Thank-you for downloading the Security Risk Assessment Report Template!

More templates to download on the:

Templates Repository for Software Development Process (click here)

Or paste the link below in your browser address bar:
http://blog.cm-dm.com/pages/Software-Development-Process-templates

Who am I? See my linkedin profile:
http://fr.linkedin.com/pub/cyrille-michaud/0/75/8b5

You can remove this first page when you've read it and acknowledged it!

TABLE OF CONTENTS

1 Introduction

1.1 Document overview

This document covers the security risk assessment report of XXX device, designed in XXX software development project.
It contains:

- The risk analysis,
- The risk assessment report,
- The risk traceability matrix with software requirements.

1.2 References

1.2.1 Project References

#	Document Identifier	Document Title
[R1]	ID	Add your documents references. One line per document

1.2.2 Standard and regulatory References

#	Document Identifier	Document Title
[STD1]		Add your documents references. One line per document

Add the standard references to the table above. It may include ISO 14971, ISO 13485, IEC 62304, IEC 80001-1, ISO 2700x, AAMI TIR 57, UL 2900-1 amongst others.
Add FDA guidances: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – October 2014, Postmarket Management of Cybersecurity in Medical Devices – December 2016.

2 Risk Analysis

2.1 Intended use

Paste here intended use

2.2 Context of risk assessment

Describe here the context of the risk assessment, as required in the risk management plan
The context may contain the following items, as appropriate:

- The medical device (hardware, software, network…)
- Its accessories,
- Its environment
  - Operating room
  - Patient room
  - At home
- Other connected devices,
  - Medical devices,
  - Non-medical devices,
  - Cloud servers
- The processes involved in the lifecycle of the device:
  - Internal processes,
  - Outsourced processes and
  - Client/user processes,
- The users and user profiles
  - Client users,
  - Users of the manufacturer (e.g. customer support)
- The level of education of users,
- The use cases associated to the users and user profiles,
- The types of data handled in the device
  - Medical and personal data,
  - Data from sensors,
  - Configuration data,
  - Logs
- The hardware network interfaces
  - Bluetooth,
  - Wifi, Zigbee,
  - RJ45,
- The software network interfaces and protocols
  - HTTP, TCP, UDP,
  - SOAP, REST
  - Network Ports
- The data input/output streams
  - With connected devices,
  - Through removable media,
  - Internally between sub-systems of the device,
- The COST/SOUP used in software
- The constraints affecting the device
  - On the device,
  - On manufacturer processes,
  - On user processes, E.g. end-users generally don't accept to un-scrub and scrub for IT security reasons,
  - Regulatory requirements: GDPR, HIPAA…

- Constraints regarding emergency access to the device for patient safety, bypassing security measures.

This context establishment can be described in a mind maps, use cases, hardware architecture, system architecture, software architecture, as appropriate.

Some information may already be documented in the IEC 62336-1 usability engineering file. E.g. Users, user profiles, use cases.

2.3 Security risk matrix

The matrix below contains the risk analysis table, used for the study of the security risks associated with the device.

Add here a matrix with risk analysis.
Given the variety of risk analysis methods, the matrix may have different forms. The risk analysis method shall be described in the risk management plan. See the possible approaches in B.4 of AAMI TRI 57, threat-oriented, asset/impact-oriented, vulnerability-oriented.

The matrix below follows the pethood described in ISO 27005.

The Risk Priority Number (RPN) below comes from the example given in the risk management plan template:

- RPN = Probability of occurrence x Consequence, with
- Probability of occurrence ranges from 1 (very low) to 5 (very high)
- Consequence ranges from 1 (remote) to 5 (catastrophic)

ID	ASSET	THREAT	VULNERA-BILITY	EXISTING CONTROLS	CONSE-QUENCES	PROB	CONS	RPN	DECISION, RISK TREATMENT	R.A. M.A.*	RESI-DUAL PROB	RESI-DUAL CONS	RESI-DUAL RISK	SAFETY RISK? **
1	Medical device	An intruder can exploit the password weakness to break into the system	Password is vulnerable for dictionary or exhaustive key attacks	Password is required but no additional provision exist	The resources within the device are prone for illegal access/ modify/ damage by the intruder	5	4	20	Risk control: Implement password strength and expiration policy: -implement user password rules in OS -create instruction for password policy for end-users	N/A	1	4	4	NO

*R.A.M.A: Risk arising from mitigation action
**The risk itself or the risk treatment has an impact on safety risk assessment?

2.4 Risk traceability matrix

The risk traceability matrix below contains the connections between the risk analysis, software requirements and test plan.
A risk is deemed mitigated when the test status is set to PASSED in the test report.

Traceability is a central activity of software design. The best way to ensure that a risk is mitigated, is to add a requirement in the software requirement specification (SRS). The requirement will be tested by one or more tests according to the test plan. When all the tests are PASSED, we have the proof that the risk is mitigated.
Some risks may be mitigated by other elements than software requirements, for example warnings in the instruction for use. These requirement about non-software elements can nonetheless be added to the SRS. See my SRS template for some samples.

ID	RISK	SRS REQUIREMENT ID	SRS REQUIREMENT TITLE	TEST ID	TEST TITLE	COMMENT
1	Vulnerable password can be exploited by an intruder	SRS-REQ-001	Password strength	TEST-REQ-001	Verify password strength rules	Four requirements and four tests to mitigate the risk #1
1		SRS-DOC-001	Password instruction	TEST-DOC-001-1	Verify that password instruction exists	
1		SRS-REQ-002	Password expiration	TEST-REQ-002-1	Verify that password expires after xx days	
1		SRS-REQ-003	Password history	TEST-REQ-003-1	Verify that the last 3 passwords cannot be reused	

Most of times, there is a one-to-many relationship between risks, mitigation requirements, and tests verifying requirements. The example above shows that 4 requirements were defined to mitigate the risk and that 4 tests are necessary to prove that the risk is mitigated.

The risk traceability matrix below contains the connections between the risk analysis and software architectural or detailed design.

ID	RISK	SOFTWARE ELEMENT	SOFTWARE UNIT	COMMENT
1	Weak Password	OS: password	N/A	Mitigation of risk 1
2	Unsecured network communication	OS: network	N/A	Mitigation of risk 2

Most of times, there is a one-to-many relationship between risks and software elements or software units. Quote the relevant element/unit that bear or mitigates the risk, or quote all elements/units. This depends on your software architecture. SOUPs can be involved in the traceability, especially when the OS implements security features

2.5 Overall assessment of residual risks

Write here a qualitative assessment that the overall residual risk is acceptable. The justification may be grounded on results of penetration testing after implementation of risk treatment plans. The qualitative assessment may be also based on impact (or absence of impact) of security risks or their mitigation on safety risks or usability.

The qualitative assessment may also be based on the device risk/benefit ratio, or it may give hints for the assessment of the device risk/benefit ratio found in the clinical evaluation report.

2.6 Risk communication

Write here to whom the risk assessment report or parts of the risk assessment report is communicated, for what purpose and how frequently.
The safety risk management team and the usability engineering team shall not be forgotten!