Cybersecurity – Next Frontier of Risk Management

Naveen Agarwal, Ph.D.

Email: Naveen.Agarwal@ExeedQM.com
Website: https://www.ExeedQM.com

ASQ Orlando Section Meeting
January 23rd, 2020

“Broken Hearts”

(Episode 10, Season 2)

Showtime, Dec 2012

Dick Cheney Feared Assassination Via Medical Device Hacking: 'I Was Aware of the Danger'

By **DAN KLOEFFLER AND ALEXIS SHAW** Oct. 19, 2013

Share Tweet

WATCH | Former Vice President Cheney Reveals Fears of Pacemaker Hack

ABC News, Oct 2013

CYBERSECURITY TRIVIA

Kahoot.it Link

Cyberattacks are Real

CBS NEWS

2nd Florida city in just a week to pay hackers big ransom for seized computer systems

CBS News
June 26, 2019

Ransomware Attack Hits 22 Texas Towns, Authorities Say

The state declined to say which towns were affected by the coordinated cyberattack. But one expert said it could signal more such attacks in the future.

New York Times
Aug 20, 2019

LATEST HEALTH DATA BREACHES NEWS

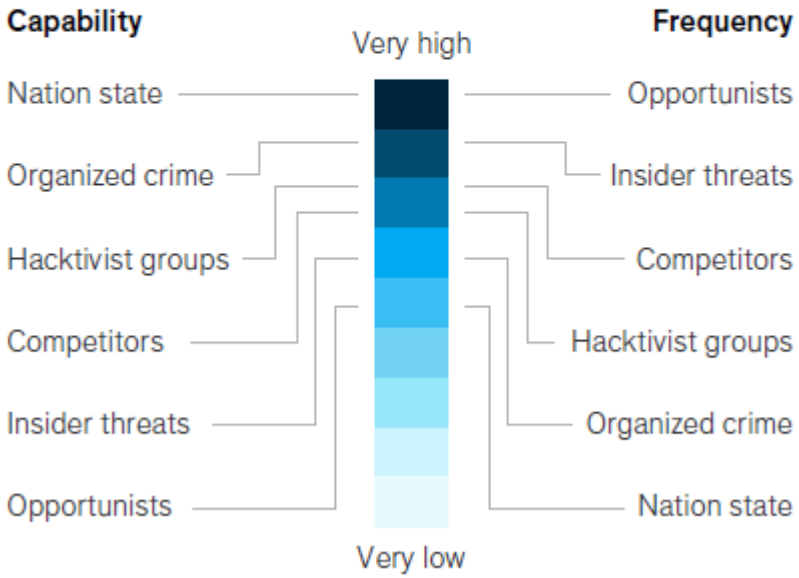
Hackers Demand $1M in Grays Harbor Ransomware Attack

The Washington-based provider initiated EHR downtime in June, but remained mum on details; a report shows hackers demanded a $1 million ransom to unlock patient files after a cyberattack.

Health IT Security
Aug 14, 2019

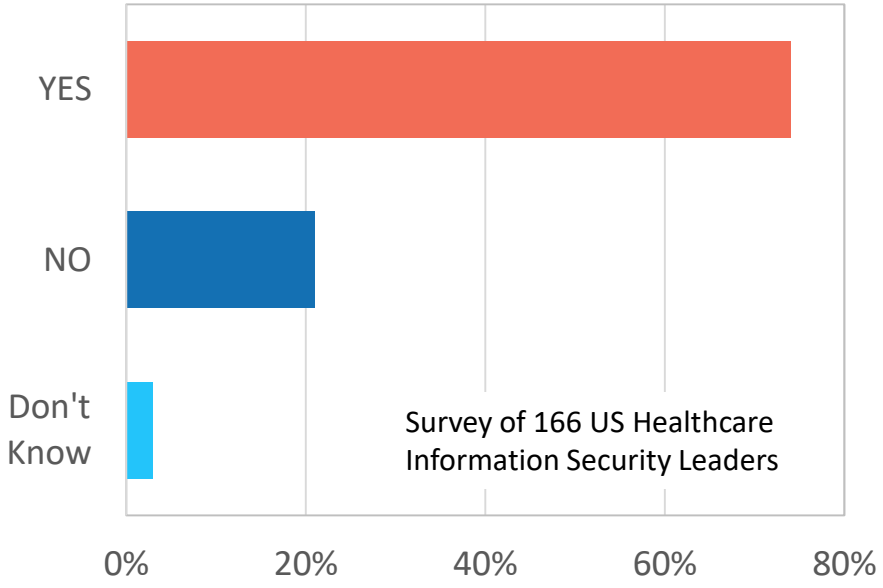
Cyberthreats are growing in severity and frequency.

Cyberthreat capacity and frequency today, threat actor



McKinsey & Company
[Risk Base Approach to Cybersecurity]

Significant Security Incidents in the Past 12 Months



Healthcare Information and Management Systems Society
[2019 HIMSS Cybersecurity Survey]

Recently Identified Vulnerabilities in Critical Medical Devices

11 vulnerabilities in IPnet, a TCP/IP stack used in a popular version of device operating systems

- 6 Critical – can allow remote code execution
- 5 can lead to denial of service

Patient monitors, Infusion pumps, MRI machines

Unauthorized software update during download from a software distribution network (SDN)

- Loss of personal health information
- Alter programmer functionality or associated implanted devices

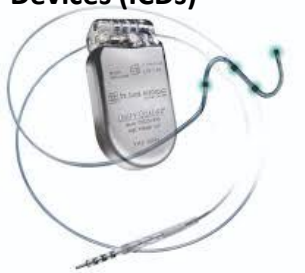
CareLink Programmers

Unauthorized access through wireless RF communication

- Alter device settings
- Denial of service

Insulin Pumps

Implantable Cardiac Devices (ICDs)



Note: There are no reports of actual exploits, malfunctions or injuries

Source: FDA Safety Communications

Not “If”, But “When”

Topics for Today

- **What is Cybersecurity?**
- **NIST Framework for Cybersecurity**
  - Framework Core, Tiers and Profile
  - Information and Decision Flow
  - 7-step Implementation Model
- **Focus on Medical Devices**
  - Industry Trends
  - Medical Device Safety is a Rising Concern
  - Applicable Standards
- **Recommendations**
  - Join an ISAO – Information Sharing and Analytics Organizations
  - Utilize ISO 14971 Framework for Risk Management
  - Build Capabilities and Tools

Merriam-Webster

cybersecurity noun

cy·ber·se·cu·ri·ty | \ ˈsī-bər-si-ˌkyu̇r-ə-tē \

Definition of *cybersecurity*

: measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

! First known use in 1989

The White House

Office of the Press Secretary

For Immediate Release February 12, 2013

Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER
EO 13636

Critical Infrastructure

"systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"

Framework for Improving Critical Infrastructure Cybersecurity

Framework Core

Set of activities to achieve specific cybersecurity *outcomes* with references for guidance

Framework Implementation Tiers

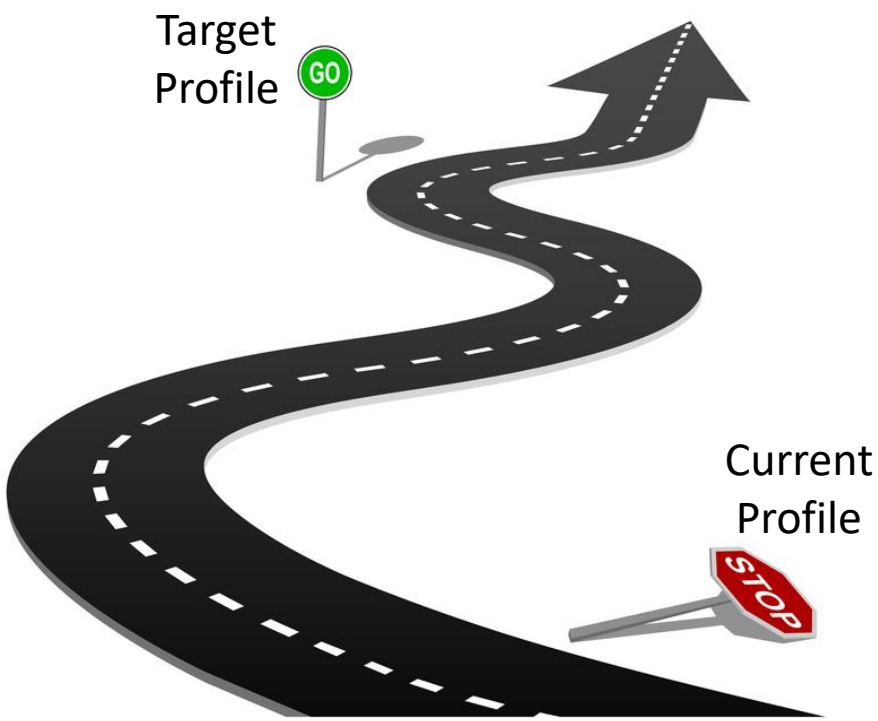
Context on how an organization views cybersecurity risk and processes to manage that risk

Framework Profile

Alignment of the framework core with business requirements, risk tolerance and resources of the organization

NIST Cybersecurity Framework, version 1.1, April 16, 2018

Framework Profile



- ❑ Profiles support business/mission requirements
- ❑ Identify and prioritize framework core category/sub-category outcomes
- ❑ Help communicate risk management priorities within and between organizations
- ❑ Help identify gaps in current and target profiles, prioritization of action plans

NIST Cybersecurity Framework, version 1.1, April 16, 2018

Framework Tiers

	1 Partial	2 Risk informed	3 Repeatable	4 Adaptive
Risk Management Process	Informal *ad hoc* Reactive	Management involved Business objectives Prioritization	Policy Regular updates Change responsive	Predictive models Lessons learned Continuous Improvement
Integrated Risk Management Program	Limited Awareness Case-by-Case Lacks Processes	Broad Awareness Informal Inconsistent	Defined Approach Formal, Consistent Skills & Knowledge Communication	Proactive Approach Risk Culture Resilience
External Participation	Undefined Role Lacks Information Unaware of Supply-Chain (SC) Risks	Limited Role Definition Some Information Aware of SC risks	Clear Role Definition Full Collaboration Responsive to SC Risks	Clear Role Understanding Community Contribution Proactive Communication

- ❑ Tiers do not represent maturity level
- ❑ Meant to support strategy, decision making and prioritization
- ❑ Consider cost-benefit for progression to higher tier
- ❑ Tier selection and approval sets the tone for cybersecurity risk management

NIST Cybersecurity Framework, version 1.1, April 16, 2018

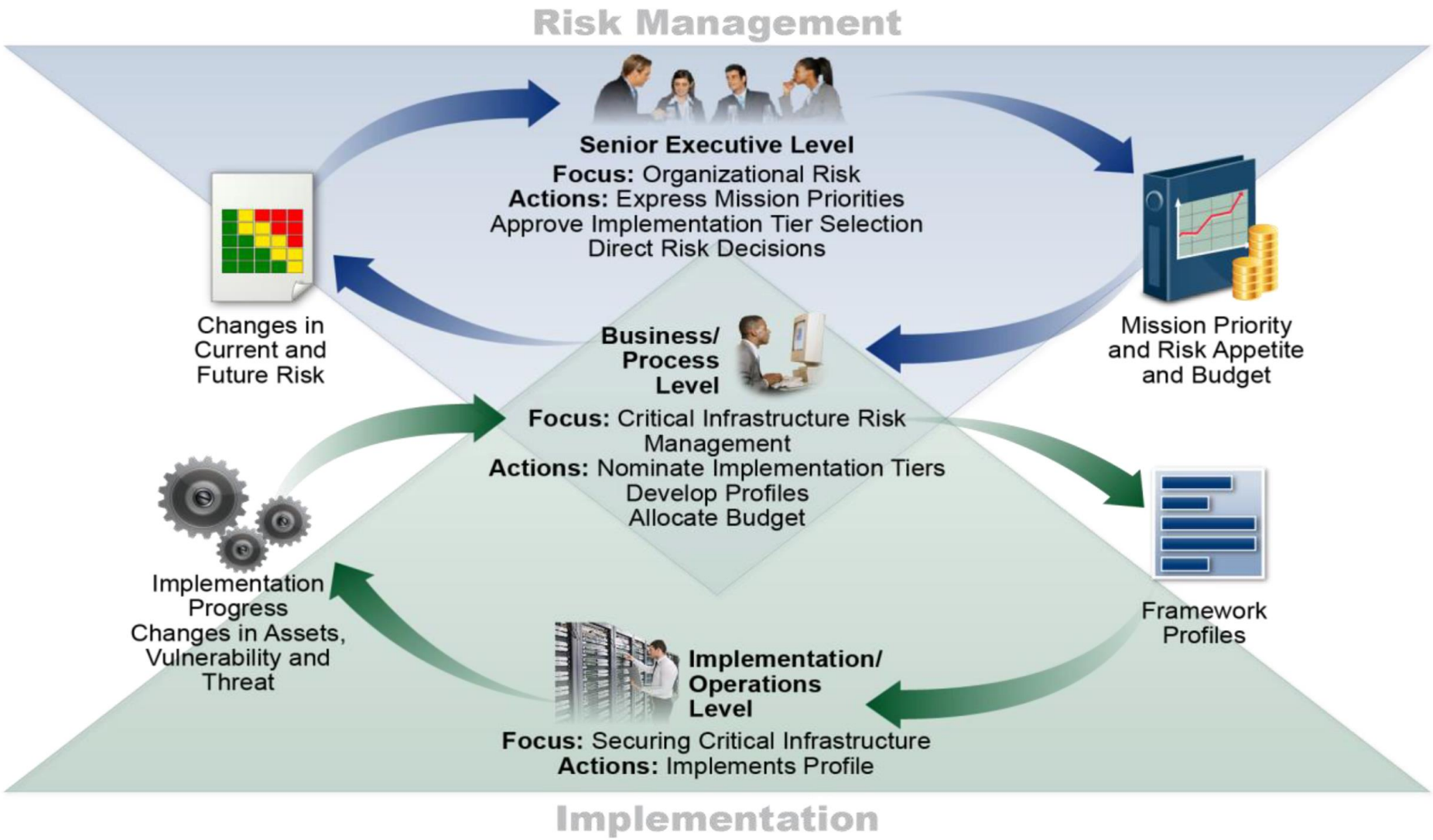
Framework Core

ID	IDENTIFY	**6 Categories** e.g. Business Environment, Governance, Risk Management Strategy	**29 Sub-Categories**
PR	PROTECT	**6 Categories** e.g. Identity Management, Access Control, Training, Data Security, Maintenance	**39 Sub-Categories**
DE	DETECT	**3 Categories** e.g. Anomalies and Events, Monitoring, Detection Processes	**18 Sub-Categories**
RS	RESPOND	**5 Categories** e.g. Response Planning, Analysis, Communications, Mitigation, Improvement	**16 Sub-Categories**
RC	RECOVER	**3 Categories** e.g. Recovery Planning, Improvements, Communications	**6 Sub-Categories**

>400 informative references

NIST Cybersecurity Framework, version 1.1, April 16, 2018

Information and Decision Flow Model



NIST Cybersecurity Framework, version 1.1, April 16, 2018

7-Step Implementation Model

1 Define Scope

- ✓ Vision, mission, priorities
- ✓ Cybersecurity program scope
- ✓ Business line or process
- ✓ Risk tolerance

2 Orient Systems

- ✓ Systems and assets
- ✓ Regulatory requirements
- ✓ Overall risk approach
- ✓ Threats and vulnerabilities

3 Create Current Profile

- ✓ Category outcomes
- ✓ Sub-category outcomes
- ✓ Level of achievement
- ✓ Applicable references

4 Assess Risks

- ✓ Risk management process
- ✓ Operational environment
- ✓ Likelihood and impact
- ✓ Risk evaluation

5 Establish Target Profile

- ✓ Stakeholder expectations
- ✓ Target implementation tier
- ✓ Desired cybersecurity outcomes
- ✓ Additional categories or sub-categories

6 Develop Plan

- ✓ Gap assessment
- ✓ Cost-benefit analysis
- ✓ Targeted improvement
- ✓ Timing and resources

7 Implement

- ✓ Prioritized specific actions
- ✓ Adjust current practices
- ✓ Competency development
- ✓ Standards and best practices

NIST Cybersecurity Framework, version 1.1, April 16, 2018

Applicable Standards and Controls – NIST Framework

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

Standard	Title	Link
CIS CSC	CIS Critical Security Controls for Effective Cyber Defense	https://www.cisecurity.org/controls/cis-controls-list/
COBIT 5	Control Objectives for Information Related Technology (COBIT)	https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
ISA 62443-2-1:2009	Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program	https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
ISA 62443-3-3:2013	Security for industrial automation and control systems Part 3-3: System security requirements and security levels	https://www.iso.org/standard/54534.html
ISO/IEC 27001:2013	Information Technology -- Security Techniques – Information Security Management Systems -- Requirements	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
NIST SP 800-53 Rev. 4	Security and Privacy Controls for Federal Information Systems and Organizations	https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731

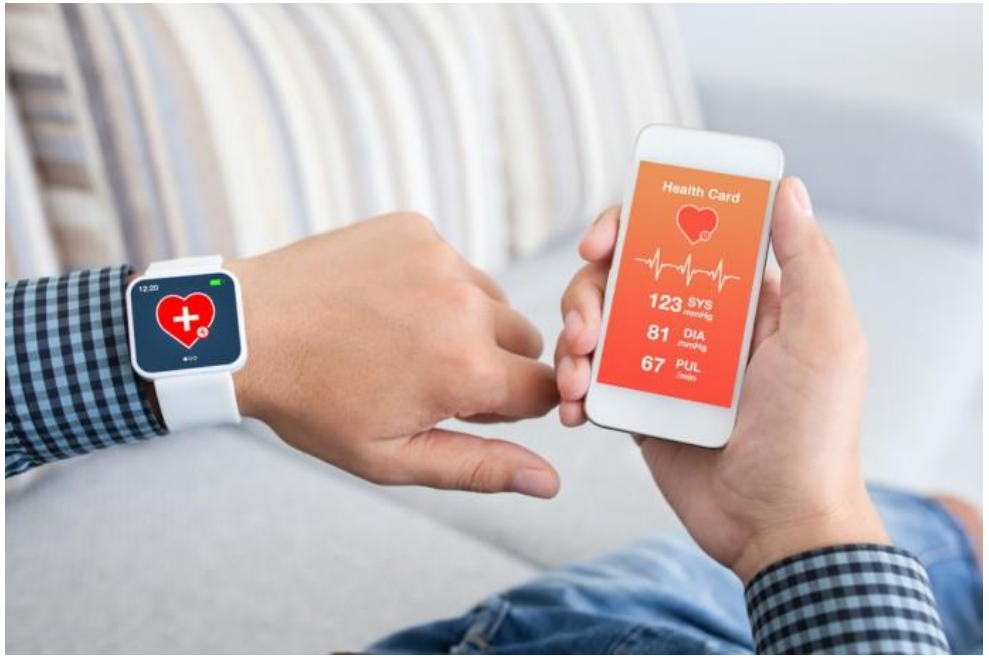
Focus on Medical Devices

Internet of Medical Things (IoMT)

Connected infrastructure of medical devices, software applications, health systems and services

Connected Medical Device Segment

From $14.9 B in 2017
To $52.2 B by 2022



67% Device makers who believe an attack on one or more of their devices is likely

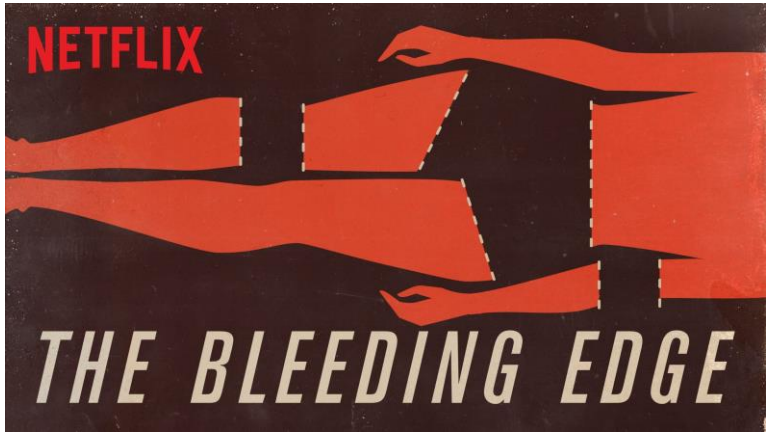
17% Device makers who are taking steps to prevent attacks

Medtech and Internet of Medical Things, Deloitte, July 2018

Effective Risk Management Now More Critical Than Ever

Increasing Public Awareness

More than **1.7 million injuries** and nearly **83,000 deaths** suspected of being linked to medical devices have been reported to the FDA (2008-2017).



Changing FDA Position

Safer Technology Program (STeP)

"We will consider how we could apply Breakthrough principles and features to products intended to treat or diagnose non-life-threatening diseases or conditions, but which ***offer substantial safety innovations*** *that either reduce the occurrence of a serious adverse event or other safety issue; address a known device failure mode or common user error; or provide for significant safety advantages for users."*

- FDA Commissioner Statement, Dec 2018

Source: https://www.exeedqm.com/new-blog/fda-wants-you-to-take-a-step-in-the-right-direction

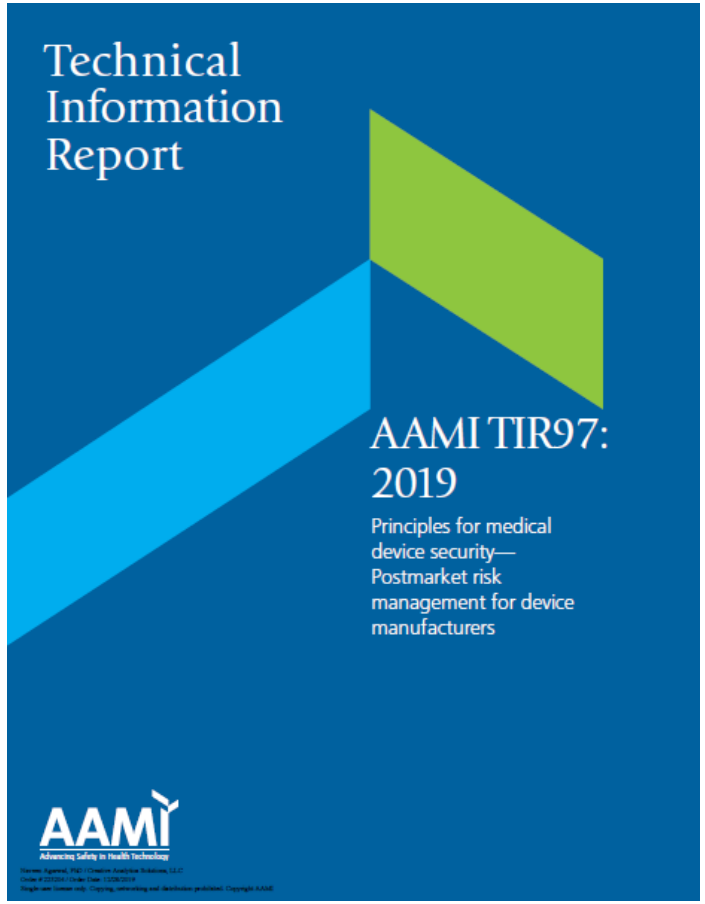
Applicable Standards for Medical Devices

Guidance for Industry

FDA

Standard	Title
ISO/IEC:27032:2012	Information Technology – Security Techniques – Guidelines for Cybersecurity
ANSI/AAMI/ISO 14971:2007	Medical Devices – Applications of Risk Management to Medical Devices (currently being revised in 2019)
ISO/IEC 30111:2013	Information Technology – Security Techniques – Vulnerability Handling Processes
ISO/IEC 29147:2014	Information Technology – Security Techniques – Vulnerability Disclosure
CLSI, AUTO11-A	IT Security of In-Vitro Diagnostic Instruments and Software System
IEC TR 80001-2-2 Edition 1.0 2012-7 AAMI/ANSI/IEC, TIR 80001-2-2:2012	Application of risk management for IT Networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
IEC, /TS 62443-1-1 Edition 1.0 2009-07	Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models
IEC, 62443-2-1 Edition 1.0 2010-11	Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program
IEC, /TR 62443-3-1 Edition 1.0 2009-07	Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems

Other Useful Resources for Medical Devices



Why Join an ISAO?

Information Sharing and Analysis Organization

ISAO

ABOUT | EVENTS | RESOURCES | INFO SHARING GROUPS | SUPPORT | FAQ | CONTACT

AREA OF INTEREST

- Show All Areas (71)
- Commercial Facilities (4)
- Communications (1)
- Healthcare and Public Health (4)
- More Areas of Interest

LOCATION

- Show All Locations (71)
- Alabama (1)
- Arizona (2)
- More Locations

TYPE OF ORGANIZATION

- Geographic (15)
- Industry/Sector (42)
- Special Interest (7)
- Other (8)

Note: This page uses cookies to save your search settings for future use.

SEARCH

Search...

Healthcare Ready

Heathcare Ready (formerly Rx Response) helps to strengthen healthcare supply chains and enhance community resiliency by fostering collaboration between public health and the private sector and by addressin...

HEALTHCARE READY — STRENGTHEN. SAFEGUARD. RESPOND.

HITRUST

HITRUST Alliance is a not-for-profit organization whose mission is to champion programs that safeguard sensitive information and manage information risk for organizations across all industries and througho...

HITRUST

Medical Device ISAO

The Medical Device ISAO is dedicated to improving the security of medical devices through education, awareness and advocacy. MedISAO provides cybersecurity information, education and tools tailor-made for ...

MedISAO

National Health ISAC

NH-ISAC is a private sector, non-profit organization that provides a trusted community for the sharing of timely, relevant and actionable physical and cyber information among stakeholders to ensure the res...

NH-ISAC — NATIONAL HEALTH - ISAC

"It is strongly recommended that manufacturers participate in an ISAO"

- FDA Guidance, Postmarket Management of Cybersecurity in Medical Devices

- ✓ Information sharing about vulnerabilities and threats impacting medical devices
- ✓ Awareness of best practices in cybersecurity risk management
- ✓ Availability of shared service resources
- ✓ Reduced reporting burden under 21 Part 806 for certain uncontrolled risks if active participant in an ISAO

https://www.isao.org/information-sharing-groups/

Key Concept– Risk is a Combination of Severity and Probability

ISO 14971: Each stakeholder *perception* of risk can vary greatly

ICH Q9: achieving a shared understanding of the application of risk management among diverse *stakeholders* is difficult

- ❑ How do we establish a common scale for risk assessment?
- ❑ How do we treat safety risks vs. product quality risks?
- ❑ How do we develop appropriate risk-acceptability criteria?
- ❑ How do we establish a suitable data and analytics infrastructure?
- ❑ How do we evolve our risk analysis and evaluation methods?

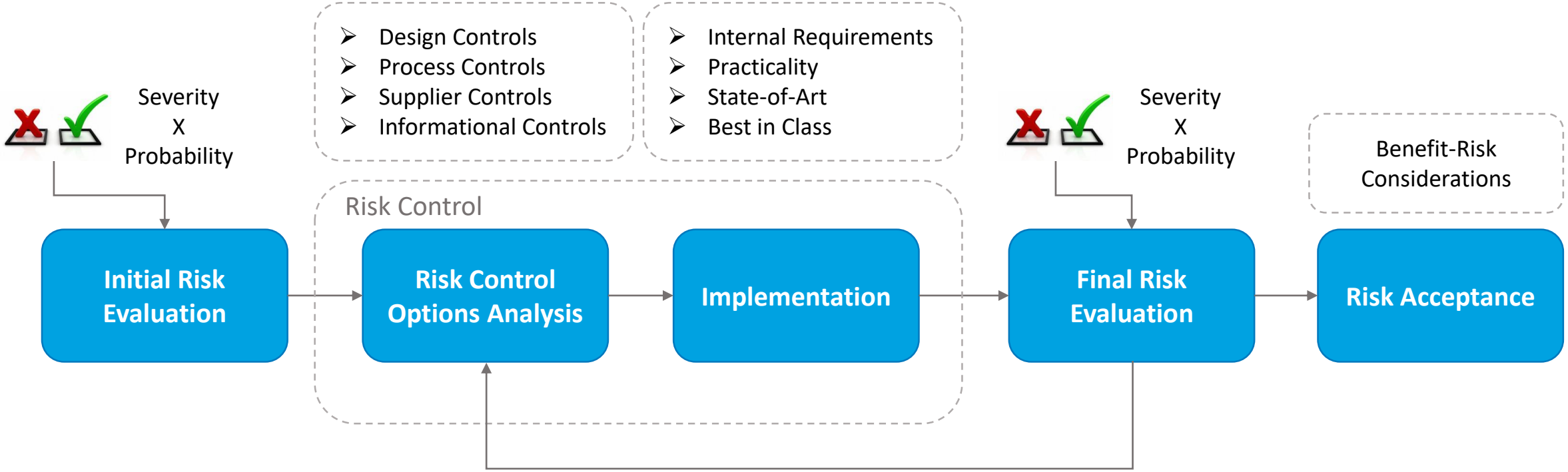
S1 E1 V4 E1 R1 I1 T1 Y4

P3 R1 O1 B3 A1 B3 I1 L1 I1 T1 Y4

Risk Control is a Process of Making Decisions

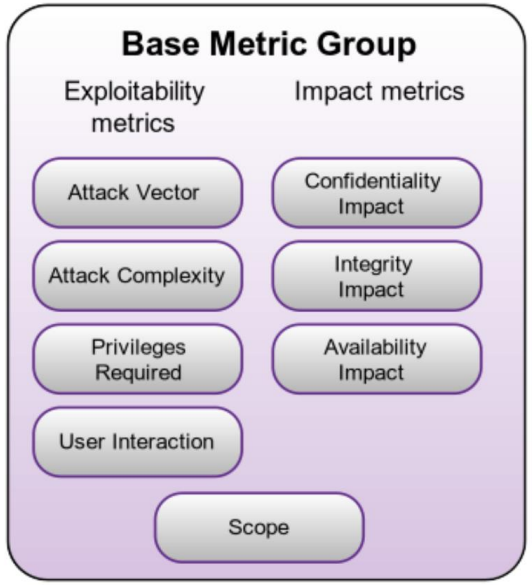
ISO 14971: Risk control is a process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels

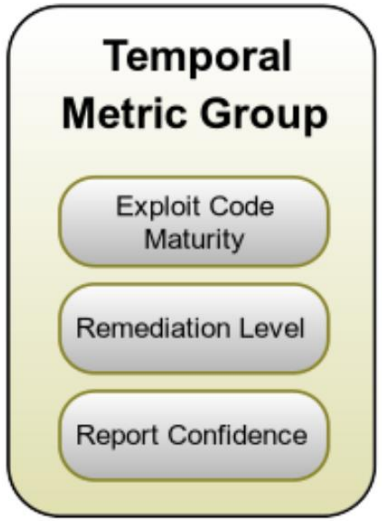
ICH Q9: Risk control includes decision making to reduce and/or accept risks.

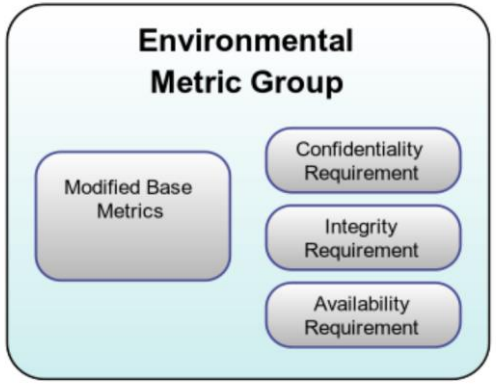


Note: Control of failure modes is <u>not</u> the same as control of risks

Common Vulnerability Scoring System







Base characteristics
Constant over time and user environments
- **Exploitability:** how easy to exploit
- **Impact:** consequences of a successful exploit

Time-dependent characteristics
May change over time and but not across user environments

User environment dependent characteristics
Relevant and unique to user environments

- CVSS measures severity, not risk
- Base score ranges from 0 – 10
- Temporal and environmental group scoring can “fine tune” the base score
- Key players – vulnerability bulletin analysts, security product vendors, application vendors

https://www.first.org/cvss/

CVSS Scoring Example – Certain Older Models of Insulin Pumps

Vulnerability Overview

Wireless communication with other devices such as glucose meters and sensor transmitters does not properly implement authentication or authorization

Common Vulnerability Scoring System Version 3.1 Calculator

Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.1 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, and notes on using this calculator (including its design and an XML representation for CVSS v3.1).

Base Score 7.1 (High)

Attack Vector (AV): Network (N), **Adjacent (A)**, Local (L), Physical (P)	**Scope (S)**: **Unchanged (U)**, Changed (C)
Attack Complexity (AC): Low (L), **High (H)**	**Confidentiality (C)**: None (N), **Low (L)**, High (H)
Privileges Required (PR): **None (N)**, Low (L), High (H)	**Integrity (I)**: None (N), Low (L), **High (H)**
User Interaction (UI): **None (N)**, Required (R)	**Availability (A)**: None (N), Low (L), **High (H)**

Vector string: AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H

FDA Safety Communication and DHS ICS Medical Advisory (ICSMA-19-187-01), June 2019

In Closing….

- Cyberattacks on the rise – the question is not “if”, but “when”
- Cybersecurity considerations now a critical aspect of risk management
- Internet of Medical Things (IoMT) expected to drive medical device innovation
- Regulatory scrutiny and expectations on the rise
- Existing risk management framework can be used for cybersecurity (e.g. ISO 14971 for medical devices)

About Exeed™

Portfolio of Innovative Quality Solutions in 4 Broad Areas

Customer Experience

Regulatory Compliance

Risk Management

Quality Culture

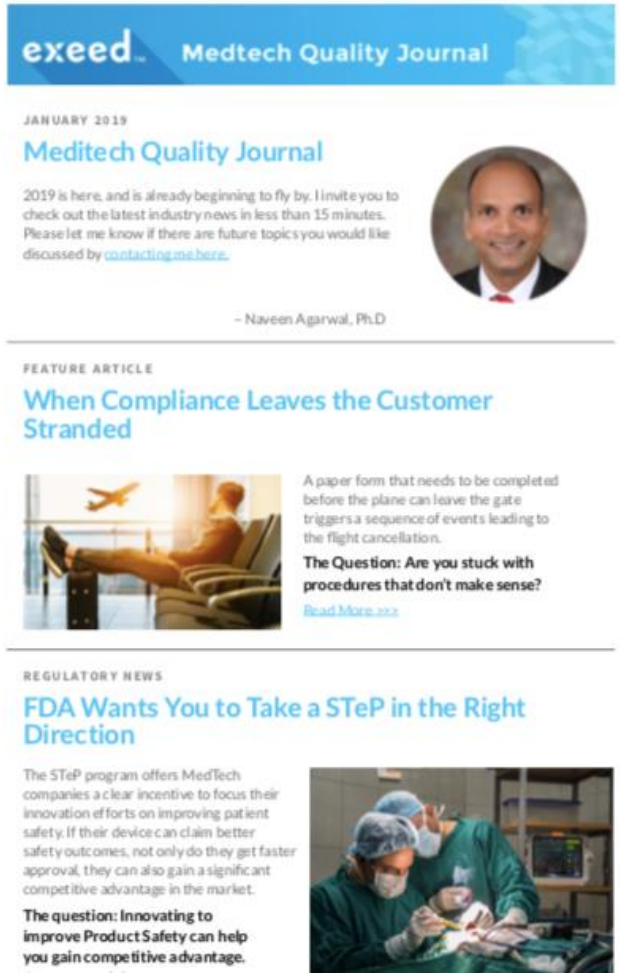
Email: Info@ExeedQM.com
Web: www.ExeedQM.com
Phone: 1-833-MY-EXEED

Sign Up for Our Newsletter: https://www.exeedqm.com/blog-sign-up

Free Monthly Industry News

In less than 15 minutes

Sign up now



exeed Medtech Quality Journal

JANUARY 2019

Meditech Quality Journal

2019 is here, and is already beginning to fly by. I invite you to check out the latest industry news in less than 15 minutes. Please let me know if there are future topics you would like discussed by contacting me here.

– Naveen Agarwal, Ph.D

FEATURE ARTICLE

When Compliance Leaves the Customer Stranded

A paper form that needs to be completed before the plane can leave the gate triggers a sequence of events leading to the flight cancellation.

The Question: Are you stuck with procedures that don't make sense?

Read More >>>

REGULATORY NEWS

FDA Wants You to Take a STeP in the Right Direction

The STeP program offers MedTech companies a clear incentive to focus their innovation efforts on improving patient safety. If their device can claim better safety outcomes, not only do they get faster approval, they can also gain a significant competitive advantage in the market.

The question: Innovating to improve Product Safety can help you gain competitive advantage.