NISTIR 8023

Risk Management for Replication Devices

Kelley Dempsey
Celia Paulsen

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8023

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8023

Risk Management for Replication Devices

Kelley Dempsey
Celia Paulsen
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8023

February 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director

National Institute of Standards and Technology Internal Report 8023
30 pages (February 2015)

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8023

Please forward any questions or comments to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: sec-cert@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

This publication provides guidance on protecting the confidentiality, integrity, and availability of information processed, stored, or transmitted on replication devices (RDs). It suggests appropriate countermeasures in the context of the System Development Life Cycle. A security risk assessment template in table and flowchart format is also provided to help organizations determine the risk associated with replication devices.

Keywords

3D printers; 3D scanners; copiers; countermeasures; exploits; mitigation; multifunction devices; printers; replication devices; risk; risk assessment; risk management; scanners; security controls; System Development Life Cycle; threats; vulnerabilities.

Table of Contents

1. Introduction

A replication device (RD) is any device that reproduces (e.g., copies, prints, scans) documents, images, or objects from an electronic or physical source. For the purposes of this NISTIR, RDs include copiers, printers, three-dimensional (3D) printers, scanners, 3D scanners, as well as multifunction machines when used as a copier, printer, or scanner. RDs in use within organizations run the gamut in terms of age and functionality. Older, single-function devices may have no internal, nonvolatile storage and cannot be networked. Other devices may provide a variety of functions, be network-connected, run commercially available operating systems, contain internal, nonvolatile storage, and contain embedded internal print servers and web server capability. In between the two extremes, there may be RDs with network and/or storage functionality but no discernable means to configure them securely. Additionally, many organizations may not have an accurate inventory of RDs or recognize what functionality each device possesses, especially with respect to information (data) storage, processing, and transmission.

Managing the risks associated with RDs requires a basic understanding of threats, vulnerabilities, potential impact and likelihood of an event, and the identification and implementation of countermeasures or mitigation strategies. This publication provides guidance on protecting the confidentiality, integrity, and availability of information processed, stored, or transmitted on RDs.

1.1 Background

Historically, the capabilities of RDs were limited to basic copying, scanning, and printing. Storage of scanned or printed information within the RDs was not part of the device functionality and RDs were locally (directly) connected to computers via a cable or were stand-alone devices so the security of information processed by RDs was generally not a consideration for most organizations. Today, however, RDs are often connected to organizational networks, have central processing units that run common commercial operating systems, store information internally on nonvolatile storage media, and may even have internal servers or routers. As a result, RDs may be vulnerable to a number of exploits if the risk is not mitigated using appropriate security practices/controls.

1.2 Purpose and Applicability

RDs are found throughout most organizations and are components included in many information systems. This document provides a brief discussion of vulnerabilities and exploits associated with RDs and provides a set of security practices/controls that can be implemented to mitigate risks.

All RDs are within the scope of this document, including multifunction devices or software applications for using tablets or cell phones as copiers/scanners, but the guidance in this document is only applicable to the copy/print/scan functions of those devices. Other functions,

such as email, web server, or faxing capabilities, are mentioned only as they relate to the security of the copy/print/scan functions.

1.3 Target Audience

This publication serves individuals responsible for the purchase, installation, configuration, maintenance, disposition, and security of RDs including:

- Individuals with acquisition responsibilities;
- Individuals with system administration responsibilities;
- Individuals with information system and security control assessment and monitoring responsibilities; and
- Individuals with information security implementation and operational responsibilities.

This publication assumes the target audience has a working knowledge of information technology and information security terms and best practices. For definitions of unfamiliar terms, please see NIST IR 7298, *Glossary of Key Information Security Terms*.

1.4 Document Structure

This publication is structured as follows:

- Section 2 describes potential threats and vulnerabilities;
- Section 3 presents considerations to help identify potential risk mitigation strategies.
- Appendix A is a glossary of key terms.
- Appendix B provides a means to help conduct a risk analysis on RDs using an example template.
- Appendix C defines key roles and responsibilities for conducting a risk assessment on RDs.

2. Threats and Vulnerabilities

RDs may be vulnerable to multiple threat vectors that can be used to compromise organizational information or disrupt the device. Appendix B of this document provides a template for analyzing vulnerabilities and determining the risk associated with a RD.

2.1 General Threats and Vulnerabilities

The following are general threats, vulnerabilities, and related exploits that may affect RDs:

- Default administration/configuration password: Many devices have default passwords which can be easily obtained and used to access configuration panels, stored data, or to control the device locally or remotely via a web interface.

- Data capture: When data is transmitted or stored unencrypted, it is subject to interception. This data may include device passwords, configuration settings, or processed jobs. Such data may appear to be unreadable but is an exploitable vulnerability if it is not encrypted.

- Disruption of service: RDs may be susceptible to a variety of threats which disrupt the availability of services. User interfaces, power consumption, and internal mechanical and software operations may be especially vulnerable.

- Spam: Most RDs, if not properly configured, will process any submitted job, without regard to the originator, without confirmation that the job is authorized, and without authentication. If exploited, this vulnerability may waste ink, paper, toner, or other materials while also resulting in a denial of service for legitimate users.

- Alteration/corruption of data: Exploits of this nature may be very difficult to detect, but could result in reduced quality, a denial of service (for example, if a password is altered), or a potentially hazardous situation (for example, if configuration settings are altered to allow the device to overheat).

- Outdated and/or unpatched operating systems and firmware: Many RDs run an embedded commercial operating system which renders them subject to the same threats and vulnerabilities as any other computing device running those same operating systems. To complicate matters, RD manufacturers may embed versions of operating systems for which the operating system provider is no longer providing updates or the functionality to install patches or updates is not available. Buffer overflows, execution of arbitrary code, and taking control of the device using remote administration capabilities via web server/site are but a few examples of exploits to which RDs with unpatched operating systems and firmware are vulnerable.

The National Institute of Standards and Technology (NIST) National Vulnerability Database (nvd.nist.gov) lists many specific vulnerabilities that affect RDs produced by multiple manufacturers. The impact of a compromise depends on the information the device handles or

processes as well as the capabilities of the device. A compromise may affect the confidentiality, integrity, or availability of both the device and the information it processes, stores, or transmits. For example, while confidentiality of the information processed may be a primary concern with regard to a small device used to copy personally identifiable information, integrity of the device may be a greater concern with regard to a 3D printer which uses metal powders to create marketing materials. When evaluating risk associated with a RD and determining what countermeasures are appropriate for the device, it is important to understand its intended use and capabilities as well as the impact levels of the information to be processed, stored, or transmitted. See FIPS 199 and NIST SP 800-60 for more information on impact levels and information types.

2.2 Network Connectivity Threats and Vulnerabilities

Many threats and vulnerabilities are related to network connectivity. Connecting RDs to organizational networks is convenient and may be more cost-effective than each individual user having a locally connected device. Cost savings may also be realized by allowing users to manage, access, and monitor a device from a distance. However, with network connectivity comes greater risk of exposing the device, information, and any connected systems to threats. Some potential threats, vulnerabilities, and related exploits associated with network connectivity include:

- Unencrypted information: Unencrypted information is subject to unauthorized exposure and modification. Any information, including configuration data or passwords, sent unencrypted to a RD could be intercepted, exposed, and/or altered.

- Open ports/protocols: Open ports and protocols allow data to flow to and from a device. When unused ports/protocols are not disabled, attackers may be able to access a machine undetected. Repudiation issues (e.g., removing origination information from file metadata, deleting entries from usage logs), data tampering, exposure of management consoles, network bouncing (hiding the source of a user's network connection), information disclosure, or denial of service are some of the associated potential security incidents.

- Denial of service (DoS): RDs connected to the Internet may be more vulnerable to this threat which results in devices being temporarily unusable.

- Wireless connectivity: Wireless functionality allows communications via Bluetooth or 802.11 to other devices or with the Internet. As with wired RDs, if not encrypted, these communications may potentially be intercepted.

- Access permissions: Anyone with the necessary equipment and access can potentially compromise a RD. Some RDs allow remote access for automatic updates, configuration changes, or maintenance. If access is not controlled or automatic downloads verified, this capability could be used to install malware or rootkits, gain access to other areas of the network, compromise configuration settings including passwords, disable a device, or expose stored information.

- Botnets: RDs' memory and processing power may be used as part of DoS botnets to attack organizational assets on the same network and/or the assets of external organizations.

- Hop/Relay Points: RDs that have been compromised may be used to reach other organizational assets on the same network or to conceal the actual point of origin of an attack on external networks.

2.3 Nonvolatile Storage Media Threats and Vulnerabilities

Many RDs use nonvolatile storage media to manage jobs and control the device. Potentially all of the information that was ever processed, stored, or transmitted by the device could remain in the nonvolatile storage indefinitely. Nonvolatile storage media for RDs is most often in the form of a hard disk drive or solid state drive.[1] Some RDs may also provide for use of removable solid state memory cards or flash drives. Information stored within a RD may leave organizational information vulnerable to numerous exploits and compromises of confidentiality or integrity. Some potential threats, vulnerabilities, and related exploits associated with storage media include:

- Unencrypted information: Any information stored unencrypted on a RD could be exposed and/or modified by anyone with access (including maintenance personnel) or in the event of a successful network-based attack.

- Sanitization: Information could be retrieved by unauthorized personnel when the RD or nonvolatile storage media is disposed, warehoused, or repurposed.

- Access: External maintenance or other personnel given physical or remote access to the RD could download or copy stored information. Removable storage media (e.g. memory cards or flash drives) may be especially vulnerable to exploits involving theft or alteration/corruption of data.

- Unauthorized Storage: RDs that have been compromised may be used to store unauthorized data in memory. Such data has typically been illegally obtained (e.g., copyrighted data, intellectual property).

[1] Note that while dynamic random-access memory (DRAM) -based Solid State Drives (SSDs) could be used in RDs, they are based on volatile memory and thus information is not retained on the DRAM-based SSDs without a constant supply of power.

3. Risk Management Activities throughout the SDLC

It is important to consider information security in each stage of the system development life cycle[2] and build security in at the earliest stages possible. In order to manage risks associated with RDs, it is important to consider the capabilities and security functionality of the device along with the security posture, system/information impact levels, and risk tolerance of the organization when identifying appropriate devices to acquire. The following sections contain basic steps to help organizations identify and implement appropriate risk management strategies.

3.1 Initiation

During the Initiation Phase, determine how the device will be used. Key questions to consider include:

- Who will use the device and where will it be located?
- Will the device be connected to a network?
- What is the impact level (i.e., low, moderate, or high as defined in FIPS 199) of the information to be processed, stored, and/or transmitted by the device?
- What kinds of capabilities (e.g., high-capacity, network connection, ability to handle special materials) are needed for the device to perform its intended functions?
- Will the device be purchased or leased?
- What security controls are needed to protect the confidentiality, integrity, and availability of both the device and the information to be processed, stored, and/or transmitted by the device at the appropriate impact level?
- What device functionality is needed to support security requirements and provide security at the appropriate impact level?
- Does the organization want or need a service contract for the device? How much control does the organization have over the terms of the service agreement (e.g., can the organization independently vet service technicians?)
- What skills/personnel are needed to install, configure, manage, maintain, and secure the device?
- Will the staff require training on how to install, configure, manage, maintain, and secure the device?

[2] The system development life cycle is described in NIST SP 800-64.

Include the owner and/or end user(s) of the device as well as information technology and security staff in the initiation process. There will likely be several areas where there may be some flexibility or uncertainty depending on the device chosen for acquisition. Document these areas for use during the development/acquisition phase.

3.2 Development/Acquisition

During the Development/Acquisition Phase, the organization investigates and considers available security options with respect to how the device will be used, as described in the previous phase. During this phase, several options may be weighed and alternatives chosen based on both security and functionality requirements as well as cost.

When security options are not available, compensating security controls may be required to ensure security at the appropriate level.[3] For example, if a device does not have a space for a chain or cord for physical protection, placing the device in a secure area may suffice. If implementation of compensating controls is not feasible, the organization considers whether a gap between the security functions offered by the device and the security functions needed to meet security requirements is a risk that is acceptable to the organization.

Some security functions to consider include:

- Editable configuration settings[4];
- Secure configuration provided by the manufacturer;
- Image overwrite capability;
- Physical protection capability (e.g., ability to be bolted to the floor or secured with a chain and padlock);
- Physical protection for nonvolatile storage media (e.g., requires a lock to access the hard drive);
- Ability to maintain the RD by internal staff and/or maintenance support throughout its expected life span (including software patches, replacement parts, etc.);
- Ability to encrypt information while in transmission or storage (including passwords, configuration settings, and user files);
- Activity monitoring with alerts/triggers (e.g., automatically block suspicious activity);
- Audit record (event logging) capability;

[3] NIST SP 800-53 provides a comprehensive set of security controls.
[4] In cases where there are multiple operating systems (OS) or virtual machines (VM) on a device, the organization should carefully consider whether each OS or VM can be configured securely.

- Authentication capabilities (e.g., password/pin, smart card, proximity badge);
- Access control levels/roles (e.g., administrative/privileged access, user access);
- Ability to configure network/port settings;
- Tamper evident solutions (e.g., anti-lift ink, copy-void pantograph); and
- Automatic safety shutdown (e.g., when overheating).

Inspect the device for defects, delivery errors (e.g., wrong version), and malware before accepting delivery. Once acquired, include networked/wireless RDs and those with nonvolatile storage in the associated system security plan. Document device information, supply chain (e.g., distributer) information, default and customized configuration settings, security/usage policies, and any other information related to the acquisition and security requirements of the device.

3.3 Implementation

Before placing the device into operation, configure the RD securely and implement appropriate security controls. There are numerous secure installation and configuration practices to consider and implement. Each device may have unique capabilities and security options. Some practices to consider (with associated NIST SP 800-53 security controls in parentheses) include:

- Review and apply the manufacturer-recommended secure configuration as appropriate/if available
    - Actively communicate with the original equipment manufacturer (OEM) as necessary to calibrate and configure the device (CM-6);
    - Isolate the device from other systems until it is calibrated and securely configured (SC-7);
    - Remove unwanted applications from the device, e.g., internet browsers, games (CM-7); and
    - Apply standardized secure configurations for RDs as available (http://web.nvd.nist.gov/view/ncp/repository) (CM-2, CM-6);
- Enable and configure encryption
    - Enable network encryption protocols, e.g., TLS/SSL, IPSec, WPA2 (AC-18, SC-8, SC-13);
    - Encrypt passwords and other configuration settings (IA-7, SC-8, SC-13); and
    - Configure encryption for nonvolatile storage (SC-13, SC-28);
- Place a warning sticker on the device to inform/remind users about the nonvolatile storage (MP-3). Instructions on how to invoke an immediate image overwrite may be included if applicable;
- Limit/restrict access

- Review user accounts and privileges (AC-2);
- Limit administrative/privileged access to a primary and secondary administrator (AC-6); and
- Restrict users and service technicians from being able to change the configuration settings (CM-5);
- Restrict/disable remote access, e.g., by vendor/service technicians (AC-17, MA-4);
- Disable any call-home features, e.g., do not allow monitoring of usage by the manufacturer (MA-4);
- Disable wireless network identifier broadcasting and network auto-connect (AC-18);
- Limit or disable file sharing (CM-7);
- Disable unused physical and network ports (CM-7);
- Implement physical security, e.g., locks (PE-3); and
- Whitelist/blacklist specific MAC addresses, IP addresses/address ranges, or email addresses (AC-18, SC-7);

- Enable identification and authentication
  - Require identification and authentication for privileged access (IA-2, IA-4, IA-5)
  - Change vendor default passwords (IA-5);
  - Implement authenticated retrieval for users, i.e., push/pull printing (IA-2);

- Configure image overwrite capability
  - Enable immediate image overwrite (MP-6); and
  - Schedule regular off-hours overwrite with three-pass minimum (MP-6);

- Enable auditing, i.e., event logging (AU-2, AU-3, AU-12); and

- Configure monitoring/error handling capabilities
  - Dump memory on reboot (SI-16);
  - Alert administrator of errors (SI-11);
  - Block repeated requests, i.e., denial of service attack (SC-5); and
  - Enable time-out of queued or stored jobs (AC-12).

3.4 Operation/Maintenance

Compromises to a device often occur while it is in the operation/maintenance phase. Outdated or unpatched software and firmware is a common vulnerability. Review vendor security bulletins or alerts on a regular basis and ensure appropriate personnel evaluate and install patches and upgrades as needed. Document a procedure and schedule for implementing updates/upgrades.

Identifying whether a device has been compromised can be challenging. Regularly scan RDs for known vulnerabilities. Review audit records/event logs regularly and investigate any suspicious activity. When possible, compare device activity with similar devices processing similar workloads. Some warning signs that may indicate misuse or a compromise include:

- Display malfunctions or shows incorrect information;
- Materials (ink, paper, or other supplies) run out faster than usual;
- Increased number of failed or timed-out jobs;
- Unexplained/unauthorized changes in configuration settings;
- Device completes processes slower than expected;
- Device uses more network time/bandwidth than usual;
- Time stamps do not align or make logical sense;
- Communications with unknown IP or email addresses increase; and
- Physical markings around key areas of the device (e.g., nonvolatile storage compartment, display area).

3.5 Disposal

It is best to obtain an estimate from the original equipment manufacturer (OEM) prior to acquisition on what the expected life of a RD is and how long they expect to support it (e.g., provide patches). Sanitize RDs when they are no longer needed by an organization or will be repurposed or stored by doing the following (with associated NIST SP 800-53 security controls in parentheses):

- Wipe/purge or destroy nonvolatile storage media (MP-6);
- Change or reset passwords and other authentication information, e.g., user pins (IA-5); and
- Reset configurations to factory default settings (CM-6).

3.6 Service Contracts/Lease Agreements

The security considerations for acquiring a RD noted in previous sections also apply to leased devices. Furthermore, some additional considerations may apply and be included in service contracts/lease agreements as follows (with associated NIST SP 800-53 security controls in parentheses):

- Remove any nonvolatile storage from the device before the device can leave the organization for repair (MA-2, MA-5, MP-6);

- Sanitize nonvolatile storage before vendor technicians are allowed access to the device for maintenance (MA-2, MA-5, MP-6);

- Do not permit vendor technicians to remove organizational information (including passwords, configuration settings) in any form (MA-2, MA-5, MP-6); and

- Escort and monitor vendor technicians to ensure that they do not violate contractual agreements and to monitor for potential change or removal of any information (including nonvolatile storage, passwords, network or configuration settings) (MA-2, MA-5).

4. Conclusion

It is important to understand risks before the acquisition of an RD. To manage risk for existing RDs that do not currently meet an organization's minimum security requirements, organizations consider replacement as soon as resources allow and in the interim, implement compensating controls (e.g., install a firewall for networked RDs that can't be patched/updated and/or don't provide encryption functionality, renegotiate the service contract or lease agreement, escort service technicians at all times).

The risks associated with owning and using RDs continually evolve. As technology, the operational environment, and an organization changes, the threats, vulnerabilities, potential impact and likelihood of an event may also change. Organizations assess their risk both when acquiring an RD, and on a regular basis thereafter to ensure the implementation of appropriate countermeasures or mitigation strategies.

Appendix A - References

PUBLICATIONS[5]	
NIST FIPS 140	National Institute of Standards and Technology Federal Information Processing Standards Publication 140, *Security Requirements for Cryptographic Modules.* http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
NIST FIPS 199	National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
NIST IR 7298	National Institute of Standards and Technology Interagency Report 7298, *Glossary of Key Information Security Terms*. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
NIST SP 800-30	National Institute of Standards and Technology, Special Publication 800-30, *Guide for Conducting Risk Assessments*. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
NIST SP 800-39	National Institute of Standards and Technology, Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
NIST SP 800-53	National Institute of Standards and Technology, Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems.* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
NIST SP 800-60	National Institute of Standards and Technology, Special Publication 800-60, *Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories.* http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf *Volume 2: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.* http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf
NIST SP 800-64	National Institute of Standards and Technology, Special Publication 800-64, *Security Considerations in the System Development Life Cycle*. http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
NIST SP 800-88	National Institute of Standards and Technology, Special Publication 800-88, *Guidelines for Media Sanitization.* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

[5] Versions of all referenced publications are as amended. Current versions are at http://csrc.nist.gov/.

NIST SP 800-161 National Institute of Standards and Technology, Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. http://csrc.nist.gov/publications/drafts/800-161/sp800_161_2nd_draft.pdf

WEBSITES/LINKS

National Vulnerability Database: http://nvd.nist.gov/

National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

Appendix B – Sample Security Risk Assessment

Important Note: The risk assessment table and flowchart provide examples/starting points for conducting focused information security risk assessments on replication devices (RDs). Organizations are encouraged to add/revise/remove questions and assumptions, recalibrate the risk scores, and make any other revisions needed to accommodate organizational requirements and specific environments of operation.

Assumptions:

- The location (physical and logical) and uses of RDs being assessed are known.
- Make, model, and capabilities of devices are known (or the information is available).
- Security control/configuration status of devices is known (access, authentication, etc.).
- Connectivity status of devices is known.

Risk Score:

Risk is a function of threat, vulnerability, impact, and likelihood. The risk scores used in this appendix may not accurately reflect an organization's specific risk environment and should be modified as appropriate. This appendix uses a scaled risk score from 0 to 5 in order to calculate a qualitative overall risk level. Other risk scales may be used depending on the needs of the organization.

0 = Negligible Risk

1 = Very Low Risk

2 = Low Risk

3 = Moderate Risk

4 = High Risk

5 = Very High Risk

Instructions:

- Answer all questions as though the RD has been acquired and integrated.
- If a score of 1 or higher is entered in the "Risk Score" column, an action to be taken or a justification for risk acceptance is entered in the last column.

Security Risk Assessment Table for Replication Devices (RDs)

Replication Device Information

Manufacturer and Model:

Associated System ID:

Assessment Information

Date of Assessment:

Name(s) of Assessor(s):

#	Risk-Related Question	Yes, No, or N/A	Risk Score	Accept Risk? (Y/N)*	Action** or Justification for Risk Acceptance
	PLANNING/SECURE CONFIGURATION				
1	Is the device included within a system security plan with applicable controls implemented?		(Yes=0; No=4)		
2	Does the device or its control software have any relevant security certifications (e.g., Common Criteria)?		(Yes=0; No=1)		
3	Does the vendor/manufacturer provide information on a secure configuration for the device?		(Yes=0; No=1)		
3.1	If a secure configuration is available, has it been implemented on the device?		(Yes=0; No=2)		
	THIRD PARTIES				
4	Is the device leased by the organization? (N/A if the organization owns the device)		(Yes=3; No=0)		
4.1	If leased, does the lease agreement stipulate federal ownership of storage devices internal to the device? (N/A if the organization owns the device)		(Yes=0; No=4)		
5	Is the device under a service contract?		(Yes=0; no=2)		
5.1	If under service contract, does the service contract stipulate that hard disk drives (HDDs) and solid state/nonvolatile storage must be removed before the device can leave		(Yes=0; no=5)		

#	Risk-Related Question	Yes, No, or N/A	Risk Score	Accept Risk? (Y/N)*	Action** or Justification for Risk Acceptance
	organizational control? (N/A if not under contract)				
5.2	If under service contract, does the service contract stipulate that service technicians are not permitted to remove information stored within the device in any form? (N/A if not under contract)		(Yes=0; No=2)		
5.3	If under service contract, does the service contract stipulate that only Original Equipment Manufacturer (OEM) or OEM-approved replacement parts should be used? (N/A if not under contract)		(Yes=0; No=3)		
6	If not under service contract, are policies and procedures in place regarding media sanitization/removal of storage media requirements before the device or storage media can leave organizational control?		(Yes=0; No=5)		
	DEVICE STORAGE				
7	Does the device have a hard disk drive (HDD) or solid state/nonvolatile storage media?		(Yes=4; No=0)		
7.1	Is the device storage media easily physically accessible (i.e., no disassembly/tools needed)?		(Yes=2; No=0)		
7.2	Can stored information be logically accessed / viewed (either at the device console or via web access)?		(Yes=2; No=0)		
7.3	Is the device storage media encrypted using approved encryption standards (i.e., FIPS 140 validation or Common Criteria certification)?		(Yes=0; No=4)		
8	Are the device configuration settings encrypted using approved encryption standards (i.e., FIPS 140 validation or Common Criteria certification)?		(Yes=0; No=2)		
9	Does the device provide image overwrite capabilities?		(Yes=0; No=5)		
9.1	If available, is image overwrite capability enabled? (N/A if not available)		(Yes=0; No=4)		
9.2	If available, is immediate data overwrite capability enabled? (N/A if not available)		(Yes=0; No=3)		

#	Risk-Related Question	Yes, No, or N/A	Risk Score	Accept Risk? (Y/N)*	Action** or Justification for Risk Acceptance
10	Does the device dump memory of replicated documents/images/objects on reboot?		(Yes=0; No=2)		
	NETWORK				
11	Is the device connected to a network?		(Yes=4; No=0)		
11.1	Is network communication encrypted using organization-approved network protocols (e.g., IPSec, SSL/TLS, WPA2)?		(Yes=0; No=5)		
11.2	Is privileged access from a network encrypted using organization-approved standards (i.e., FIPS 140 validation or Common Criteria certification)?		(Yes=0; No=2)		
11.3	Does the device prevent communications **to** unknown/unwanted addresses? (whitelist/blacklist)		(Yes=0; No=2)		
11.4	Does the device prevent communications **from** unknown/unwanted addresses? (whitelist/blacklist)		(Yes=0; No=4)		
11.5	Is the device protected by a firewall?		(Yes=0; No=2)		
11.6	Does the device allow remote configuration?		(Yes=4; No=0)		
11.7	Does the device allow call-home features?		(Yes=2; No=0)		
11.8	Does the device allow remote monitoring?		(Yes=3; No=0)		
12	Is the device connected via wireless (e.g., Bluetooth, 802.11)?		(Yes=4; No=0)		
12.1	Is the wireless identifier broadcasting disabled?		(Yes=0; No=4)		
13	Does the device allow external access by vendor technicians (for troubleshooting, updates, etc.)?		(Yes=2; No=0)		
13.1	Does the device or vendor *require* external access?		(Yes=4; No=0)		
14	Does the device have unused, open ports?		(Yes=5; No=0)		
	SOFTWARE/FIRMWARE				

#	Risk-Related Question	Yes, No, or N/A	Risk Score	Accept Risk? (Y/N)*	Action** or Justification for Risk Acceptance
15	Can the device be patched/updated?		(Yes=0; No=4)		
15.1	Must the device be patched by manufacturer's technicians?		(Yes=2; No=0)		
16	Can the print server be securely configured? (N/A if no print server)		(Yes=0; No=3)		
16.1	Can the print server be patched/updated? (N/A if no print server)		(Yes=0; No=4)		
16.2	Must the print server be patched by manufacturer's technicians? (N/A if no print server)		(Yes=2; No=0)		
17	Is the device included in the organization's patch management program to keep software and firmware up to date?		(Yes=0; No=5)		
18	Is the device scanned for vulnerabilities with the organizationally required frequency?		(Yes=0; No=4)		
	PHYSICAL SECURITY				
19	Is physical access to the device controlled (e.g., in a locked room)?		(Yes=0; No=2)		
20	Is physical access to internal device storage media controlled (e.g., using locks)?		(Yes=0; No=2)		
21	Are materials (e.g., paper, ink, filament) secured within the device?		(Yes=0; No=1)		
22	Does the device use sensitive or potentially hazardous materials or components (e.g., metal powder, laser, battery)?		(Yes=1; No=0)		
22.1	Are the sensitive or potentially hazardous materials or components secured within the device? (N/A if no sensitive or hazardous materials or components)		(Yes=0; No=3)		
	ACCESS CONTROL				
23	Is logical access to the device storage controlled (e.g., using passwords, PINs, user accounts or roles, etc.)?		(Yes=0; No=2)		
24	Is access to the device settings (configuration) controlled (e.g., using passwords, PINs, etc.)?		(Yes=0; No=2)		
25	Have all vendor default passwords been changed?		(Yes=0; No=4)		

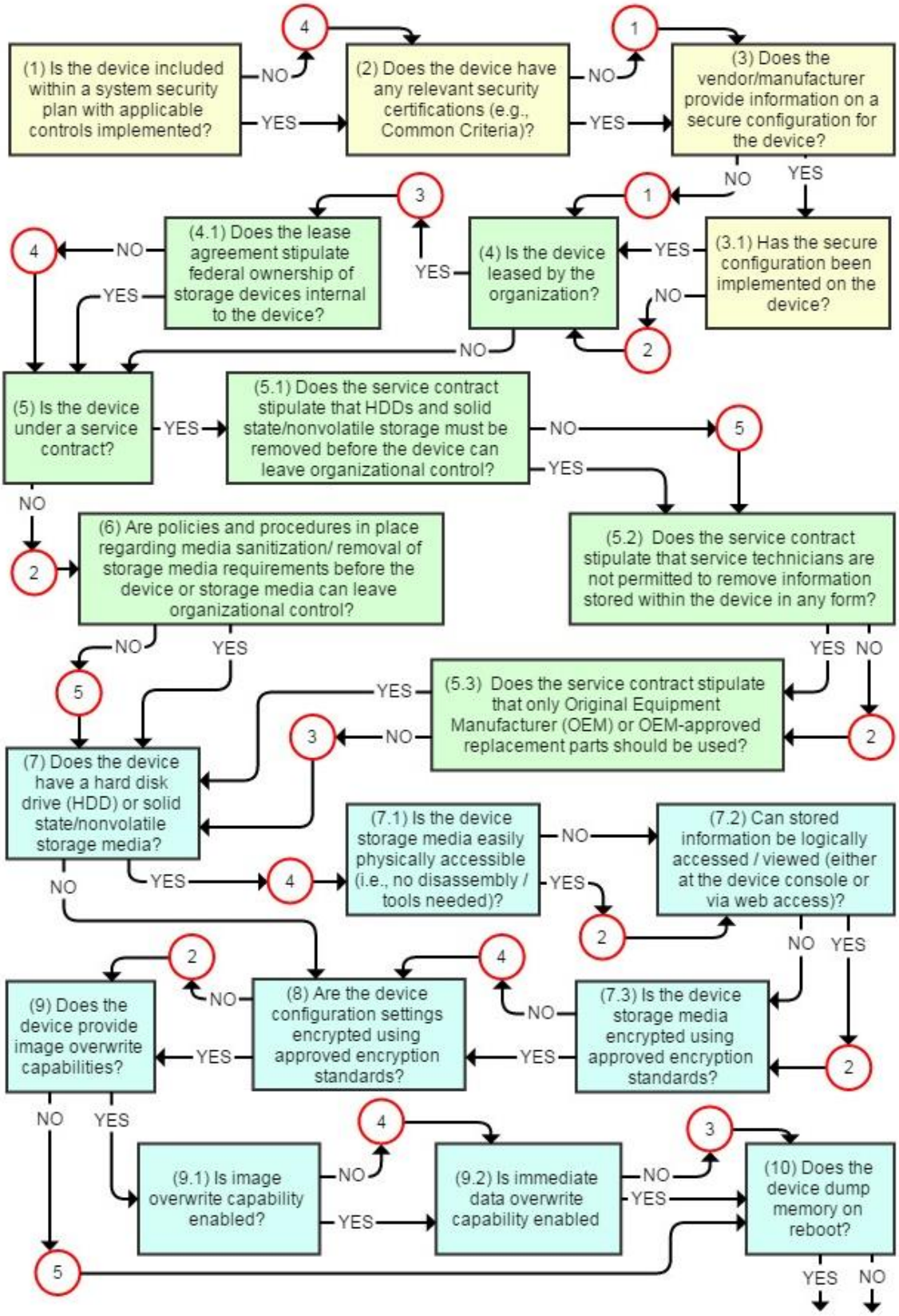
#	Risk-Related Question	Yes, No, or N/A	Risk Score	Accept Risk? (Y/N)*	Action** or Justification for Risk Acceptance
26	If available, is privileged access (physical and logical) to the device limited to designated trained and knowledgeable staff? (N/A if not available)		(Yes=0; No=3)		
27	Is in-person user verification required to complete a job (i.e., push/pull printing)?		(Yes=0; No=1)		
28	Does the device provide functionality for controlling authentication and account management in accordance with organizational policy (e.g., password strength requirements, password changes, lockout procedures)?		(Yes=0; No=2)		
29	Does the device allow identification and authentication synchronization with domain credentials?		(Yes=0; No=1)		
30	Are logged-in users automatically logged off after a specified amount of time?		(Yes=0; No=2)		
	MONITORING				
31	Is usage of the device monitored?		(Yes=0; No=3)		
32	Does the device notify (e.g., send email) administrators of errors or potential incidents (e.g., multiple account lockouts)?		(Yes=0; No=2)		
33	Is audit/logging available and enabled on the device?		(Yes=0; No=3)		
34	Does the device automatically detect and mitigate DOS attacks?		(Yes=0; No=1)		
35	Does the device enforce time-out of queued jobs?		(Yes=0; No=2)		
36	Is the device temperature monitored and controlled with automatic shutoff in case of overheating?		(Yes=0; No=2)		
		Total Risk Score:			

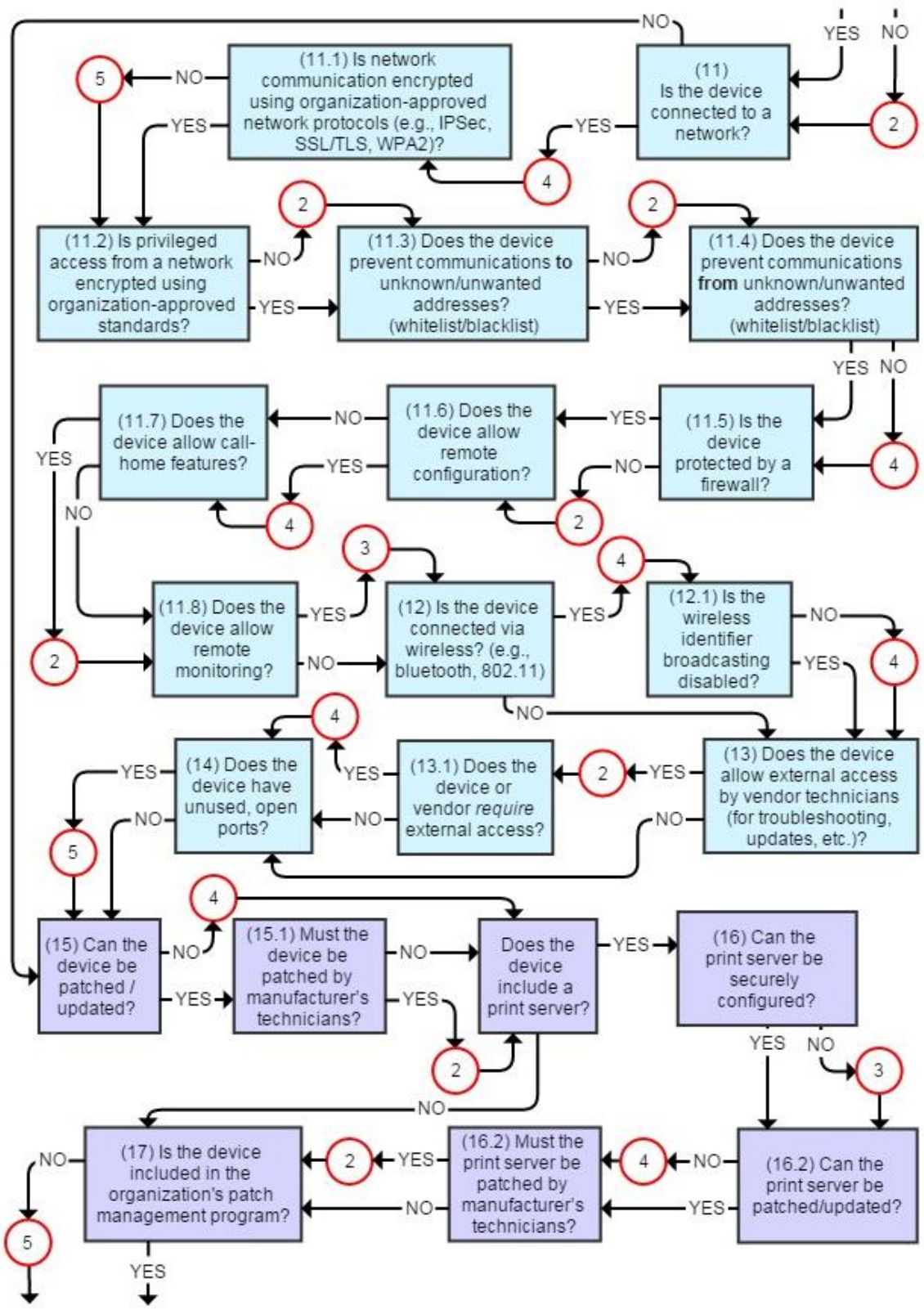
***Accepted risks remain as residual risks and are documented in the Security Assessment Report for the associated system.**

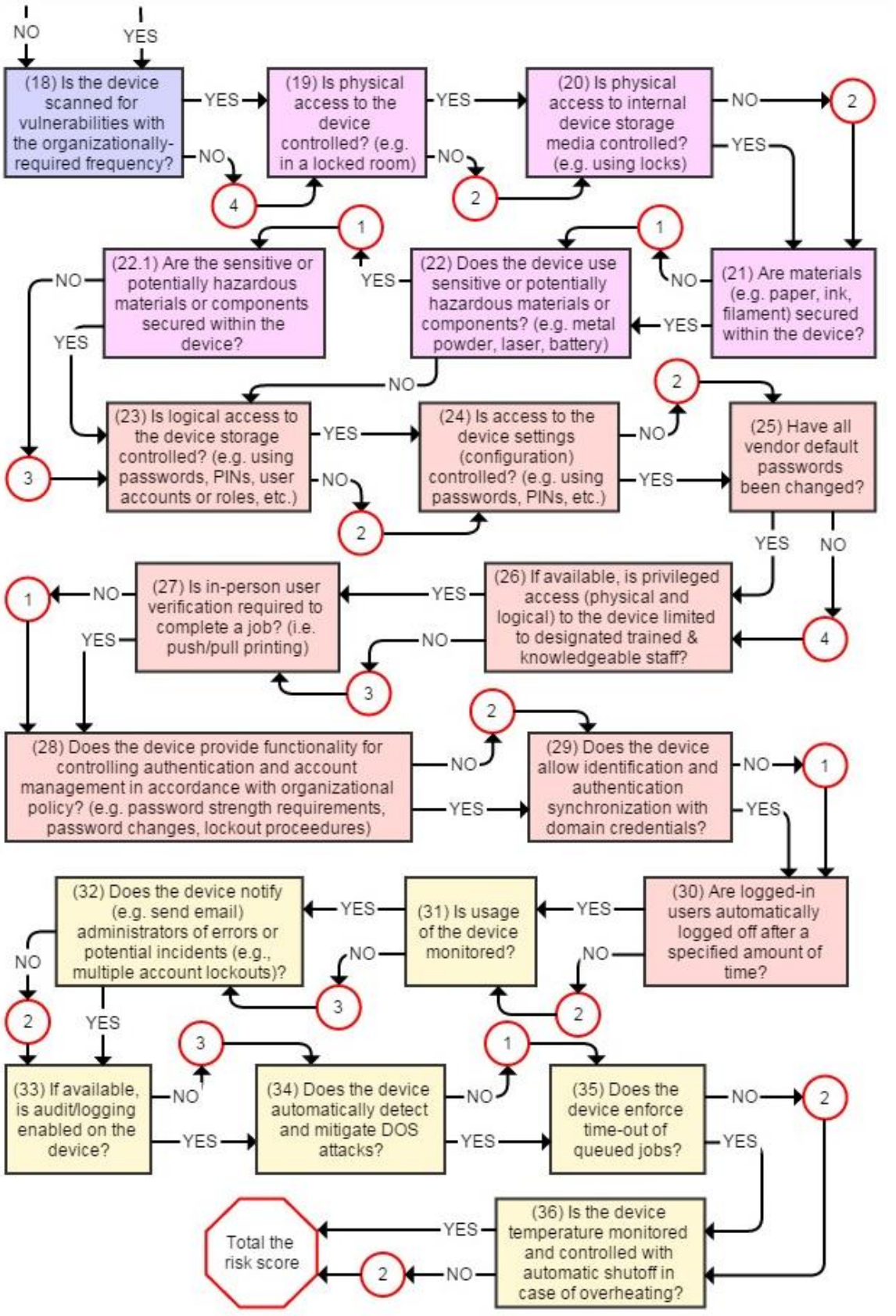
**** Actions to be taken are added to the Plan of Action and Milestones (POA&M) for the associated system.**

Security Risk Assessment Flow Chart for Replication Devices (RDs)

The security risk assessment flow chart that begins on the next page provides another view of the sample security risk assessment. Any answer with a risk score (in red circles) requires an action or justification as in the Security Assessment Table above. Different colors represent the various categories shown in the Security Risk Assessment Table (e.g., “Planning/Secure Configuration).


(1) Is the device included within a system security plan with applicable controls implemented?
NO
YES
4
(2) Does the device have any relevant security certifications (e.g., Common Criteria)?
NO
YES
1
(3) Does the vendor/manufacturer provide information on a secure configuration for the device?
NO
YES
1
(3.1) Has the secure configuration been implemented on the device?
YES
NO
2
(4) Is the device leased by the organization?
YES
NO
3
(4.1) Does the lease agreement stipulate federal ownership of storage devices internal to the device?
NO
YES
4
(5) Is the device under a service contract?
YES
NO
(5.1) Does the service contract stipulate that HDDs and solid state/nonvolatile storage must be removed before the device can leave organizational control?
NO
YES
5
(5.2) Does the service contract stipulate that service technicians are not permitted to remove information stored within the device in any form?
YES
NO
2
(5.3) Does the service contract stipulate that only Original Equipment Manufacturer (OEM) or OEM-approved replacement parts should be used?
YES
NO
3
(6) Are policies and procedures in place regarding media sanitization/ removal of storage media requirements before the device or storage media can leave organizational control?
NO
YES
5
(7) Does the device have a hard disk drive (HDD) or solid state/nonvolatile storage media?
YES
NO
4
(7.1) Is the device storage media easily physically accessible (i.e., no disassembly / tools needed)?
NO
YES
2
(7.2) Can stored information be logically accessed / viewed (either at the device console or via web access)?
NO
YES
2
(7.3) Is the device storage media encrypted using approved encryption standards?
NO
YES
4
(8) Are the device configuration settings encrypted using approved encryption standards?
NO
YES
2
(9) Does the device provide image overwrite capabilities?
NO
YES
4
(9.1) Is image overwrite capability enabled?
NO
YES
3
(9.2) Is immediate data overwrite capability enabled
NO
YES
(10) Does the device dump memory on reboot?
YES
NO
5


(11) Is the device connected to a network?
(11.1) Is network communication encrypted using organization-approved network protocols (e.g., IPSec, SSL/TLS, WPA2)?
(11.2) Is privileged access from a network encrypted using organization-approved standards?
(11.3) Does the device prevent communications to unknown/unwanted addresses? (whitelist/blacklist)
(11.4) Does the device prevent communications from unknown/unwanted addresses? (whitelist/blacklist)
(11.5) Is the device protected by a firewall?
(11.6) Does the device allow remote configuration?
(11.7) Does the device allow call-home features?
(11.8) Does the device allow remote monitoring?
(12) Is the device connected via wireless? (e.g., bluetooth, 802.11)
(12.1) Is the wireless identifier broadcasting disabled?
(13) Does the device allow external access by vendor technicians (for troubleshooting, updates, etc.)?
(13.1) Does the device or vendor *require* external access?
(14) Does the device have unused, open ports?
(15) Can the device be patched / updated?
(15.1) Must the device be patched by manufacturer's technicians?
Does the device include a print server?
(16) Can the print server be securely configured?
(16.2) Can the print server be patched/updated?
(16.2) Must the print server be patched by manufacturer's technicians?
(17) Is the device included in the organization's patch management program?
YES
NO


NO
YES
(18) Is the device scanned for vulnerabilities with the organizationally-required frequency?
YES
NO
(19) Is physical access to the device controlled? (e.g. in a locked room)
YES
NO
(20) Is physical access to internal device storage media controlled? (e.g. using locks)
NO
YES
2
4
2
1
1
(22.1) Are the sensitive or potentially hazardous materials or components secured within the device?
NO
YES
YES
(22) Does the device use sensitive or potentially hazardous materials or components? (e.g. metal powder, laser, battery)
NO
YES
(21) Are materials (e.g. paper, ink, filament) secured within the device?
NO
2
3
(23) Is logical access to the device storage controlled? (e.g. using passwords, PINs, user accounts or roles, etc.)
YES
NO
(24) Is access to the device settings (configuration) controlled? (e.g. using passwords, PINs, etc.)
NO
YES
2
(25) Have all vendor default passwords been changed?
YES
NO
2
1
(27) Is in-person user verification required to complete a job? (i.e. push/pull printing)
NO
YES
YES
NO
(26) If available, is privileged access (physical and logical) to the device limited to designated trained & knowledgeable staff?
4
3
2
(28) Does the device provide functionality for controlling authentication and account management in accordance with organizational policy? (e.g. password strength requirements, password changes, lockout proceedures)
NO
YES
(29) Does the device allow identification and authentication synchronization with domain credentials?
NO
YES
1
(32) Does the device notify (e.g. send email) administrators of errors or potential incidents (e.g., multiple account lockouts)?
YES
NO
(31) Is usage of the device monitored?
YES
NO
(30) Are logged-in users automatically logged off after a specified amount of time?
NO
3
2
2
YES
3
1
(33) If available, is audit/logging enabled on the device?
NO
YES
(34) Does the device automatically detect and mitigate DOS attacks?
NO
YES
(35) Does the device enforce time-out of queued jobs?
NO
YES
2
Total the risk score
YES
2
NO
(36) Is the device temperature monitored and controlled with automatic shutoff in case of overheating?

Total Risk Scores and Risk Levels

Add up the total risk score from either the Security Risk Assessment Table or Flow Chart. The maximum total risk score is 170.

- **115 and Above: High Risk -** Consider obtaining a replacement RD that meets minimum security requirements within the next fiscal year; implement compensating controls in the interim, e.g., install a firewall for networked RDs that can't be patched/updated and/or don't provide encryption functionality, renegotiate the service contract or lease agreement, escort service technicians at all times.
- **60-115: Moderate Risk –** Actions to be taken as stated in the "Action" column in the table along with compensating controls are sufficient until a new RD is needed for functional reasons. Risks identified as accepted in the table or for which compensating controls are not available or are impractical are monitored closely in the interim.
- **50 and Below: Low Risk –** Acceptable level of risk, excepting actions to be taken as stated in the "Action" column in the table. Risks identified as accepted in the table are monitored.

Appendix C: Roles and Responsibilities

Authorizing Official (AO) - An AO is a senior official or executive with the authority to formally assume responsibility for operating an information system (including copy/print/scan devices) at an acceptable level of risk to organization operations and assets, individuals, other organizations, and the Nation.

Common Control Providers – Common control providers are responsible for ensuring that organization-defined common controls are implemented, documented, and operating as intended in accordance with the organizational risk management strategy.

Contracting Officer - The contracting officer is the person who has the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

Information Owner/Steward and/or Program Manager - The program manager and/or information owner/steward represents the business and programmatic interests in the information system throughout the system development life cycle.

Information System Owner - The information system owner is responsible for ensuring that system security controls are selected, implemented, documented, and operating as intended in accordance with the organizational risk management strategy.

Information System Security Officer (ISSO) – The ISSO is responsible for ensuring that the appropriate operational security posture is maintained for an information system, and thus works closely with the information system owner. The ISSO has the detailed knowledge and expertise required to manage the security aspects of an information system and may be assigned responsibility for the day-to-day security operations of a system.

Security Control Assessors – Security control assessors are responsible for conducting assessments of the security controls employed within or inherited by an information system to determine the overall effectiveness of the controls.

Information System Administrators – Information system administrators are responsible for implementing agreed-upon controls and incorporating secure configuration settings for IT products. Information system administrators may also be responsible for managing information system accounts.