess Patients and Users Safety Risks –** It may be helpful to focus on the level of access gained by the penetration tester and the security controls that were bypassed, rather than the specific effects the penetration tester was able to demonstrate. Any other function that can be affected given the same level of access is also potentially vulnerable and may potentially benefit from security controls.
- **Assess Patient and User Privacy Risks –** Organizations may wish to focus on the level of access gained by the penetration tester, and the security controls that were bypassed, rather than the specific information the penetration tester was able to demonstrate access to. Any other sensitive information which is available at the same level of access is also potentially vulnerable and may potentially benefit from security controls.

Penetration test findings which reveal risks that could impact patient or user safety can be propagated to the risk management documentation in the device's DHF. There are several considerations related to transferring these risks:

- Translating the risks warrants highly detailed knowledge of the device's functioning to fully analyze the possible failure modes presented by the identified vulnerability, and the device design team is likely to have the most complete expertise to perform this task. The penetration testing team may assist to fully understand the identified vulnerabilities.
- The manufacturer's risk management documentation uses the risk rating system which is specified by the manufacturer's QMS. The penetration test findings may not initially be presented by the penetration test provider using this same risk rating system. In this case, it may help to translate the risk to conform to the manufacturer's QMS requirements, considering the finding in the specific context of the device. This may result in adjusting the risk upwards or downwards. Throughout the process, it is important to preserve the original details of the finding.

- Manufacturer risk rating systems generally require that risks be analyzed in terms of their likelihood and impact. Expression of the likelihood of cybersecurity risks in terms of probability has posed a challenge since it involves predicting the future actions of unknown threat actors with unknown and varying motivations. Efforts to objectively estimate the probability of cybersecurity risks can be hampered by limited information on potential unauthorized actors, inherent subjectivity in assessing potential unauthorized actors, and a constantly changing environment over a long period of time that a given device may be in the field. Consequently, many modern standards and certain regulators are now recommending that manufacturers replace "probability"/"likelihood" with "exploitability."
- When translating vulnerability scores from scoring systems such as CVSS (Common Vulnerability Scoring System) to the manufacturer risk rating system, it is important to separate components of the score and translate them into the appropriate metrics.[15] To facilitate translation, it is helpful to include the full vectors or otherwise contain enough detail in the penetration test findings to disaggregate exploitability and impact for purposes of risk translation.
- Organizations may wish to establish two-way, traceable linkages between the penetration test report, with the penetration test findings, and the risk management documentation, which contains information about security controls and risk decisions.
- When penetration test findings have traceability to the risk management file where they are dispositioned, it can help stakeholders, including security engineers and regulatory reviewers, determine whether and how penetration test findings have been assessed and addressed. Similarly, when entries in the risk management file which originate from penetration test findings maintain traceability back to the penetration test report it can enable stakeholders to understand the nature of the risks.

For penetration test findings that could result in patient safety risk, consider:

- These findings are dispositioned through the manufacturer's normal risk management process for safety risk.
- Such findings are only accepted when they meet the standard criteria for safety risk acceptance, such that they have been reduced as low as possible and the benefits outweigh the risk.
- A manufacturer's QMS specifies the criteria used to determine when a security risk that does not result in a safety risk may be deferred for a future update or monitored.
- Formal acceptance of cybersecurity risks in a particular release is documented in the DHF for the device in the manner dictated by the manufacturer's QMS and these risks are monitored (e.g., periodically reevaluated) throughout the device lifecycle for any changes to the risk level.

[15]For example, separate a vulnerability's CVSS Exploitability Metrics, which relate to probability/likelihood, and Impact Metrics, which relate to impact. Directly translating the numerical CVSS score into either probability/likelihood or impact in the risk management file would not be appropriate, as the CVSS score aggregates information related to both categories. The optimal starting point for translation would be the individual metrics, such as the exploitability subscore, which form the basis of the score. In CVSS, these are contained within the full CVSS vector.

2.4.2.2 Determining Impact

The impacts to the device that the penetration testing team was able to directly demonstrate may not fully enumerate the potential impacts that could have been caused. The penetration tester has an inherently limited understanding of the device, whereas the device team has an inherent advantage in extrapolating from the penetration tester's demonstrated findings to a more complete understanding of the potential impacts on the device.

As such, full analysis of the findings of the penetration test can help identify impacts that may not be explicitly stated in the report, but which may be revealed by analyzing the findings in the context of more extensive knowledge of the system. For example, a penetration tester may report that they were able to compromise a particular user account, and as a result, compromise patient information. The device team may realize that, given access to this user account, the penetration tester would have been able to affect the delivery of therapy, even if the penetration tester did not realize this possibility and did not report this impact. By leveraging relevant threat models and critical analyses, an organization can explore the full potential impact of penetration test findings and not limit their response to addressing only the specific impact identified in the penetration test report.

2.4.2.3 Identifying Root Cause

Understanding the root cause of any identified vulnerabilities found is another part of risk assessment, management and rating. If the vulnerability results from software packages or security architecture that is shared with other devices, the device team may choose to initiate a process to notify the appropriate parties to begin an assessment of potential known security vulnerability in the additional devices(s). Sometimes this may result in the device team opening a Corrective Action/ Preventative Action (CAPA) using their organization's established CAPA procedures to determine whether process or other systematic changes are necessary to prevent similar findings in future development.

2.4.2.4 Trend Analysis

Penetration test findings may be aggregated with findings from previous penetration tests and/ or findings from other projects to then perform a trend analysis. If similar penetration test findings occur repeatedly, this may indicate a systematic shortcoming of the manufacturer's Secure Product Development Framework (SPDF) or device team development practices which if addressed could reduce the probability of recurrence of similar vulnerabilities in the future.

Analysis of penetration tests may help determine whether they correspond to a threat which was anticipated in the device's threat model. If the threat was not anticipated in the threat model, the organization can update the threat model to include the threat and then analyze the security controls that apply to that threat. If the threat was anticipated but the penetration tester was still able to exploit an identified vulnerability, it may be necessary to consider modifying security controls.

2.4.2.5 Chained Exploits

A successful exploit is often not the result of a single vulnerability. Frequently, a series of vulnerabilities may be chained to enable an unauthorized actor to progress through an entire attack process from initial reconnaissance to initial foothold, to privilege escalation, and finally to achieving desired effects.

By analyzing the entire attack chain from a penetration test finding, an organization can potentially identify multiple security controls that would interrupt this sequence at multiple points. This enables the organization to implement more effective security controls, such as through defense-in-depth processes.

A Note on "Low" or "Informational" Findings and Vulnerabilities: While information disclosure vulnerabilities may have a "Low" score in CVSS or other scoring systems, or be rated as "Informational," they may provide important information to unauthorized actors for developing or targeting further exploits. The "Low" scored findings may very well be the first link in a chain of exploits which culminate to a "High" or "Critical" finding. This indirect impact can be considered in the cost-benefit analysis when determining whether to remediate such vulnerabilities.

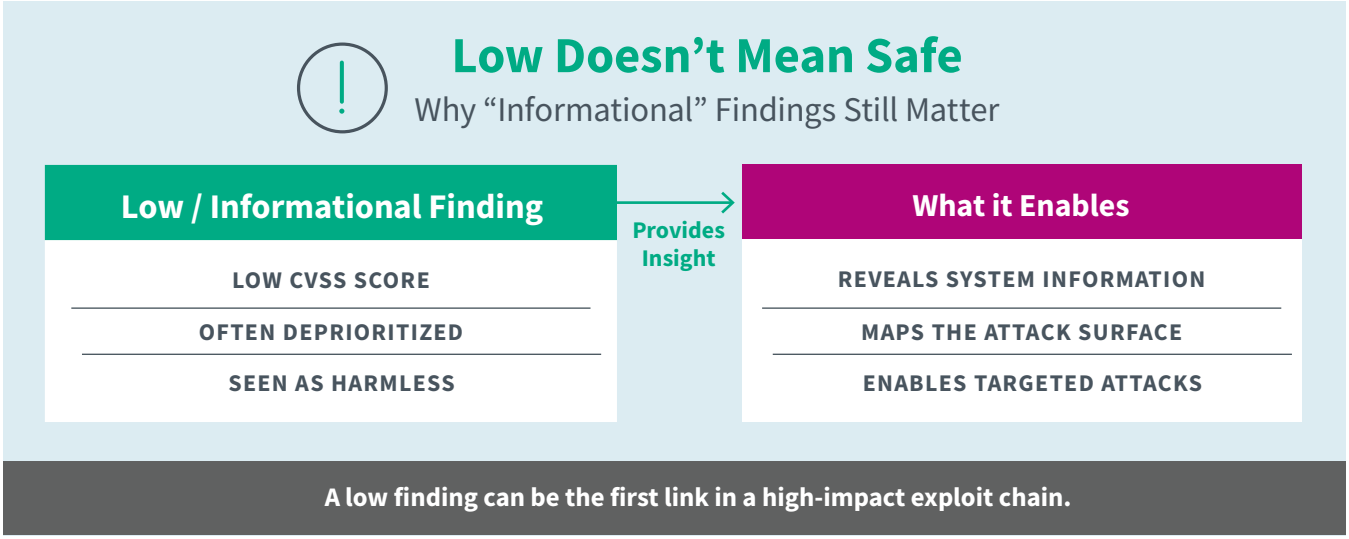

Figure 2. Why Informational Findings Still Matter

2.5 Communicate Penetration Test Results

Communicating penetration testing and results for relevant stakeholders is key for their understanding of the risk a given device poses. The level of detail at which information is provided may vary across stakeholders. For example, step by step actions on how to exploit an identified vulnerability may not be necessary for an HDO (Healthcare Delivery Organization) or all regulators, whereas a summarization of the risk and manufacturer plan to address the risk may be more relevant. Whatever level of detail is used, it is important for organizations to be able to confirm that any mitigation for the identified penetration test findings is effective.

Types of penetration testing communications are explained in the following table:

Penetration Test Artifact	Owner	Confidentiality	Potential Stakeholders
Penetration Testing Summary Report: • Traces disposition of each finding to appropriate records such as change request, new requirement, security risk assessment entry that traces to how a specific risk identified by a finding was accepted. • Raw penetration test report often attached to the cover report to allow the DHF to have full context and traceability.	Development Team	High (raw penetration test report attached)	Device Security, Software Development, Quality Assurance, Business Leaders, Regulators
Raw Penetration Test Report: • Includes scope, testing methodologies, named penetration testers, executive summary and detailed findings including evidence and specific steps of exploitation.	Independent Penetration Test Team	High	Device Security, Software Development, Regulators
Letter of Attestation: • Summary of finding severity levels • If available, final status of identified known vulnerabilities.	Independent Penetration Test Team	Low	Device Security, Software Development, Quality Assurance, Customers, Potential Customers

The more detailed penetration testing results are, the more sensitive they may become. Thus, manufacturers may wish to carefully consider access to artifacts on a "need to know" basis. When sharing outside the organization, Non-Disclosure Agreements (NDAs) may be utilized to legally protect access to sensitive information. However, even with an NDA in place, the organization's control over the security of the information diminishes significantly once the information leaves the organization's boundary. Where possible, consider sharing penetration testing artifacts over a secure channel such as encrypted email or secure file share.

2.5.1 Communicating to Regulators

A detailed penetration test report may be provided as part of a regulatory submission, including:

- testing scope
- date(s) of testing
- methodology, including tools used as well as associated version(s) and configuration information
- system details

- overall risk level including the highest remaining penetration test supplier score and the affirmation that all remaining risks are acceptable based on the organization's security risk management process
- who performed the test along with a description of independence, qualifications and technical expertise
- a POC (point of contact) for additional details
- test results, including all detailed identified vulnerabilities (name, category, severity, score & description).[16]

In addition to the penetration test report, clear penetration test finding disposition information may also be provided to the regulatory authority, including each penetration test finding along with additional details such as:

- Exploitability, severity, and potential safety impact
- Risk decision (i.e., remediate, backlog with target date and tracking record reference, mitigate, defer/monitor, transfer risk)
- Plan to remediate residual risks or rationalization for acceptance

2.5.2 Communicating to Customers

Providing relevant information to potential and current customers supports their ability to make risk-based decisions. To confirm independent penetration testing has been performed on devices, potential customers may request that manufacturers provide a Letter of Attestation. Letters of Attestation typically do not require a Non-Disclosure Agreement (NDA) and typically contain relevant high-level information about the penetration test, including the scope, date(s) of testing, system details, methodology, overall risk level, who performed the test, and contact for additional details.

To further understand penetration test findings, customers may request penetration testing findings, which may require an NDA. When responding to the request, manufacturers may provide a synopsis of the count of finding criticalities the threat ranking methodology (e.g., CVSS), and a mitigation plan and strategy for the findings, including an estimated date of completion.

[16] It may not be necessary to include step by step actions on how to exploit an identified known vulnerability (e.g., exploit code, identified security keys, etc.).

3. Potential Pitfalls

This section details potential pitfalls that may arise when integrating penetration testing into the Secure Product Development Framework (SPDF). The purpose of this section is to help highlight common mistakes and help teams identify and avoid them in the device development process.

1. **Planning and Resourcing Penetration Testing During Development Lifecycle and After Release**

   Planning for and resourcing penetration tests properly takes significant time and preparation. Penetration testing can be expensive, so it is important that organizations plan and allocate a budget. Penetration Test Services may need to be qualified through supplier management or internal quality agreement processes. As a result, it may be helpful to plan and start penetration testing work from the start of a development project being sanctioned so that it can be completed without rushing the testing or delaying the project schedule. Also, penetration testing may need to be completed periodically as part of maintenance to ensure a device's security controls remain effective against the latest real-world attacks and techniques.

2. **Confusing a Vulnerability Scan Report with a Penetration Test Report**

   Security testing includes the use of tools, such as Nessus vulnerability scanners, to identify known vulnerabilities. Vulnerability scan reports contain identified potential known vulnerabilities, but they do not demonstrate how the vulnerability could affect the system. While part of the reconnaissance work to prepare for penetration testing, vulnerability scans by themselves are not considered complete security validation. Security validation is exposing a device to real world attacks by an experienced professional to understand the impact that vulnerabilities may have on a system. The penetration test may use known vulnerabilities identified by vulnerability scans in their work, but they go further to exploit the vulnerabilities and demonstrate impact on the device. A vulnerability scan report is not a penetration test report.

3. **Using Bug Bounty Programs to Replace the Need to Perform Penetration Testing**

   Bug bounty programs encourage finding high severity findings, and as such, do not ensure a comprehensive assessment of the entire system attack surface. Device manufacturers are also not able to control the qualifications of testers, the time invested, or the thoroughness/coverage of testing through bug bounty programs. Additionally, the logistics of making devices, especially physical devices, broadly available for testing by external researchers may not be feasible.

   As such, bug bounty programs are not a feasible replacement for penetration testing. For certain categories of devices, they may be considered an optional complement to formal penetration testing.

4. **Using Penetration Testing to Cover Security Requirements Verification**

   An organization may attempt to consider the penetration test as covering verification of security requirements. However, security requirement verification is not the purpose of penetration testing. Giving security requirements, in untested form, to the penetration tester to verify distracts from the core function of penetration testing – identifying vulnerabilities and other

means to bypass the implemented security controls.

Instead, organizations may complete security verification by the normal software verification team before the penetration test is initiated. Having basic security failures reported so late in the development process may only increase the work needed to ready the device for regulatory submission.

5. **Using Security Requirements Verification Testing to Cover Penetration Testing**

   Security verification testing includes confirmation that identified security requirements were implemented correctly along with the use of tools, such as Nessus vulnerability scanners, to identify known vulnerabilities. This verifies that the security designed into the system has been implemented, but it does not validate that the security design can remain resilient to real-world attacks. Penetration testing supports validation of a device's security design. Similar to human factors, penetration testing exposes the device to real world use conditions to see if the security controls maintain device resilience. See the discussion in the introduction of this document for additional information.

6. **Limited Test Reports**

   While the goal of penetration testing is to find means an actor might use to access and/or misuse a device, if the tester only reports on what was broken, it can give a misleading characterization of security preparedness.

   It is helpful for the penetration tester to report on the techniques that they attempted, and the device was resilient to, as it provides a more comprehensive picture of the device's baseline security.

7. **Using the Real Environment or Real Patient Data**

   Ideally penetration testing is not performed on the production environment, nor does it involve actual patient data. This is because of the potential for unintentionally disrupting the availability of the system under test. It may also modify data and in some cases cause cross pollution of data across accounts, including sensitive patient data.

8. **Limited Review of the Penetration Testing Results by the Receiving Organization**

   Understanding the penetration testing results in their entirety includes reviewing and assessing all findings from the penetration test. If the penetration test is not fully reviewed, organizations may dismiss some findings as "non-reproducible" or otherwise irrelevant.

   Part of this review and assessment may include dialogue between the penetration tester and the development team to discuss complex findings which may be difficult to reproduce. Use of an agreed upon standard scoring mechanism for severity identification may increase the efficiency and usability of results. This is particularly important when the penetration tester is a third party and is billing their work by the hour.

9. **Limiting Penetration Testing Only to Unauthorized Users**

   Optimal penetration testing is scoped to include the possible behaviors of intended/authorized users to conduct unintended behaviors. A penetration test may include simulating unauthorized use with valid access such as a patient with valid credentials to a cloud service attempting to expose health data of other patients.

4. References

Title	Key section(s)
AAMI — TIR 57:2016, Principles for Medical Device Security—Risk Management	3.4 (Plan), 4.3.2 (Identification of vulnerabilities), 7 (Evaluation of Overall Security Risk Acceptability)
AAMI — TIR 97:2019, Principles for Medical Device Security—Postmarket Risk Management for Device Manufacturers	Appendix B.2.2 (Active Monitoring)
ANSI/AAMI — SW96:2023, Standard for Medical Device Security—Security Risk Management for Device Manufacturers	Entire document applies
UL — UL 2900-1-1, Standard for Medical Device Security – Part 1-1: Security Risk Management for Medical Devices, April 2023	16 *Structured Penetration Testing*
UL — UL 2900-2-1, Standard for Medical Device Security – Part 2-1: Particular Requirements for Network-Connectable Medical Devices, September 2023	16 *Structured Penetration Testing*
U.S. Food and Drug Administration (FDA) — Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions, 2023	Cybersecurity Testing, Security Assessment of Unresolved Anomalies
Medical Device Coordination Group (MDCG) — MDCG 2019-16, Guidance on Cybersecurity for Medical Devices, January 2020	"Methods can include security feature testing, fuzz testing, vulnerability scanning and penetration testing." *"According to ENISA, penetration testing is the assessment of the security of a system against different types of attacks performed by an authorized security expert. The tester attempts to identify and exploit the system's vulnerabilities."*
International Medical Device Regulators Forum (IMDRF) — Principles and Practices for Medical Device Cybersecurity, March 2020	Section 5.3 *Security Testing* "Conduct technical security analyses (e.g., penetration testing). These include efforts to identify unknown vulnerabilities through fuzz testing, for example; or checks for alternative entry points, e.g., by reading hidden files, configuration, data streams or hardware registers."

Title	Key section(s)
International Electrotechnical Commission (IEC) — IEC 81001-5-1, Health Software and Health IT Systems Safety, Effectiveness and Security — Part 5-1: Security — Activities in the Product Life Cycle, December 2021	5.7 *Software System Testing*, 5.7.4 *Penetration Testing* "The manufacturer shall establish an ACTIVITY (or ACTIVITIES) to identify and characterize WEAKNESSES via tests that focus on discovering and exploiting SECURITY VULNERABILITIES in the HEALTH SOFTWARE."
International Electrotechnical Commission (IEC) — IEC 62443-4-1, Security for Industrial Automation and Control Systems — Part 4-1: Secure Product Development Lifecycle Requirements, January 2018	9.5 SVV-4: Penetration testing
Health Canada Guidance Document: Pre-market Requirements for Medical Device Cybersecurity, June 2019	"Structured Penetration Testing: This type of testing requires a cybersecurity expert who is familiar with hacking techniques (i.e., white hat or ethical hacker). The cybersecurity expert attempts to circumvent the layers of defense that were designed into the device. "
Therapeutic Goods Administration (TGA), Australia — Medical Device Cyber Security Guidance for Industry, Version 1.1, March 2021	Sections *Cybersecurity Assessment and Penetration Testing*
Cyber Security Agency of Singapore (CSA) — Cybersecurity Labeling Scheme for Medical Devices, October 2022	See latest update at https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cls-md

Title	Key section(s)
National Medical Products Administration (NMPA), China — Medical Device Cybersecurity Guidance, 2023 (translated excerpts privided for convenience)	（五）网络安全验证与确认 (V) Cybersecurity verification and validation 网络安全验证与确认作为软件验证与确认的重要组成部分，需在软 与确认的框架下，结合产品网络安全特性开展相关质控工作，如源代 审核、威胁建模、漏洞扫描、渗透测试、模糊测试等。软件验证与确 要求详见医疗器械软件指导原则第二章。 As an important part of software verification and validation, cybe verification and validation require relevant quality control to be conduc the framework of software verification and validation and in combina product cybersecurity features, such as source code security audit, threat vulnerability scanning, penetration testing, and fuzzy testing, etc. For requirements for software verification and validation, please refer to Cha the *Guidance for Registration Review of Medical Device Software*. 注册申请人需针对不同类型网络威胁，采用相应技术手段来保证医 的网络安全。例如：针对读取攻击、操作攻击、欺骗攻击、泛洪攻击 向、勒索攻击等网络威胁，可采用用户访问控制、端口与服务关闭 数字签名、标准协议、校验、防火墙、入侵检测、恶意代码防护、网 配置等方法与技术来保证产品的网络安全。 Registration applicants shall adopt corresponding technical means to e cybersecurity of medical devices for different types of network thr example: for reading attack, operation attack, trick attack, floodin redirection, ransomware attack and other network threats, registration a

Discover more at mdic.org