NOVA LEAH

Informing design controls – the true value of MDS²

email: anita.finnegan@novaleah.com
twitter: @anita_finnegan

Anita Finnegan, Ph.D.

CEO / FOUNDER

NOVA LEAH

email: anita.finnegan@novaleah.com
twitter: @anita_finnegan

Bio

Nova Leah was founded in 2015 by Anita Finnegan, award-winning international expert in cybersecurity risk management solutions and government advisor.

Projects:

- IPL: IEC 80001-2-8
- IPL: IEC 80001-2-9
- IPL: Security Assurance Cases, ISO/IEC 81001
- ENISA Expert

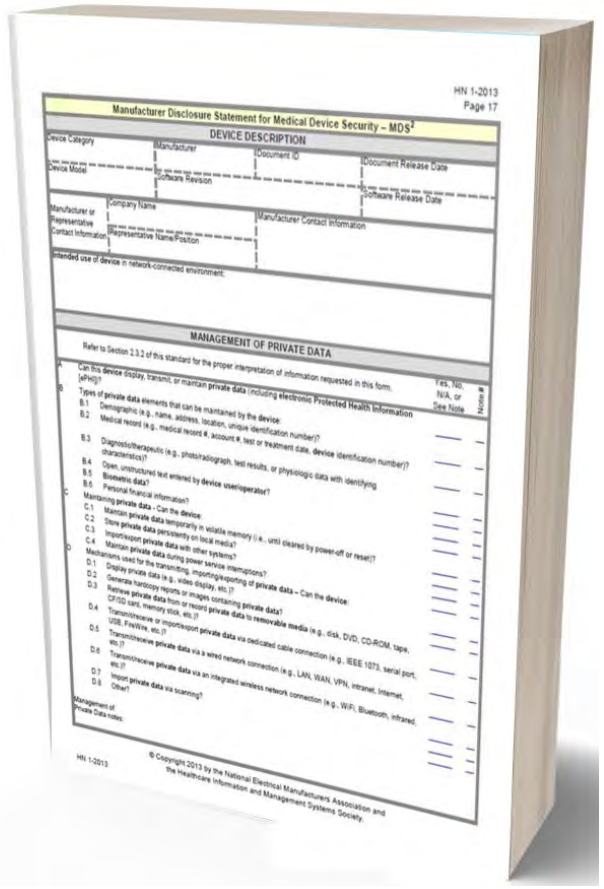
Memberships:

- ISO/TC 215 JWG 7
- JWG 3
- STP UL 2900
- MDS2 Canvass Group
- NTIA Software Transparency Taskforce

NOVA LEAH

MDS2 - Introduction

Manufacturer Disclosure Statement


HN 1-2013
Page 17

Manufacturer Disclosure Statement for Medical Device Security – MDS²

DEVICE DESCRIPTION

Device Category | Manufacturer | Document ID | Document Release Date

Device Model | Software Revision | Software Release Date

Manufacturer or Representative Contact Information | Company Name | Representative Name/Position | Manufacturer Contact Information

Intended use of device in network-connected environment:

MANAGEMENT OF PRIVATE DATA

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.

		Yes, No, N/A, or See Note	Note #
A	Can this device display, transmit, or maintain private data (including electronic Protected Health Information [ePHI])?		
B	Types of private data elements that can be maintained by the device:		
B.1	Demographic (e.g., name, address, location, unique identification number)?		
B.2	Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?		
B.3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?		
B.4	Open, unstructured text entered by device user/operator?		
B.5	Biometric data?		
B.6	Personal financial information?		
C	Maintaining private data - Can the device:		
C.1	Maintain private data temporarily in volatile memory (i.e., until cleared by power-off or reset)?		
C.2	Store private data persistently on local media?		
C.3	Import/export private data with other systems?		
C.4	Maintain private data during power service interruptions?		
D	Mechanisms used for the transmitting, importing/exporting of private data – Can the device:		
D.1	Display private data (e.g., video display, etc.)?		
D.2	Generate hardcopy reports or images containing private data?		
D.3	Retrieve private data from or record private data to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?		
D.4	Transmit/receive or import/export private data via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?		
D.5	Transmit/receive private data via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?		
D.6	Transmit/receive private data via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?		
D.7	Import private data via scanning?		
D.8	Other?		

Management of Private Data notes:

HN 1-2013

- Standard which includes a form to provide healthcare delivery organizations with crucial security related information;
- Intended to be used as part of the security procurement process;
- Clarifies roles and responsibilities of manufacturers and healthcare delivery organisations for the upkeep and maintenance of a connected device security posture.

NOVA LEAH

MDS2

Development and history of MDS2

+ Streamlined
+ Transparency

2008

NEMA/HIMSS

- 3-page form 50/50 free form
- Description of OS, PHI use, antivirus etc

2013

NEMA/HIMSS

- Aligned with IEC 80001
- 20 security capabilities more relevant to connected technology advancements and increasingly complex threat landscape

2019

NEMA/MITA

- Additional security capabilities
- More comprehensive suite of questions
- Again...more relevant capabilities addressing industry needs

NOVA LEAH

IEC TR 80001-2-2

Guidance for the disclosure and communication of medical device security needs, risks and controls

2012

email: anita.finnegan@novaleah.com
twitter: @anita_finnegan

NOVA LEAH

IEC 80001-2-2

Guidance for the disclosure & communication of medical device security needs, risk & controls

Security Disclosure Framework

A framework for the disclosure of security-related capabilities and risks necessary for managing the risk in connecting medical devices to IT-networks.

Common Security Goals

This technical report presents an informative set of common, high-level security-related capabilities useful in understanding the user needs, the type of security controls to be considered and the risks that lead to the controls.

Information Sharing

The capability descriptions in the report are intended to supply healthcare delivery organizations (HDOs) and medical device manufacturers (MDMs) with a basis for discussing risk & their respective roles & responsibilities toward its management.

HIMSS / NEMA MDS2

Alignment with MDS2 – Manufacture Disclosure Statement for Medical Device Security

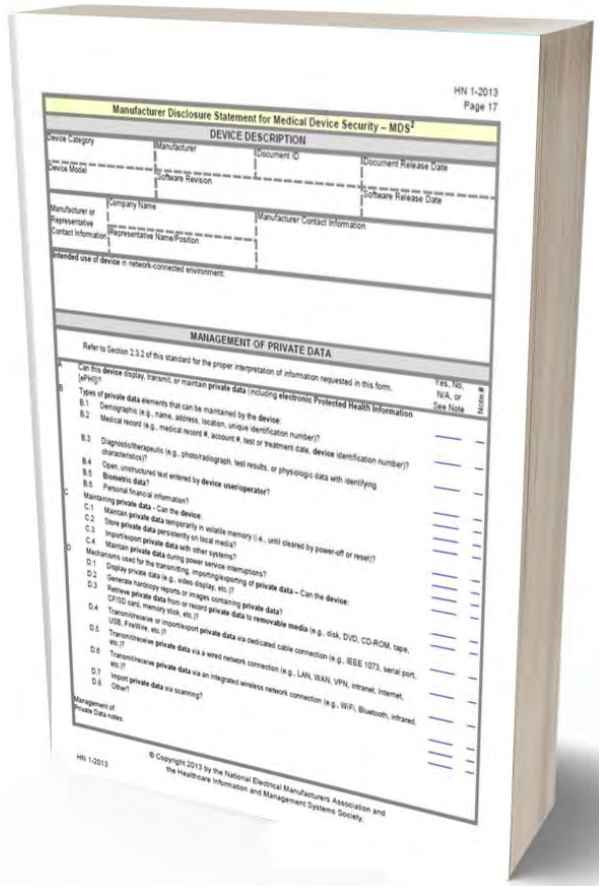
IEC/TR 80001-2-2 Security Capabilities

Automatic Log of	Audit Controls	Authorization	Configuration of Security Features
Cyber security product Upgrades	Data backup and disaster recovery	Emergency access	Heath data de-identification
Health data integrity and authenticity	Health data storage confidentiality	Malware protection/detection	Node authentication
Person authentication	Physical locks on devices	Security guides	System and application hardening
Third party components in product lifecycle roadmaps	Transmission confidentiality	Transmission integrity	

NOVA LEAH

MDS² 2019

Manufacturer Disclosure Statement - Revision



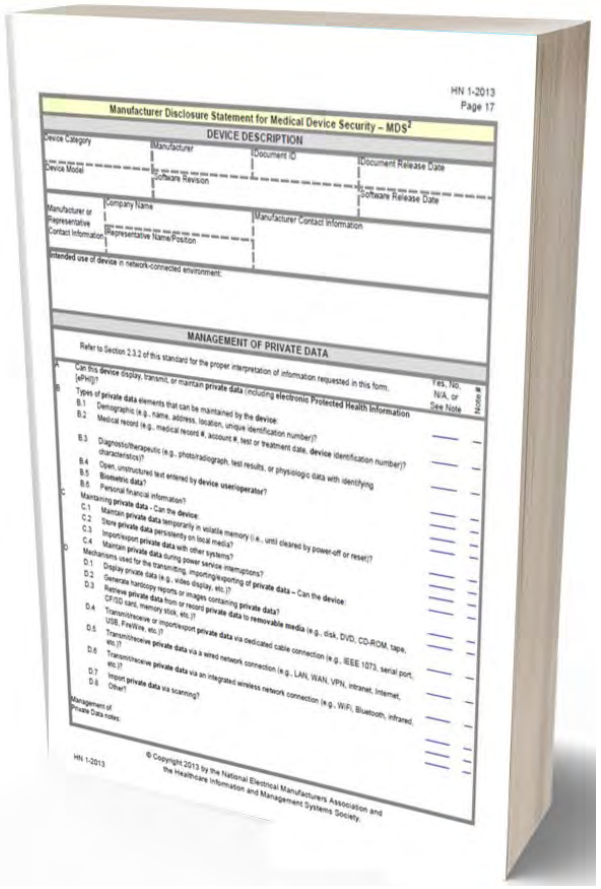
MDS² Security Capabilities

Automatic Log of	**Audit Controls**	**Authorization**	**Management of personally identifiable information**
Cyber security product Upgrades	Data backup and disaster recovery	Emergency access	Heath data de-identification
Health data integrity and authenticity	Health data storage confidentiality	Malware protection/detection	Node authentication
Person authentication	Physical locks on devices	Security guides	System and application hardening
Roadmap for third party components in device life cycle	Transmission confidentiality	Transmission integrity	**Remote Service**
Connectivity capabilities	**Software bill of materials**		

NOVA LEAH

MDS² 2019

MDS² shortcomings


HN 1-2013
Page 17

Manufacturer Disclosure Statement for Medical Device Security – MDS²

DEVICE DESCRIPTION

Device Category | Manufacturer | Document ID | Document Release Date

Device Model | Software Revision | Software Release Date

Manufacturer or Representative Contact Information: Company Name | Manufacturer Contact Information | Representative Name/Position

Intended use of device in network-connected environment:

MANAGEMENT OF PRIVATE DATA

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.

		Yes, No, N/A, or See Note	Note #
A	Can this device display, transmit, or maintain private data (including electronic Protected Health Information [ePHI])?		
B	Types of private data elements that can be maintained by the device:		
B.1	Demographic (e.g., name, address, location, unique identification number)?		
B.2	Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?		
B.3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?		
B.4	Open, unstructured text entered by device user/operator?		
B.5	Biometric data?		
B.6	Personal financial information?		
C	Maintaining private data - Can the device:		
C.1	Maintain private data temporarily in volatile memory (i.e., until cleared by power-off or reset)?		
C.2	Store private data persistently on local media?		
C.3	Import/export private data with other systems?		
C.4	Maintain private data during power service interruptions?		
D	Mechanisms used for the transmitting, importing/exporting of private data – Can the device:		
D.1	Display private data (e.g., video display, etc.)?		
D.2	Generate hardcopy reports or images containing private data?		
D.3	Retrieve private data from or record private data to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?		
D.4	Transmit/receive or import/export private data via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?		
D.5	Transmit/receive private data via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?		
D.6	Transmit/receive private data via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?		
D.7	Import private data via scanning?		
D.8	Other?		

Management of Private Data notes:

HN 1-2013

- **Checkbox exercise**
- **Add little value to the development life cycle**
- **Limited / restricted use / failure to update**

NOVA LEAH

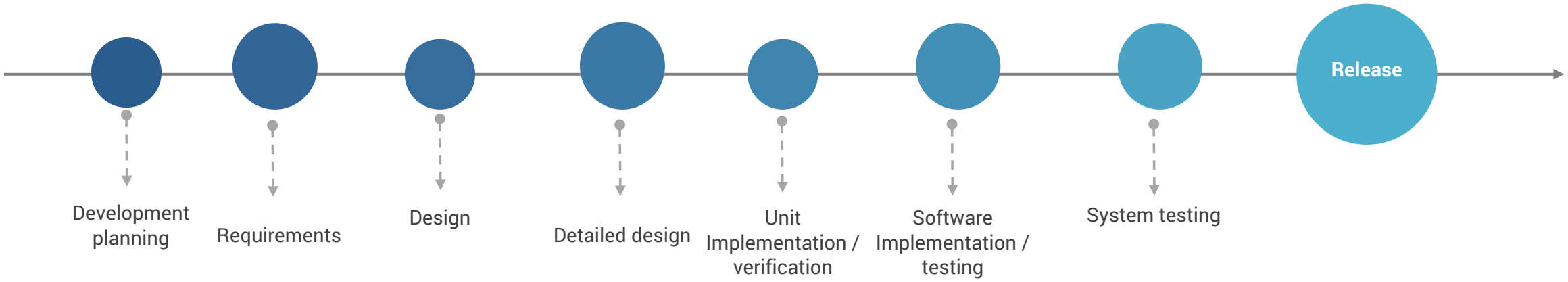

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
Guidance for Industry and Food and Drug Administration Staff
Document Issued on: October 2, 2014
The draft of this document was issued on June 4, 2013
For questions regarding tis document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.
CDRH
CBER
FDA
Postmarket Management of ybersecurity in Medical Devices
lance for Industry and Food and Drug Administration Staff
Document Issued on: December 28, 2016
raft of this document was issued on January 22, 2016
rding this document, contact Suzanne Schwartz, Center for Devices and h, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, ring, MD 20993-0002, 301-796-6937. For questions regarding this d to devices regulated by CBER, contact the Office of Communication, opment in CBER at 1-800-835-4709 or 240-402-8010 or
FDA

NOVA LEAH

MDS²

Informing design controls

IEC 62304 life cycle



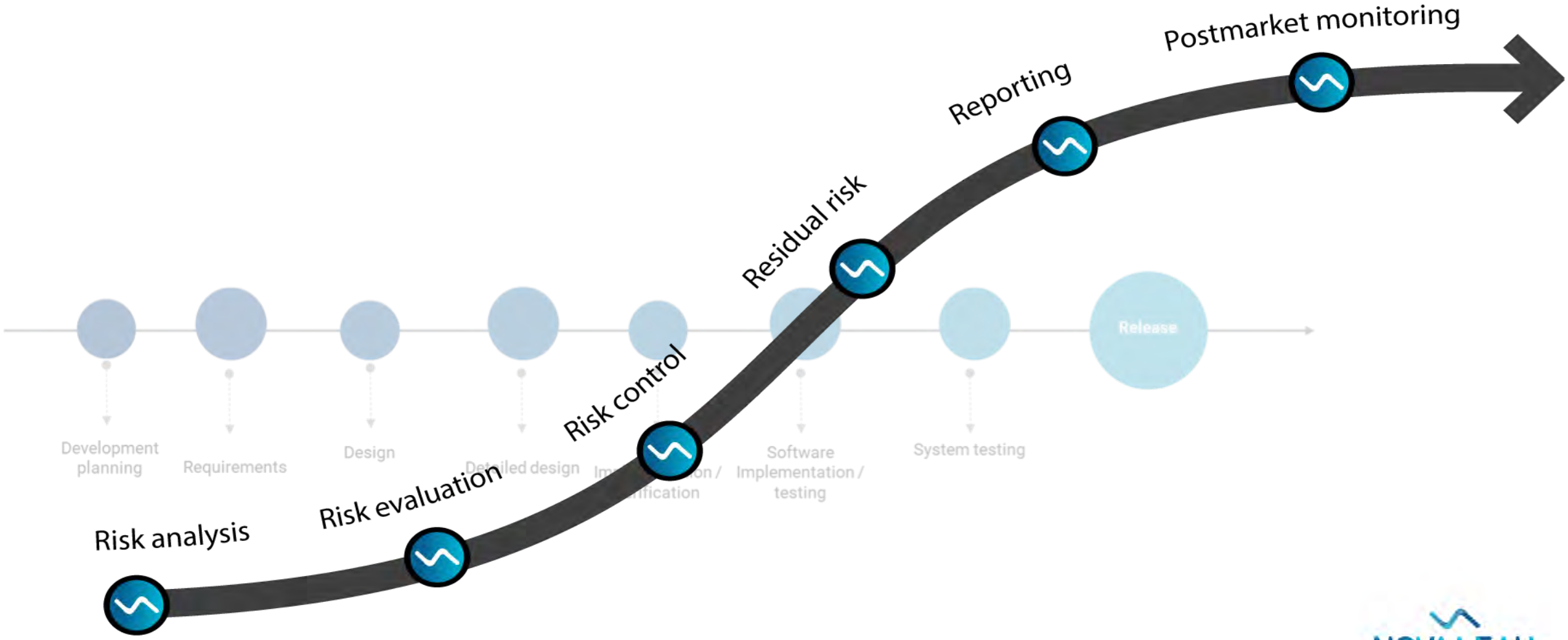
email: anita.finnegan@novaleah.com
twitter: @anita_finnegan

NOVA LEAH

MDS²

Informing design controls

Risk assessment overlay



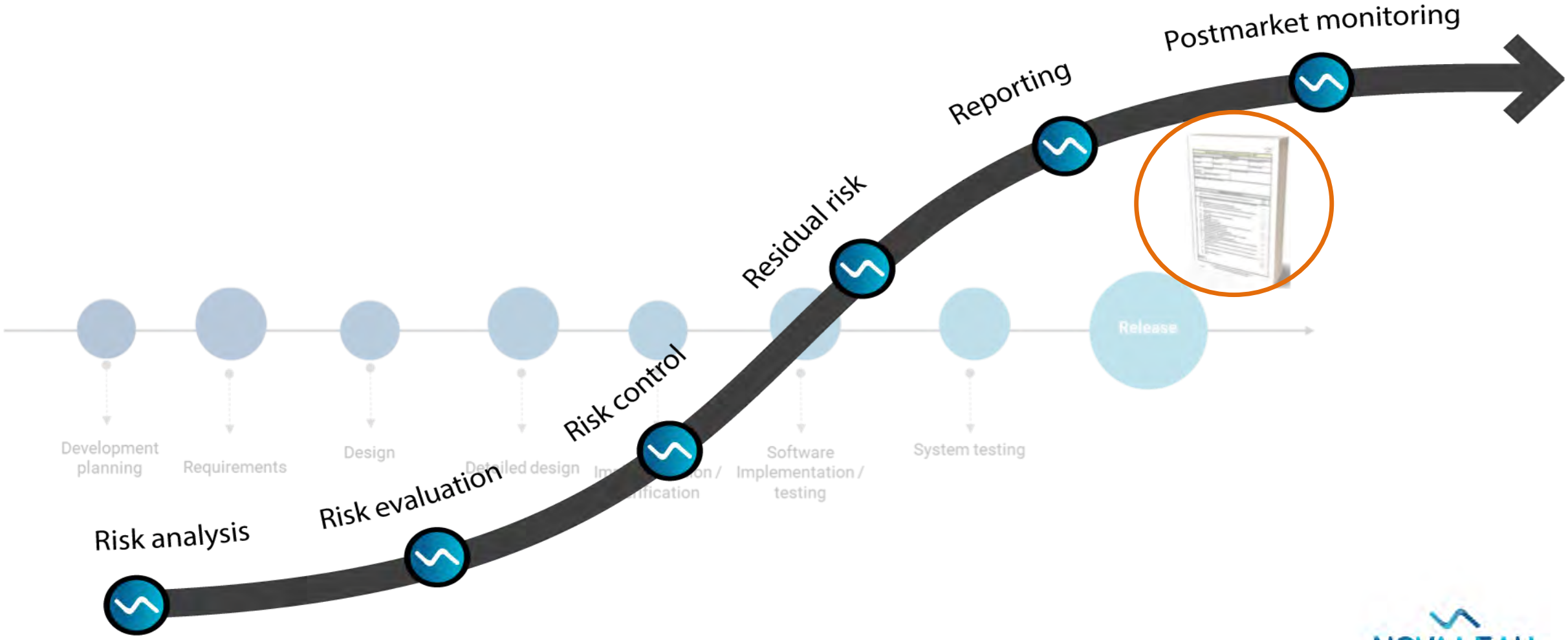
email: anita.finnegan@novaleah.com
twitter: @anita_finnegan

NOVA LEAH

MDS²

Informing design controls

Creation of MDS²



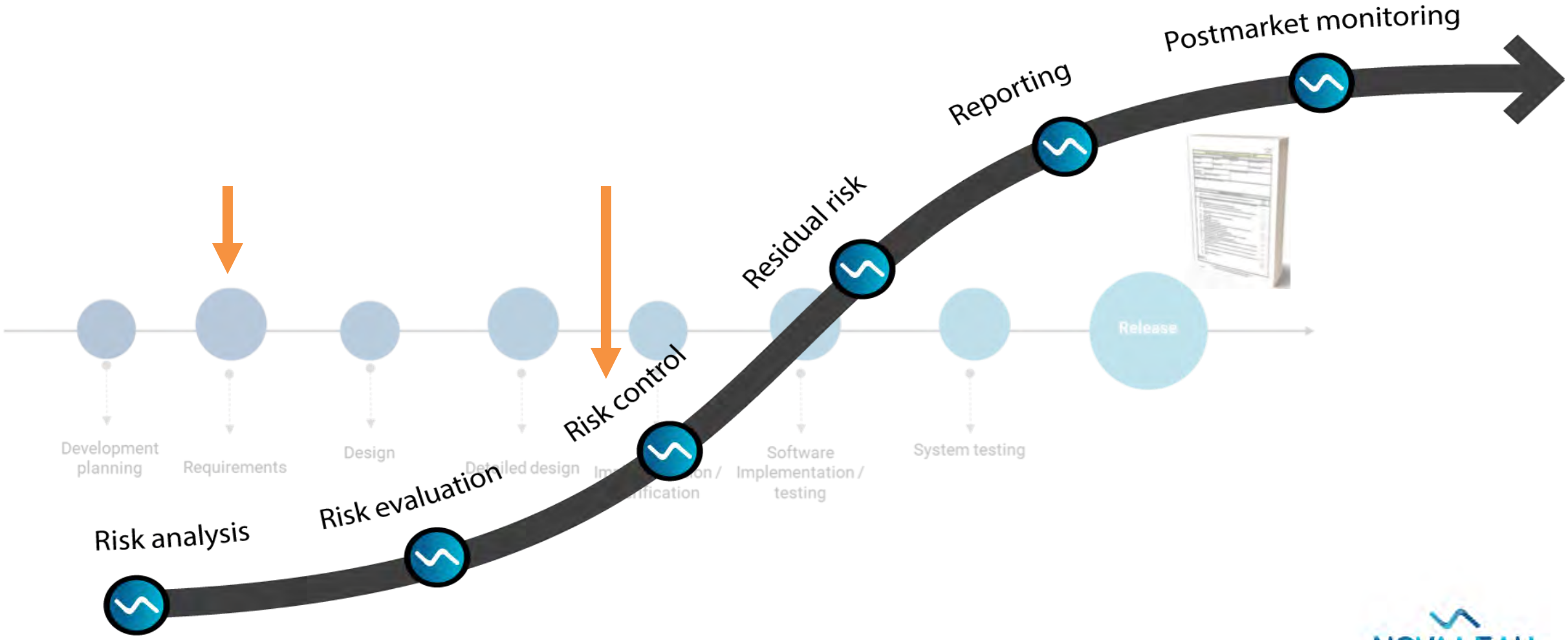
email: anita.finnegan@novaleah.com
twitter: @anita_finnegan

NOVA LEAH

MDS²

Informing design controls

Design controls identification



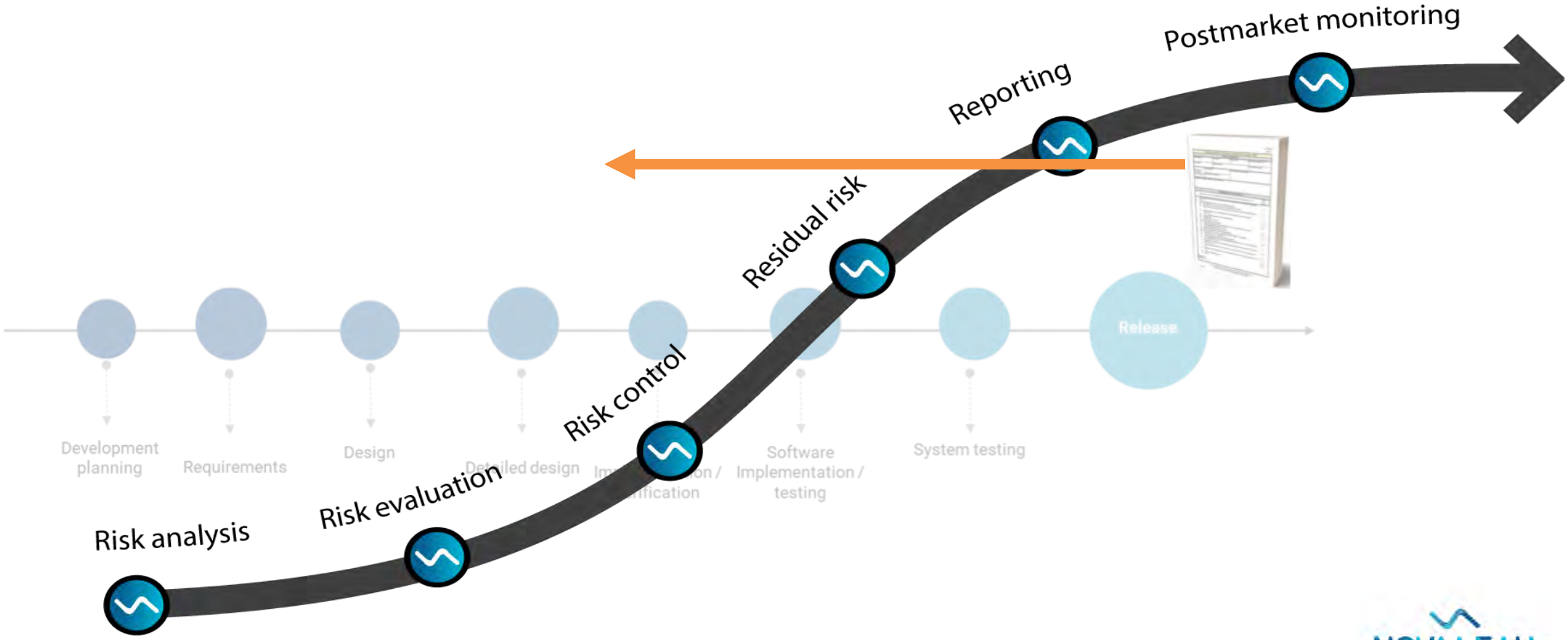
email: anita.finnegan@novaleah.com
twitter: @anita_finnegan

NOVA LEAH

MDS²

Informing design controls

Introduce security capabilities earlier in the cycle



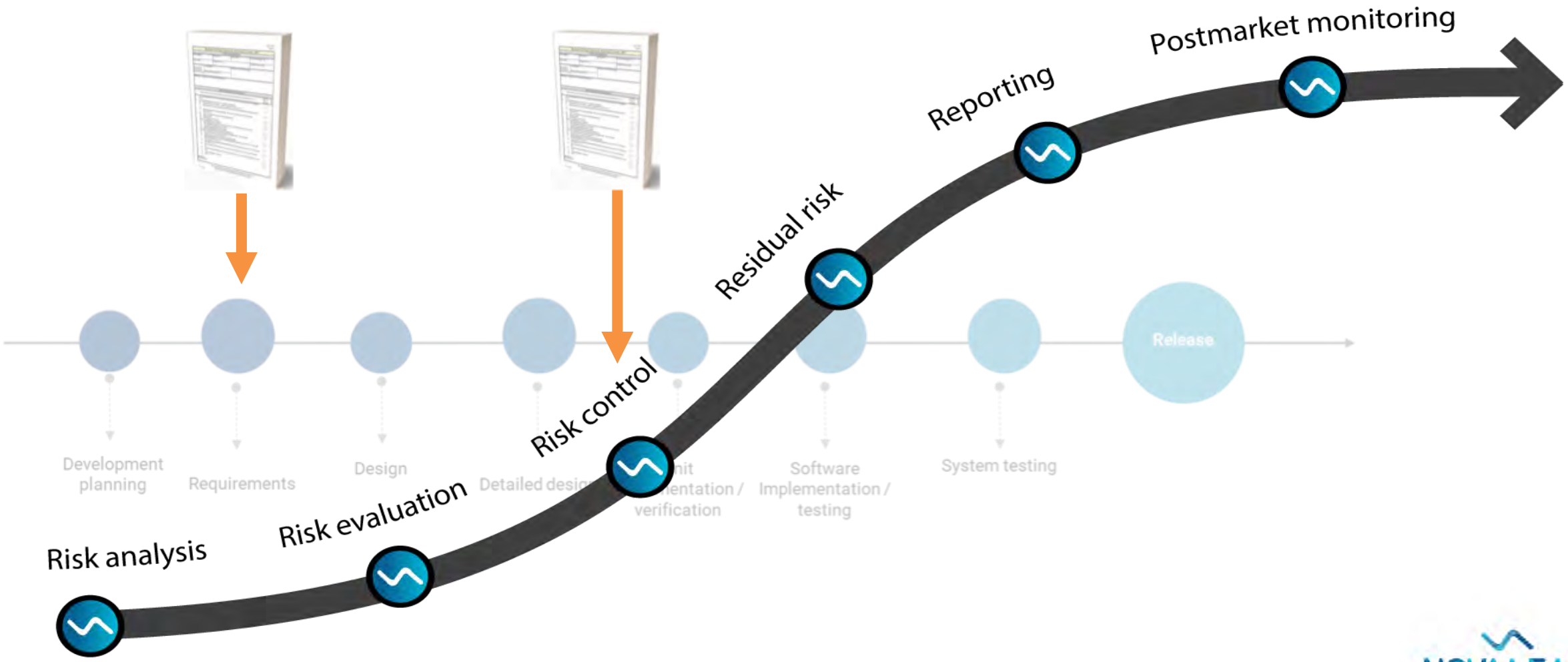
email: anita.finnegan@novaleah.com
twitter: @anita_finnegan

NOVA LEAH

MDS²

Informing design controls

Security capabilities informing development and risk assessment



email: anita.finnegan@novaleah.com
twitter: @anita_finnegan

NOVA LEAH

MDS2 in Threat Modelling

Can a threat be introduced without the capability??

NOVA LEAH

IEC 80001-2-8

Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2

Standard	Ref	Control
SP 800-53	AC-1	Access Control Policy and Management
	AC-11	Session Lock
	AC-12	Session termination
	IA-11	Re-authentication
ISO/IEC 15408-2	FTA_SSL	Session Locking and Termination
	FMT_SAE	Security Attribute Expiration
	FIA_UAU	User Authentication
ISO/IEC 27002	5.1.1	Policies for information security
	5.1.2	Review of the Information Security Policy
	9.1.1	Access control policy
	9.4.2	Secure Log-On Procedures
	11.2.8	Unattended user equipment
	11.2.9	Clear desk and clear screen policy
	18.2.2	Compliance with Security Policies and Standards
ISO 27799	7.2.1	Information Security Policy Document
	7.2.2	Review of the Information Security Policy
	7.8.1.2	Access Control Policy
	7.8.3	Unattended User Equipment
	7.8.3	Clear desk and Clear Screen Policy
	7.8.4	Secure Log-On Procedures
	7.8.4	Session Time-Out
	7.8.4	Limitation of Connection Time
	7.12.3	Compliance with Security Policies and Standards
IEC 62443-3-3	SR 1.10	Session Lock
	SR 2.5	Remote session termination

IEC 80001-2-8

Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2

80001-2-2 Framework Guidance

Provide guidance to healthcare providers and manufacturers for the application of the framework outlined in IEC TR 80001-2-2

Catalogues of Security Control-How To

Addresses each of the security capabilities in 80001-2-2 & identify catalogues of relatable security controls during risk management activities, device implementation, supplier selection, device selection, operation etc.

Through life Cybersecurity Control Guidance

Provide hospitals with a catalogue of management, operational and administrative security controls to maintain the effectiveness of a security capability for a device on a healthcare IT network;

Technical Cybersecurity Control Guidance

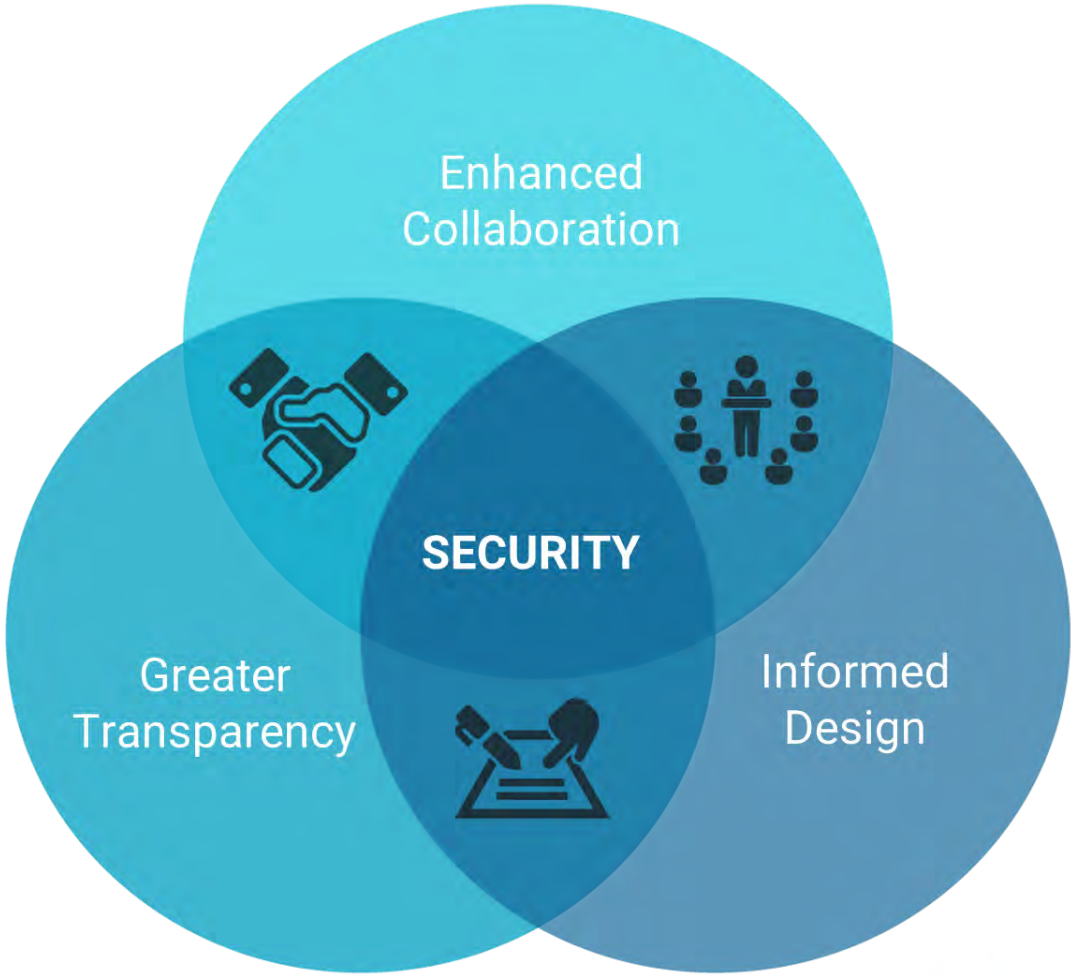
Provide manufacturers with a catalogue of technical security controls for the establishment of each of the 19 security capabilities during product development.

Standard	Ref	Control
SP 800-53	AC-1	Access Control Policy and Management
	AC-11	Session Lock
	AC-12	Session termination
	IA-11	Re-authentication
ISO/IEC 15408-2	FTA_SSL	Session Locking and Termination
	FMT_SAE	Security Attribute Expiration
	FIA_UAU	User Authentication
ISO/IEC 27002	5.1.1	Policies for information security
	5.1.2	Review of the Information Security Policy
	9.1.1	Access control policy
	9.4.2	Secure Log-On Procedures
	11.2.8	Unattended user equipment
	11.2.9	Clear desk and clear screen policy
	18.2.2	Compliance with Security Policies and Standards
ISO 27799	7.2.1	Information Security Policy Document
	7.2.2	Review of the Information Security Policy
	7.8.1.2	Access Control Policy
	7.8.3	Unattended User Equipment
	7.8.3	Clear desk and Clear Screen Policy
	7.8.4	Secure Log-On Procedures
	7.8.4	Session Time-Out
	7.8.4	Limitation of Connection Time
	7.12.3	Compliance with Security Policies and Standards
IEC 62443-3-3	SR 1.10	Session Lock
	SR 2.5	Remote session termination

Conclusion

Value of MDS2

- Baseline industry expectations
- Increased pick up and recognition
- Strong foundation for risk assessment & threat modelling
- Easier to update and maintain MDS2 when directly aligned with design controls and risk assessment
- Adding value to the early stage life cycle



NOVA LEAH

NOVA LEAH

THANK YOU

email: anita.finnegan@novaleah.com
twitter: @anita_finnegan
@NovaLeahLtd