MASTER OF SCIENCE
IN ENGINEERING

TSM_SecIndOpT

Product lifecycle (PL)

Version: 1.2

Luca Haab | 13.04.2026 | Cours MSE

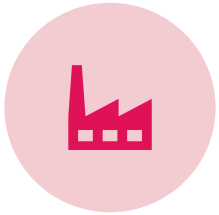
What is Product Lifecycle Management

- PLM is a key strategy in business
- It manages products from first concept to their eventual retirement
- It provides a framework for overseeing the different stages a product goes through, offering structure and consistency

PLM : a picture is 1000 words worth

IDEA

DESIGN



MANUFACTURING

SERVICE AND MAINTENANCE

DISPOSAL

PLM - Idea

IDEA

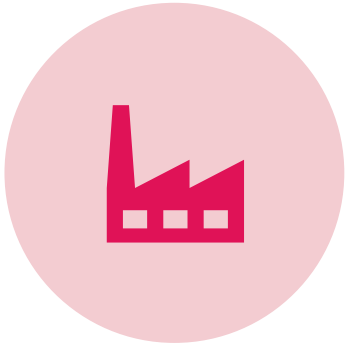
- New ideas based on market research
- Creative but structured phase to check whether product can succeed
- Understanding customer needs and market trends to create product ideas with strong market potential

PLM - Design

DESIGN

- Detail specifications, plans and prototypes
- Ensure that it is not only functional but can also be produced
- Change management ensures that changes are tracked and everyone is on the latest version
- Marketing teams work on packaging, branding and positioning strategies to make the product appealing to the target audience

PLM - Manufacturing



MANUFACTURING

- Theoretical designs -> real products
- Includes sourcing materials, setting up production lines and implementing quality control measure
- PLM ensures design data is integrated into manufacturing processes to keep errors down and improve efficiency
- Marketing might involve ensuring that the product meets the brand promises and quality standards that were advertised

PLM – Service and Maintenance

SERVICE AND MAINTENANCE

- Includes distribution, customer service, and maintenance
- PLM systems help track product performance and customer feedback, providing data that can be used to improve future versions of the product
- Effective management here helps to ensure customer satisfaction and can lead to a longer product lifespan

PLM - Disposal

DISPOSAL

- Disposal phase deals with the end of the product's lifecycle - including the safe and responsible disposal or recycling of products
- Managed according to environmental regulations and sustainability practices

PLM in Marketing

- Introducing the product to the market
- Promotion of the product
- Management of brand image

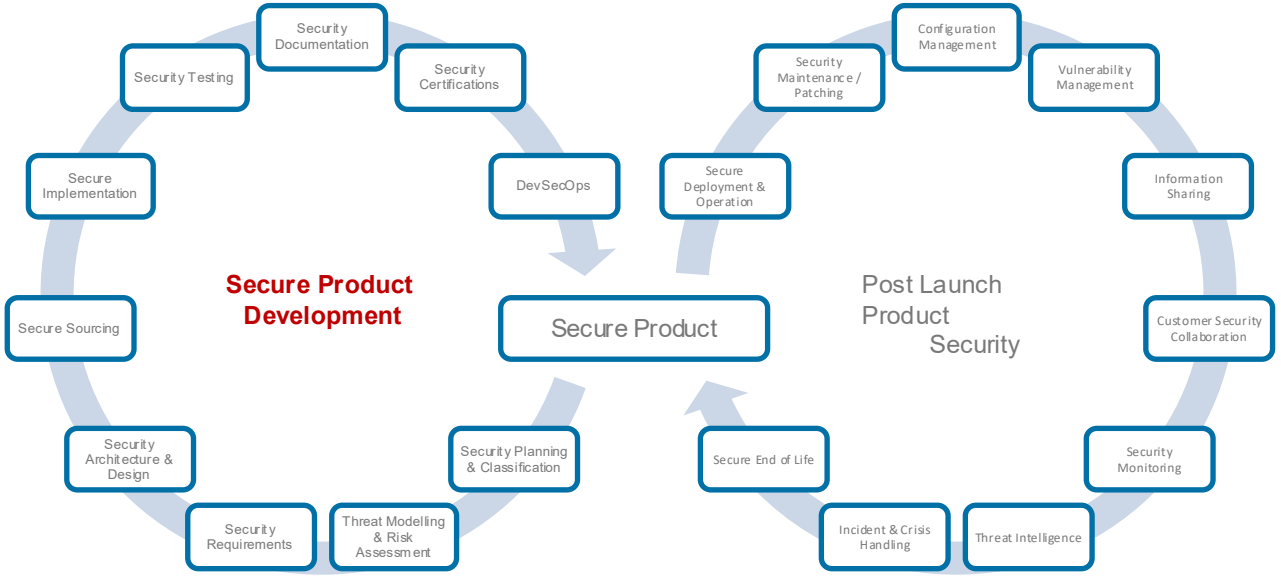
PLM for Product / Service and Marketing

Principles of PLM are constant – be in development, manufacturing or marketing

PLM manages the entire lifecycle of a product efficiently and effectively, ensuring that everyone involved has access to current information and that all processes align towards the common goal of delivering high quality products to the market

Adding cybersecurity to it

Product Cybersecurity Lifecycle (HSLU SPREN)



Cyber Security Management System(s)

Development & Production Security

Organization, Culture, Awareness & Training

Security Risk Management

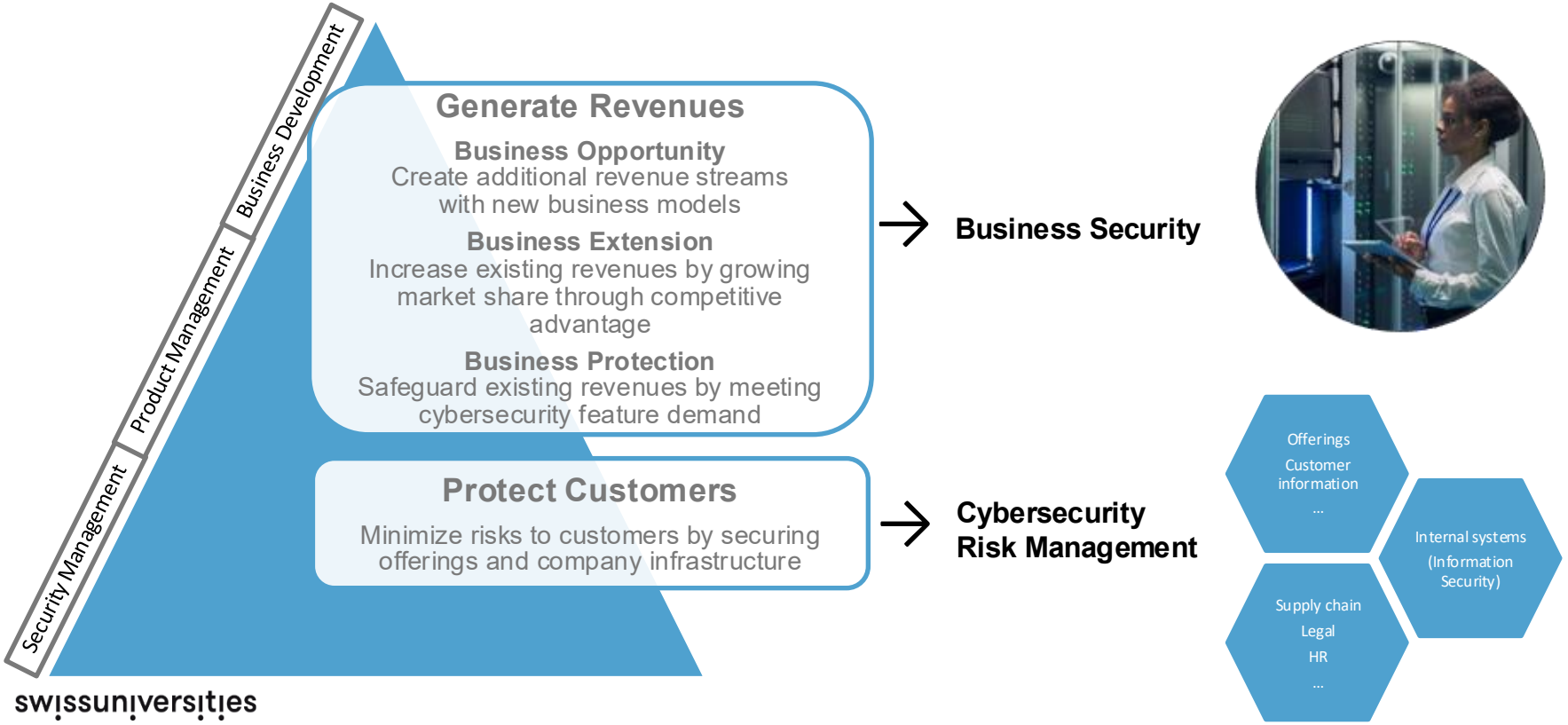
Supply Chain Security

swissuniversities

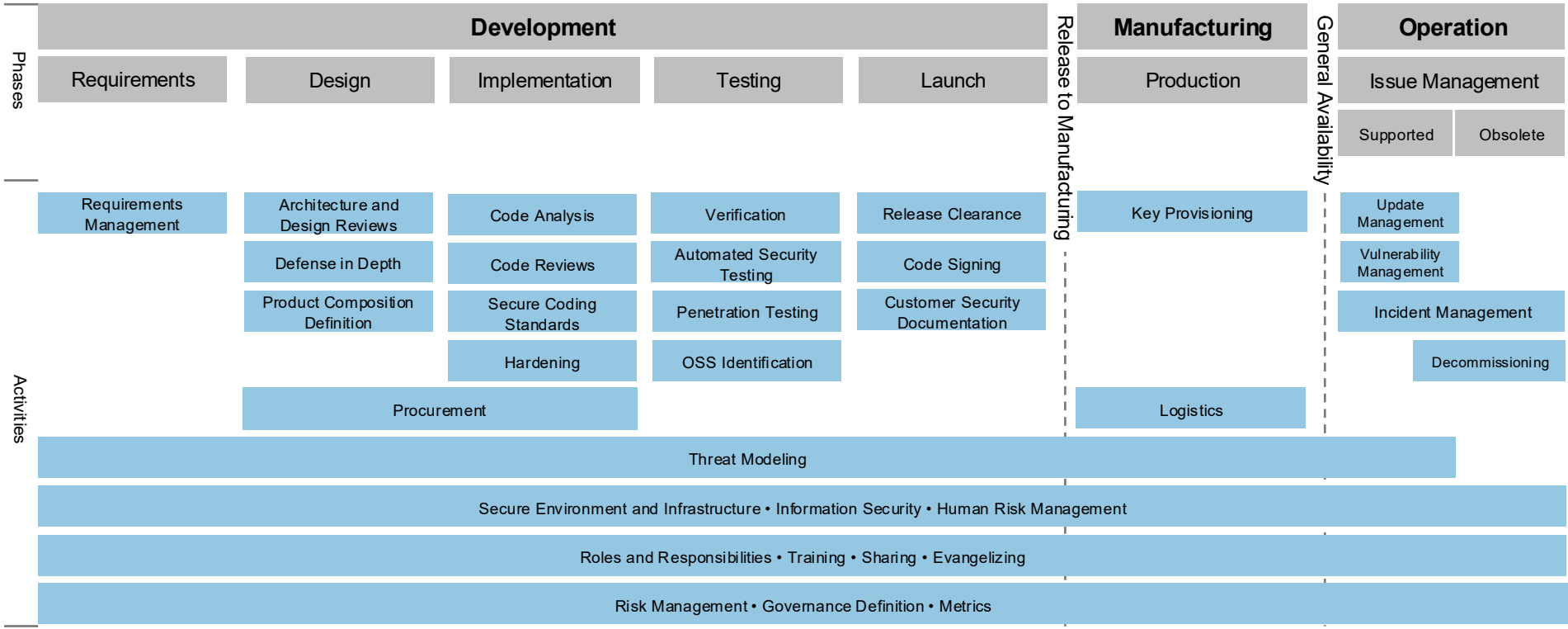
IEC 62443-4-1

- Practices for Secure Development & Maintenance of IACS Products
- Covers
  - Pre- & Post Launch Product Security
  - Development Security
  - Credential Management
- CMMI-based Maturity Levels 1-4 per practice
- Classification concept "Security Level" 1-5 to tailor controls

Company organization

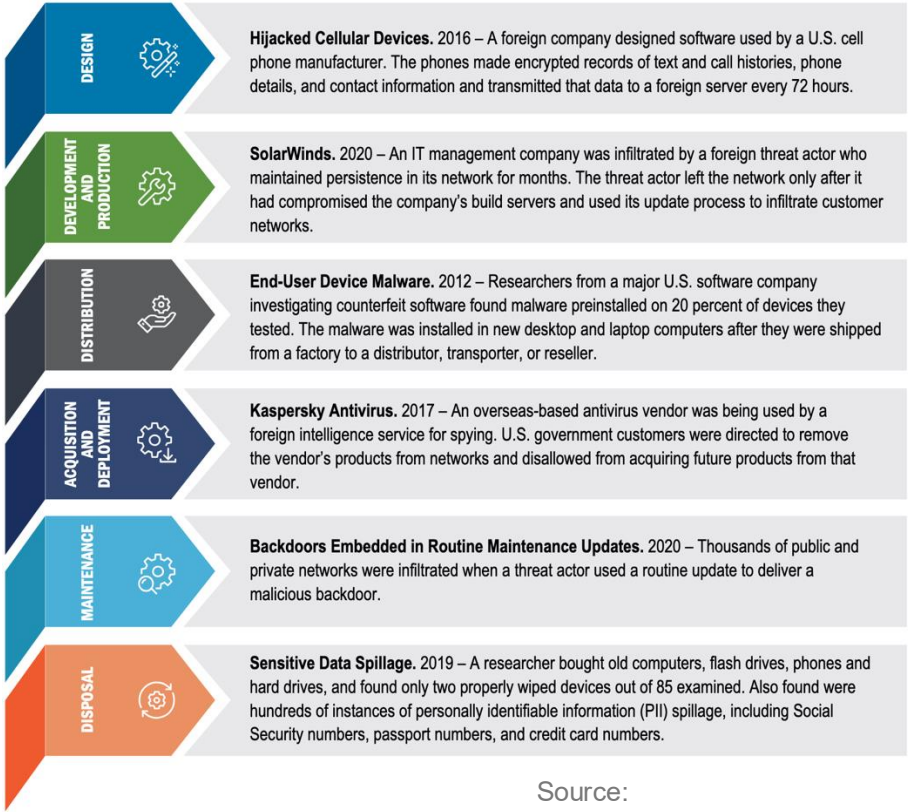


Activities within a company – big picture



Generated with https://wordclouds.ethz.ch/

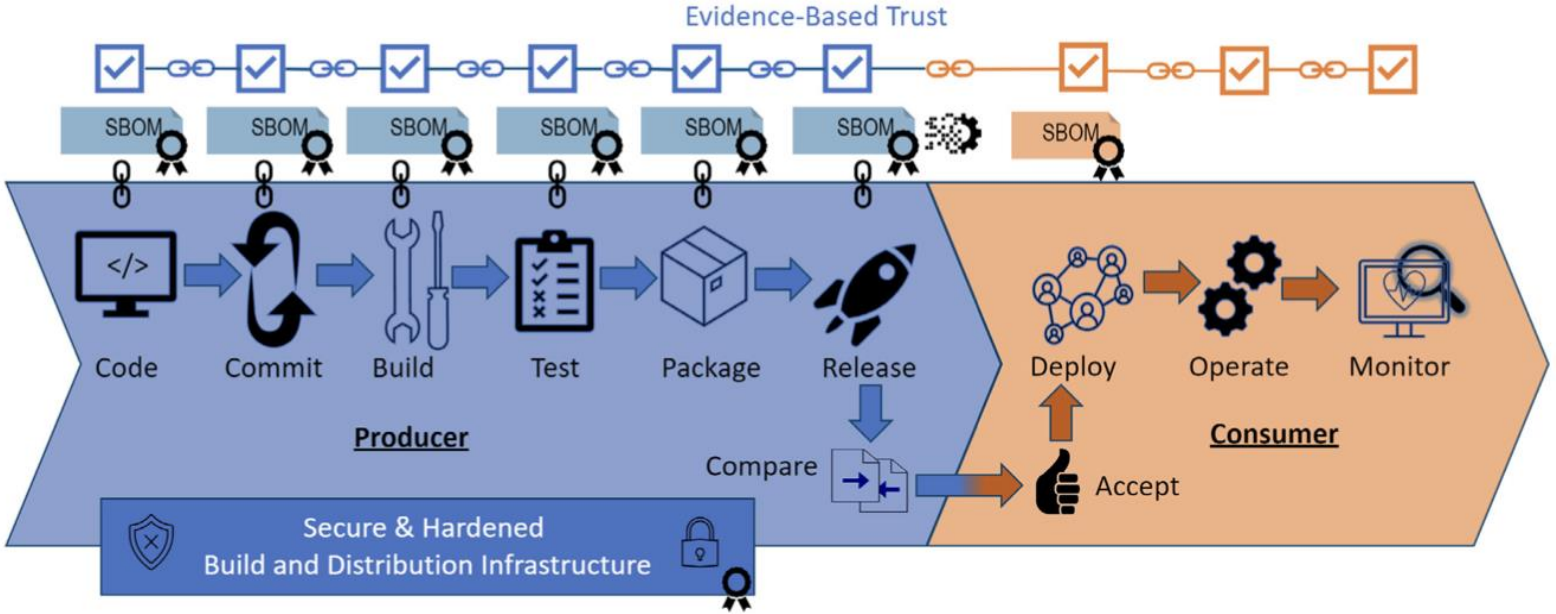
Securing Software Supply Chains



Concrete examples of attacks in different phases of development

Source: https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508.pdf

Securing Software Supply Chains – MITRE's proposal



1: https://www.mitre.org/news-insights/publication/deliver-uncompromised-securing-critical-software-supply-chains

SW Bill Of Material (SBOM)

The Case for Transparency

The Administration notes in the EO, "the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is."[2] In the modern world, software systems involve complex, dynamic — and, too often, obscure — supply chains. Bringing transparency to the components and connections within and across supply chains is important to discovering and addressing the weak links in those chains. SBOMs are a critical step toward securing the software supply chain. Without them, a lack of transparency into the contributors, composition, and functionality of these systems contributes substantially to cybersecurity risks and increases costs of development, procurement, and maintenance.

Transparency is best achieved using an understandable model supported by industry. An SBOM model achieves this systematic sharing by tracking component metadata, enabling mapping to other sources of information, and tying the metadata to software as it moves down the supply chain and is deployed. To scale this model globally, it is necessary to address the problem of universally identifying and defining certain aspects of software components to allow the data to be effectively and efficiently consumed by downstream users.[3]

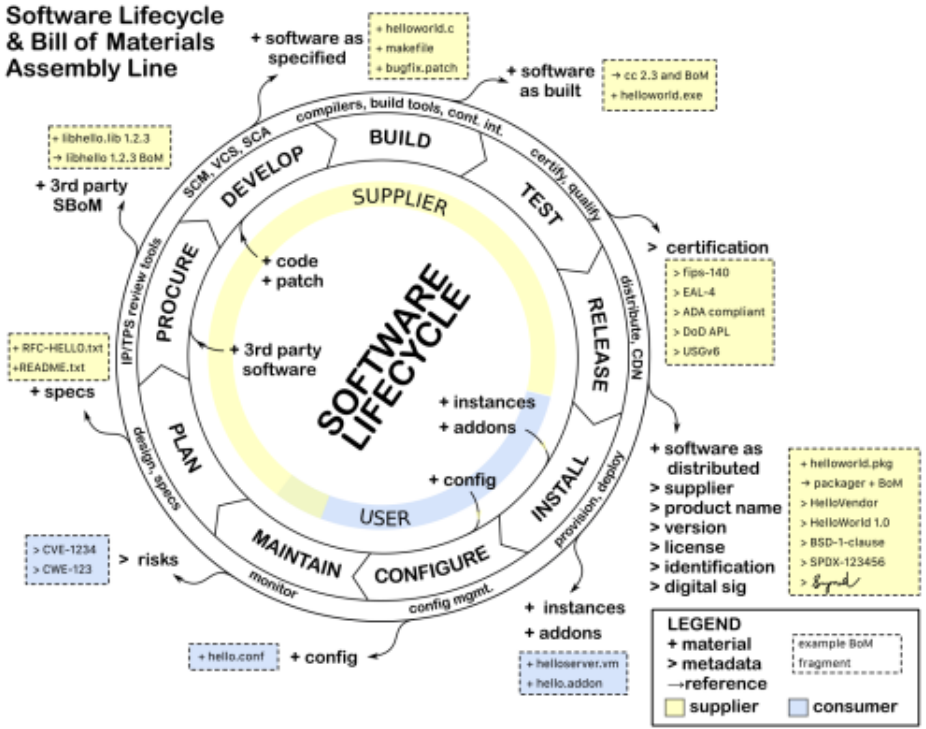
Note: "Administration" refers to the administration of the United States of America

Source: https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

SBOM - MVD

Minimum viable definition:

- The **organization/person** that created the artifact.
- The **tool** used to generate the SBOM
- The **timestamp** when the SBOM was generated
- **Component name**
- **Component version** number
- A **UUID** (CPE, PURL, SWID)
- **Relationship** with other components - with an enumeration of the included dependent components



Extracted from https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

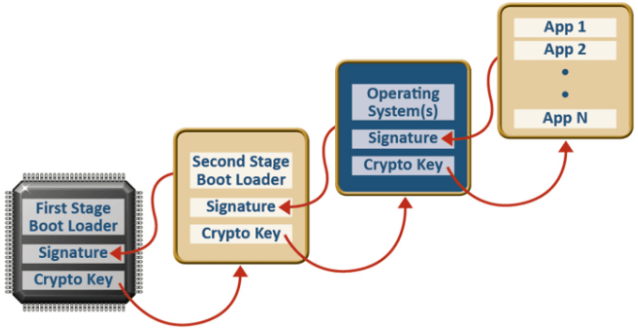
SBOM – Some more requirements

- **Frequency**: SBOMs must be updated per any change in content or version of the software product
- **Depth**: The SBOM must contain all direct and indirect dependencies of the software product
- **Known Unknowns**: In any case that a piece of information is missing, the SBOM must state whether that information is missing because it is unavailable, unknown, etc.
- **Distribution & Delivery**: The SBOM must be accessible to the customer by means of being both machine- and human-readable
- **Access Control**: Proper access control must be set to access the SBOM
- **Accommodation of Mistakes**: All users of SBOM must acknowledge that the standards are still in development and be patient with mistakes in the process and substantial changes to the standard.

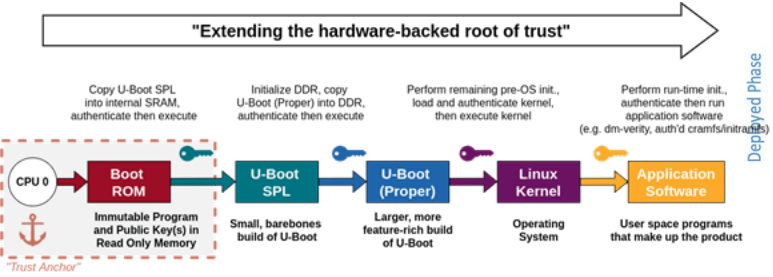
SBOM in practice

Name	CycloneDX	SPDX (aka Software Package Data Exchange)	SWID (aka SoftWare Identification)
Who & When	OWASP @ 2017	Linux Foundation @ 2010	NIST @ 2009
Audience	Developer-centric	Standard-centric (ISO/IEC 5962:2021)	Standard-centric (ISO/IEC 19770-2:2015)
(Original) Focus	Security	Licensing	Deployment Life Cycle
Supported Unique Identifiers	SPDX License ID SWID, PURL, CPE SHA, BLAKE	SPDX License ID SWID, PURL, CPE	SWID, CoSWID
Main Advantage	Verbosity, Security Info	Components Relationships	Government-backed, multi-purpose

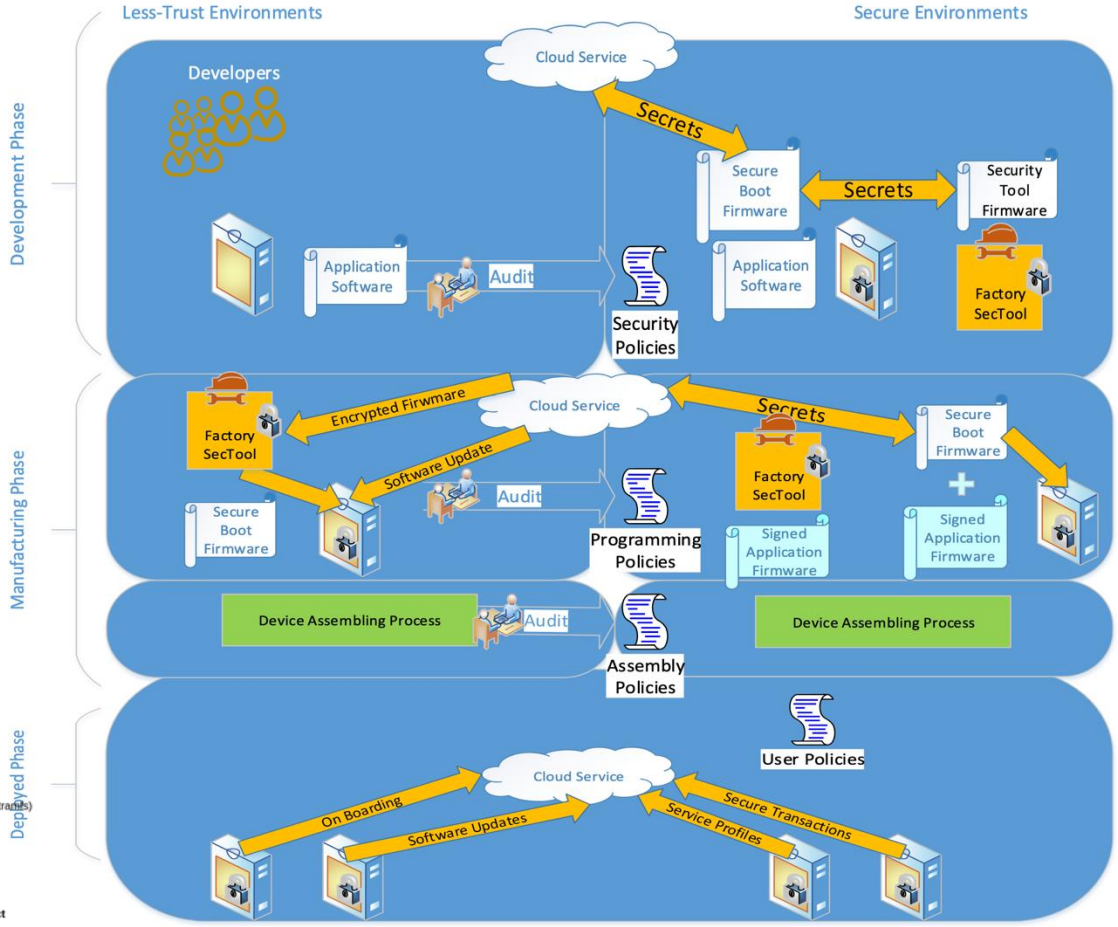
(I)IoT & Secure boot



Source. https://theembeddedkit.io/blog/enable-secure-boot-in-embedded-systems/



Source: https://www.nccgroup.com/us/research-blog/shining-new-light-on-an-old-rom-vulnerability-secure-boot-bypass-via-dcd-and-csf-tampering-on-nxp-imx-devices/



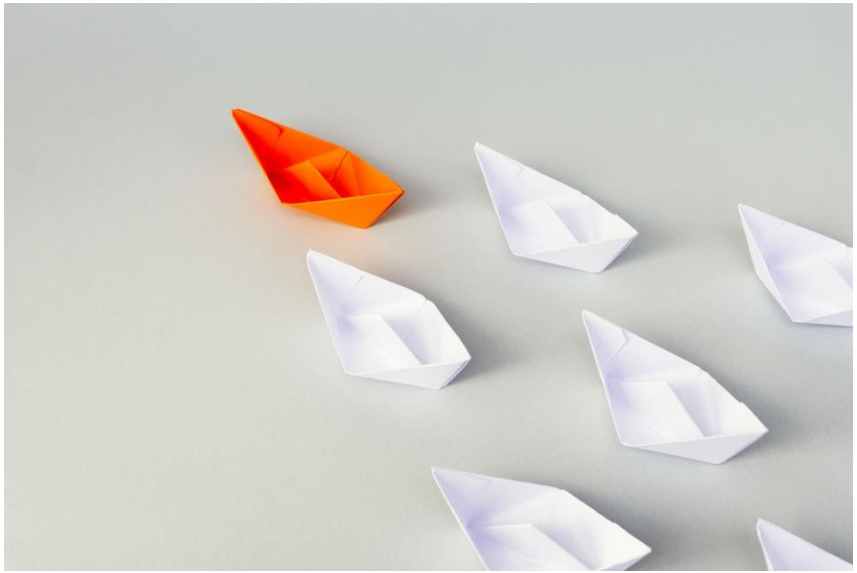
Source: https://www.nxp.com/docs/en/supporting-information/Designing-Secure-IoT-Devices-Starts-with-a-Secure-Boot.pdf

(I)IoT & Secure boot - Challenges

- Secure boot is vendor-specific as some require NDA to access documentation
- Key management (on and off device)
- Key rotation
- OSS licences (specifically GPL[1])
- 3rd-party applications integration

[1]: https://events19.linuxfoundation.org/wp-content/uploads/2017/11/Safely-Copylefted-Cars-Reexamining-GPLv3-Installation-Information-Requirements-ALS-Bradley-Kuhn-Behan-Webster-1.pdf and https://www.fsf.org/campaigns/secure-boot-vs-restricted-boot/whitepaper-web

“Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations” – a guidance



Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf

Cybersecurity Supply Chain Risk Management Practices

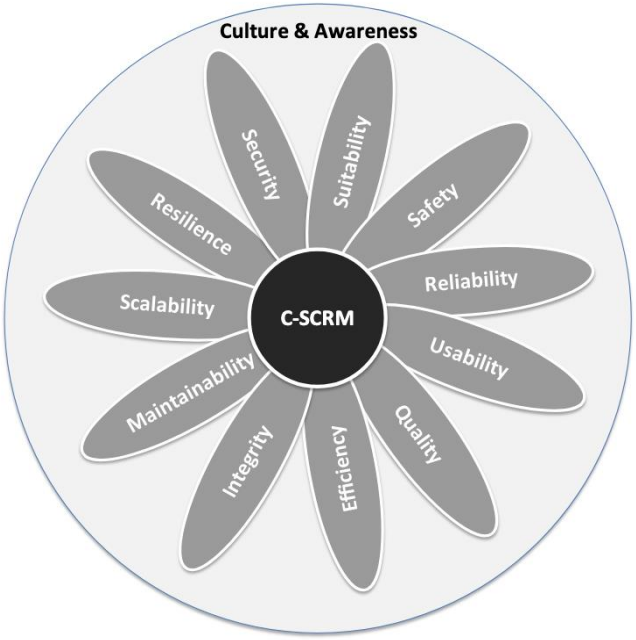
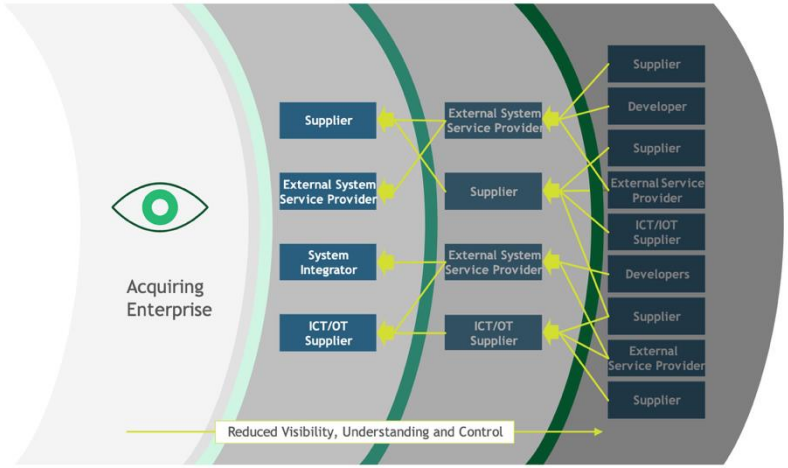


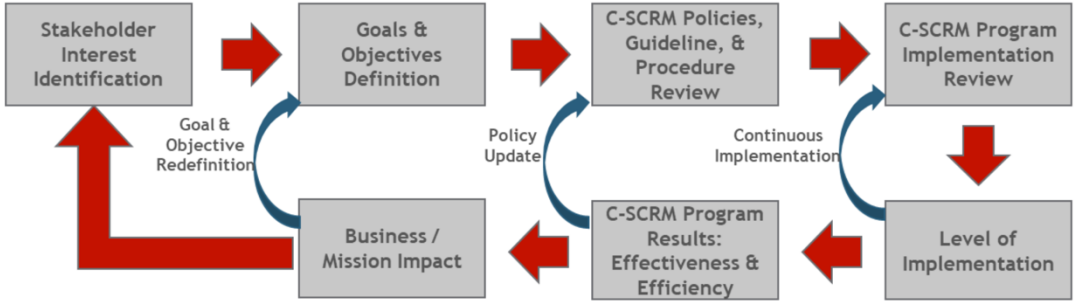
Fig. 1. Dimensions of C-SCRM

"In this document, the practices and controls described for Cybersecurity Supply Chain Risk Management (C-SCRM) apply to both information technology (IT) and operational technology (OT) environments and are inclusive of IoT. Similar to IT environments that rely on ICT products and services, OT environments rely on OT and ICT products and services, with cybersecurity risks arising from ICT/OT products, services, suppliers, and their supply chains. Enterprises should include OT-related suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers within the scope of their C-SCRM activities.

Sources: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf

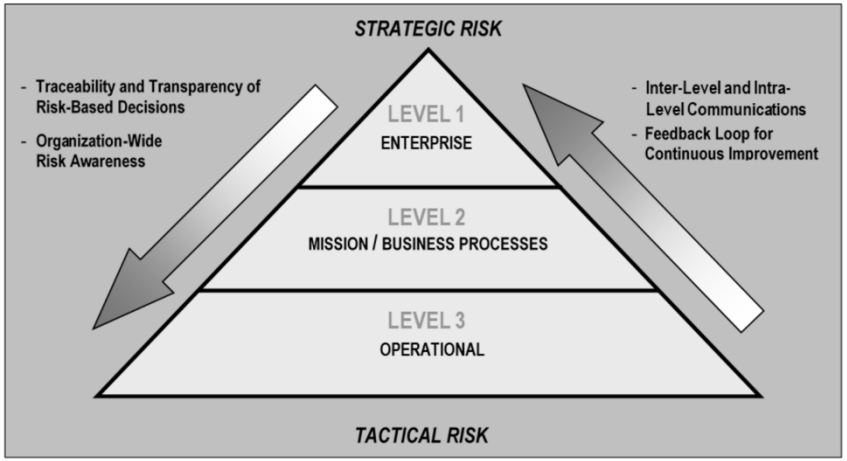
Blind side - Aligning the stakes





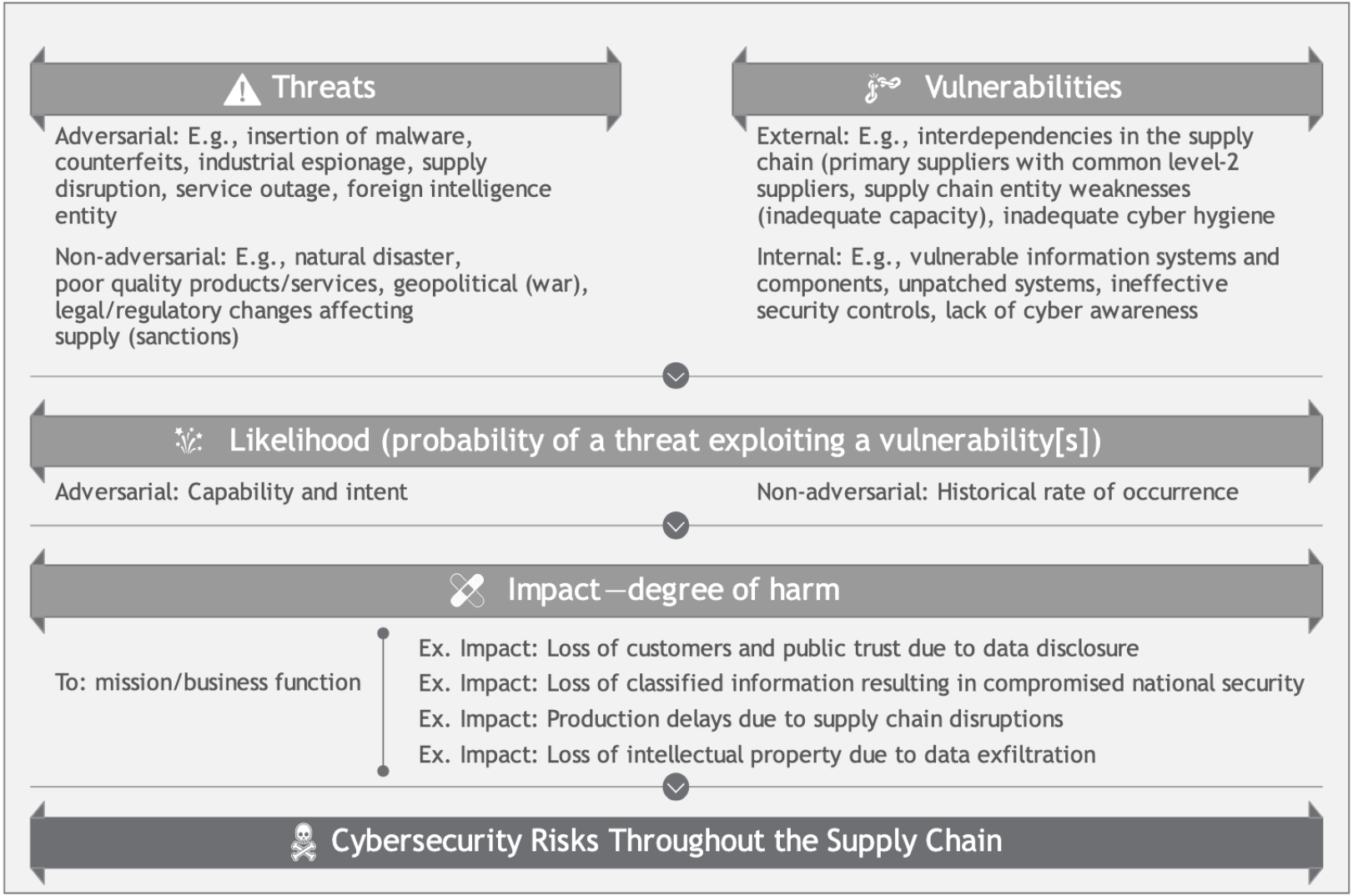
Sources: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf

Supply chain



- ICT/OT relies on a globally distributed, interconnected supply chain ecosystem that consists of public and private sector entities
- This ecosystem offers benefits such as cost savings, interoperability, rapid innovation, product feature variety and the ability to choose between competing vendors. With the risk the same also introduces a variety of cybersecurity risks throughout the supply chain
- Cybersecurity Supply Chain Risk Management (C-SCRM) is a systematic process that aims to help enterprises manage cybersecurity risks throughout the supply chain. Enterprises should identify, adopt, and tailor the practices described in this document to best suit their unique strategic, operational, and risk context

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf



Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf

swissu

Threat Scenario	**Threat Source**	Nation-state with significant resources looking to steal IP		
	Vulnerability	Supplier considering partnership with company that has relationship with threat source		
	Threat Event Description	Nation-state helps KXY meet industry compliance requirements, and ABC Company partners with KXY to develop chips		
	Existing Practices	Strong contractual requirements as to the functionality of the system and elements Comprehensive inventory tracking system at ABC Company Industry compliance requirements		
	Threat Event Outcome	Nation-state extracts technology threat actor, modifies technology, or exploits previously unknown vulnerability		
Enterprise units, processes, information, assets, or stakeholders affected		KXY Supplier ABC Company integrator functionality testing Technology users Other federal agencies / customers		
Risk	**Impact**	Technology modified / vulnerabilities exploited – High		Technology sold to interested parties – Moderate
	Likelihood	Moderate		Moderate
	Risk exposure (Impact x Likelihood)	High		
	Acceptable Level of Risk	Moderate		
Mitigation	**Potential Mitigating Strategies and C-SCRM Controls**	(1) Improve traceability and monitoring capabilities	(2) Increase provenance and information control requirements	(3) Choose another supplier
	Estimated Cost of Mitigating Strategies	20 % increase	20 % increase	40 % increase
	Change in Likelihood	Moderate → Low		
	Change in Impact	High → Moderate		
	Selected Strategies	Develop and require unique, difficult-to-copy labels, or alter labels to discourage cloning or modification of the component [C-SCRM_PE-3]. Minimize the amount of information that is shared to suppliers. Require that the information be secured [C-SCRM AC-21]. Require provenance be kept and updated throughout the SDLC [C-SCRM_SR-4].		
	Estimated Residual Risk	Moderate – The residual risk was determined to be equivalent to the existing risk without the partnership.		

An Example: Industrial Espionage

- ABC Company, a semiconductor (SC) company used by the enterprise to produce military and aerospace systems, is considering a partnership with a KXY Co. to leverage their fabrication facility. This would represent a significant change in the supply chain related to a critical system element.
- While not classified, the element that KXY would be expected to manufacture is unique, patented, and critical to the operational status of the systems. The loss of availability of the element while the system is operational could have significant, immediate impacts across multiple agencies and the civilian populous, including the loss of life and millions of dollars in damages

Source: C.1.3. SCENARIO 3: Industrial Espionage, NIST SP 800-161r1-upd1