ISO 21434

A Brief Overview

Presented by the GENIVI Security Team

GENIVI®

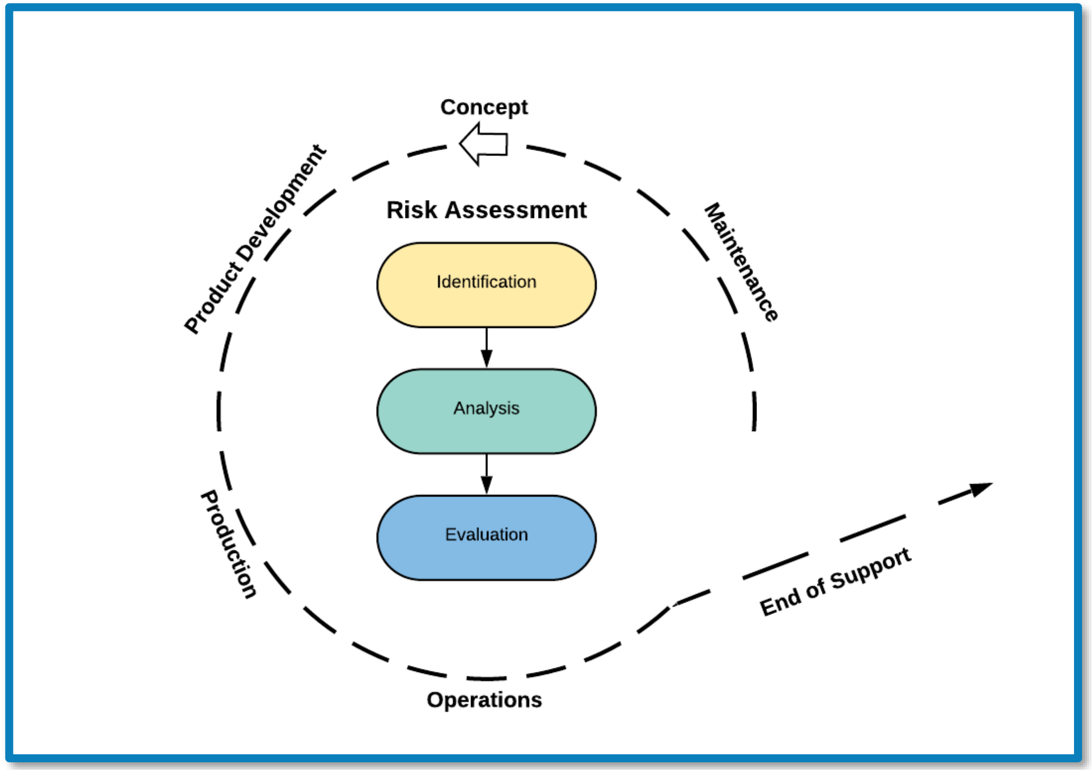
Overall and Project-Dependent Cybersecurity

Key Takeaways: Clauses 5 and 6

- Organizations Must Maintain Documentation Relevant to ALL Cybersecurity Activities
  - Iterative Process
  - Assign and Communication of Cybersecurity Roles and Responsibilities to Appropriate Authorities

- Plan(s) Must Include:
    - Objectives of the Activities Performed
    - Dependencies of these Activities
    - Who is Responsible for the Activity
    - Required Resources
    - Time (Start, End, Duration)
    - ID of the Work Product
        - Work products are the output from each of the Clauses

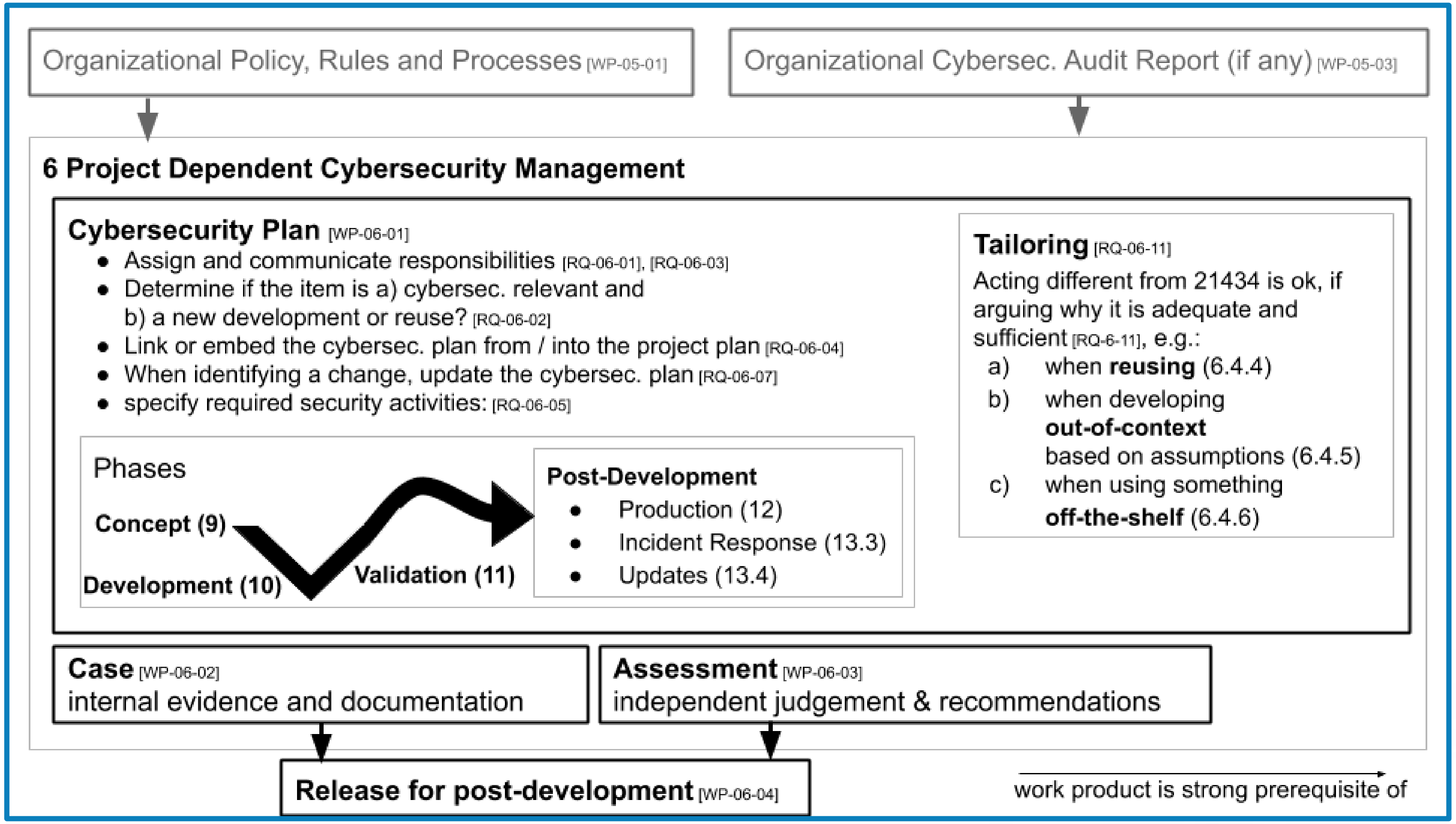
Clause 5 Process Flow



* All figures and charts are original works by GENIVI Security Team

Iterative Process	• Allows for evolution of Requirements and Activities related to Overall and Project-Dependent Goals
Easily Applied Against Current Standards	• Aligns to ISO 31000, 26262
Foster And Maintains Culture	• Creates Normative and Formal Discussions Around Cybersecurity

Clause 6 Process Flow



Organizational Policy, Rules and Processes [WP-05-01]

Organizational Cybersec. Audit Report (if any) [WP-05-03]

6 Project Dependent Cybersecurity Management

Cybersecurity Plan [WP-06-01]

- Assign and communicate responsibilities [RQ-06-01], [RQ-06-03]
- Determine if the item is a) cybersec. relevant and b) a new development or reuse? [RQ-06-02]
- Link or embed the cybersec. plan from / into the project plan [RQ-06-04]
- When identifying a change, update the cybersec. plan [RQ-06-07]
- specify required security activities: [RQ-06-05]

Phases

Concept (9)

Development (10)

Validation (11)

Post-Development

- Production (12)
- Incident Response (13.3)
- Updates (13.4)

Tailoring [RQ-06-11]

Acting different from 21434 is ok, if arguing why it is adequate and sufficient [RQ-6-11], e.g.:

a) when **reusing** (6.4.4)

b) when developing **out-of-context** based on assumptions (6.4.5)

c) when using something **off-the-shelf** (6.4.6)

Case [WP-06-02]
internal evidence and documentation

Assessment [WP-06-03]
independent judgement & recommendations

Release for post-development [WP-06-04]

work product is strong prerequisite of

Begins with Work Products from Clause 5

Allows for integration into Systems Engineering “V” model

Customizeable

Subject to:

- Change Management
- Requirements Management
- Document Management

* All figures and charts are original works by GENIVI Security Team

Additional Notes Clause 6:

- Off-the-shelf Components Are Allowed If:
  - Can Comply With Current Requirements
  - Is Suitable For The Application
  - Sufficient To Support The Cybersecurity Activities Of The Plan
- All Judgments Require An Independently Reviewed Rationale
  - Could Be Costly!

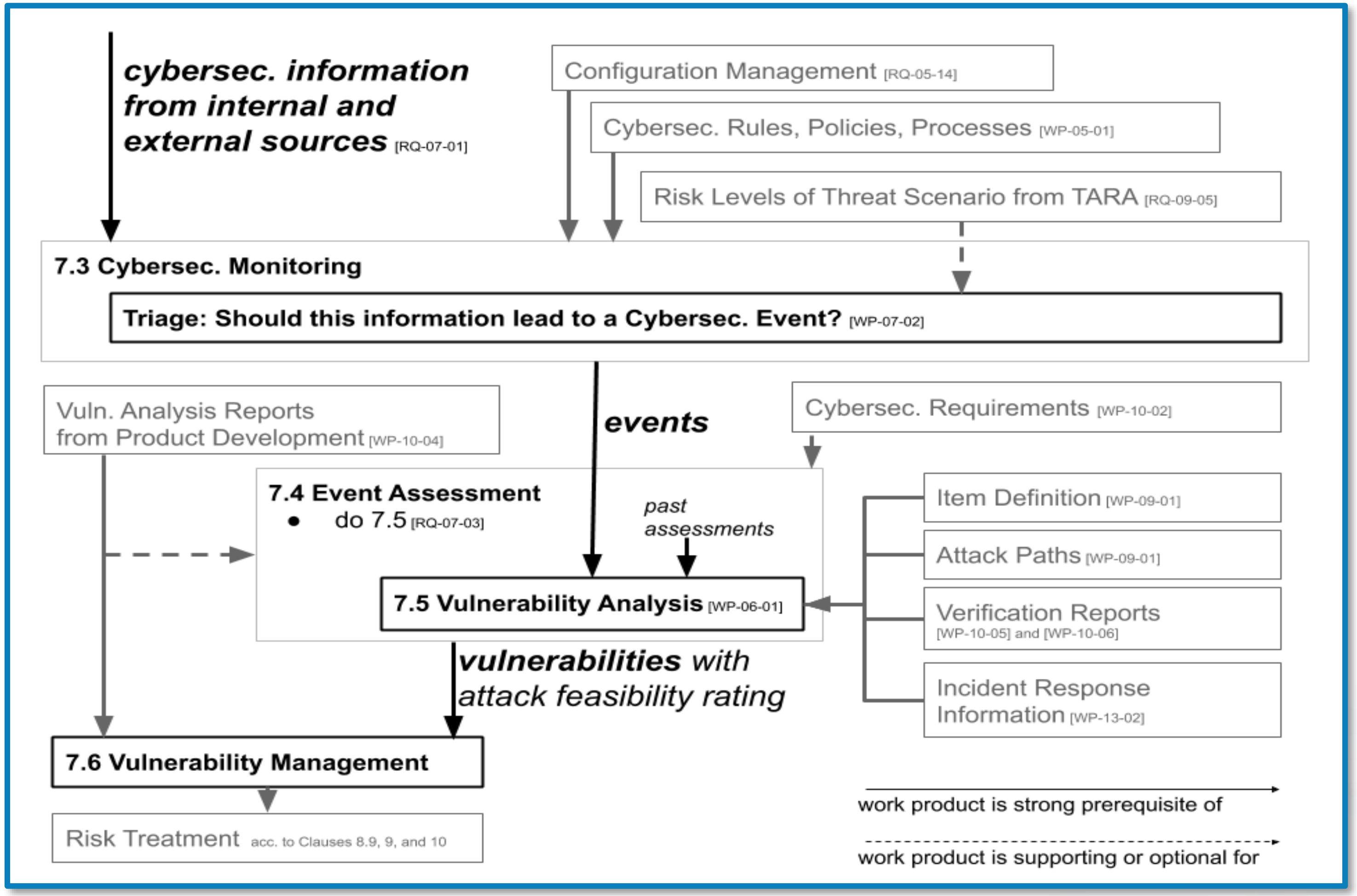
This Photo is licensed under CC BY-SA

Continuous Cybersecurity Activities

Key Takeaways: Clause 7

- Process For Management of Vulnerabilities
  - Monitor for Vulnerabilities
  - Detect Events
  - Assess Events
  - Analysis of Events
  - Management (Control or Correction) of Vulnerabilities
- Management of Vulnerability ID Shall Include (if applicable):
  - Missing Requirements
  - Design Weaknesses
  - Bugs/Wrong Implementation
  - Process Failures
  - Use of Deprecated Functions (Cryptographic)
- If New Information That Changes Risk, Vulnerability is No Longer Considered "Managed"

Clause 7 Process Flow



cybersec. information from internal and external sources [RQ-07-01]

Configuration Management [RQ-05-14]

Cybersec. Rules, Policies, Processes [WP-05-01]

Risk Levels of Threat Scenario from TARA [RQ-09-05]

7.3 Cybersec. Monitoring

Triage: Should this information lead to a Cybersec. Event? [WP-07-02]

Vuln. Analysis Reports from Product Development [WP-10-04]

events

Cybersec. Requirements [WP-10-02]

7.4 Event Assessment

- do 7.5 [RQ-07-03]

past assessments

7.5 Vulnerability Analysis [WP-06-01]

Item Definition [WP-09-01]

Attack Paths [WP-09-01]

Verification Reports [WP-10-05] and [WP-10-06]

Incident Response Information [WP-13-02]

***vulnerabilities** with attack feasibility rating*

7.6 Vulnerability Management

Risk Treatment acc. to Clauses 8.9, 9, and 10

work product is strong prerequisite of

work product is supporting or optional for

* All figures and charts are original works by GENIVI Security Team

Notate Sources of Information Monitoring

Triage Decisions

Analysis Should be Tied to Vulnerability IDs

Subject to:

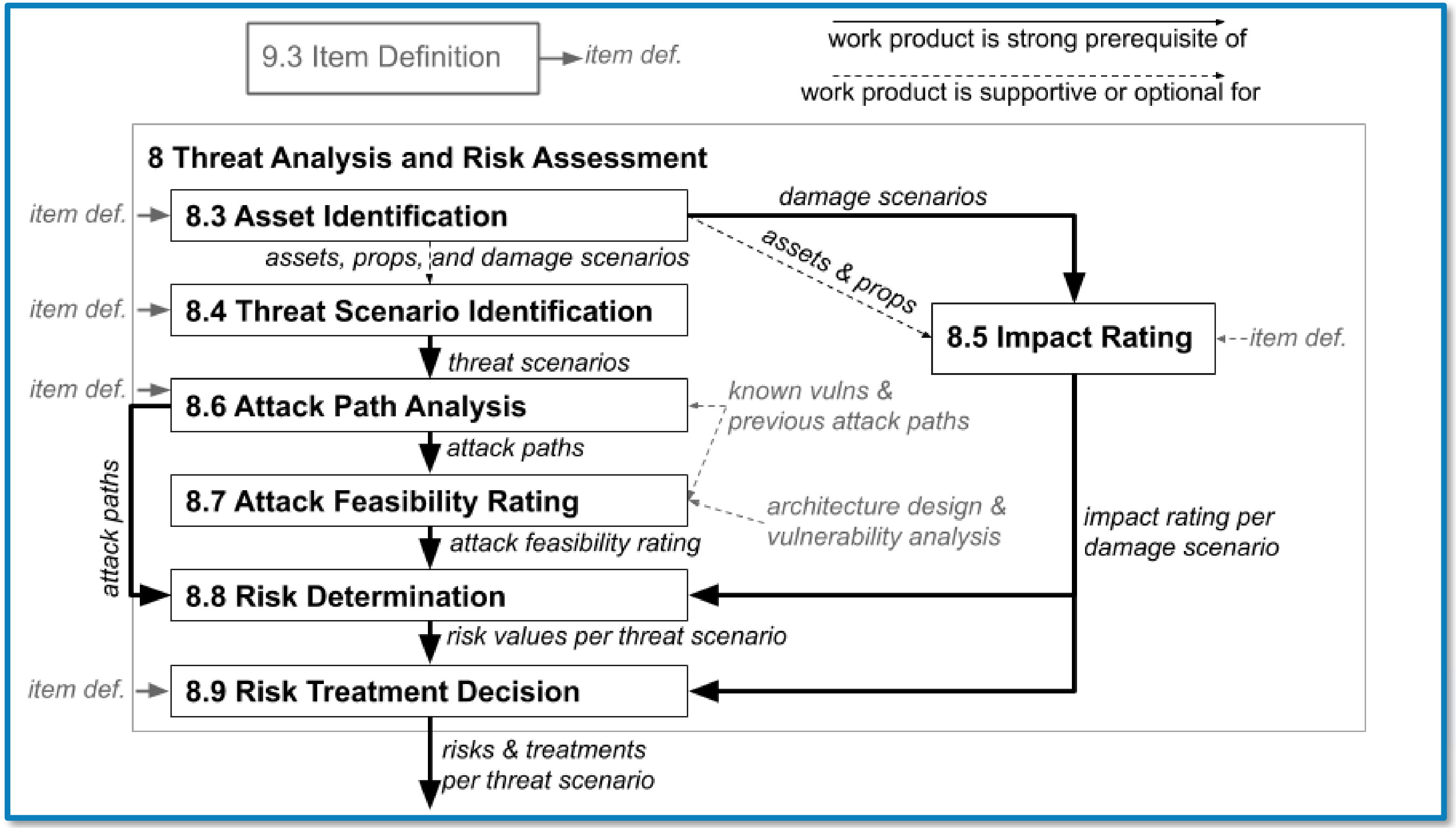
- Incidence Response
- Informational Updates
- Required Reporting

Risk Assessment Methods

Key Takeaways: Clause 8

- All Risk Scenarios Should be Assessed against **SFOP**:
  - **S**afety (Recommends Using ISO 26262)
  - **F**inancial
  - **O**perational
  - **P**rivacy
- Impact Ratings for Each Impact Category
  - Severe
  - Major
  - Moderate
  - Negligible
- Allows for the following approaches for Risk Assessment:
  - Attack Potential-based
  - Attack Vector-based
  - CVSS[2]

Clause 8 Process Flow



9.3 Item Definition → item def.

work product is strong prerequisite of

work product is supportive or optional for

8 Threat Analysis and Risk Assessment

item def. → 8.3 Asset Identification

damage scenarios

assets, props, and damage scenarios

assets & props

item def. → 8.4 Threat Scenario Identification

8.5 Impact Rating ← item def.

threat scenarios

item def. → 8.6 Attack Path Analysis

known vulns & previous attack paths

attack paths

8.7 Attack Feasibility Rating

architecture design & vulnerability analysis

attack feasibility rating

impact rating per damage scenario

attack paths

8.8 Risk Determination

risk values per threat scenario

item def. → 8.9 Risk Treatment Decision

risks & treatments per threat scenario

Impact Ratings Are Set by 21434

Must Be Documented to Threat/Vulnerability ID

Impact Rating Tied to Risk Determination and Treatment Decision

Subject to (Potentially):

- Legally Mandated Retention
- Required Reporting of Results

* All figures and charts are original works by GENIVI Security Team

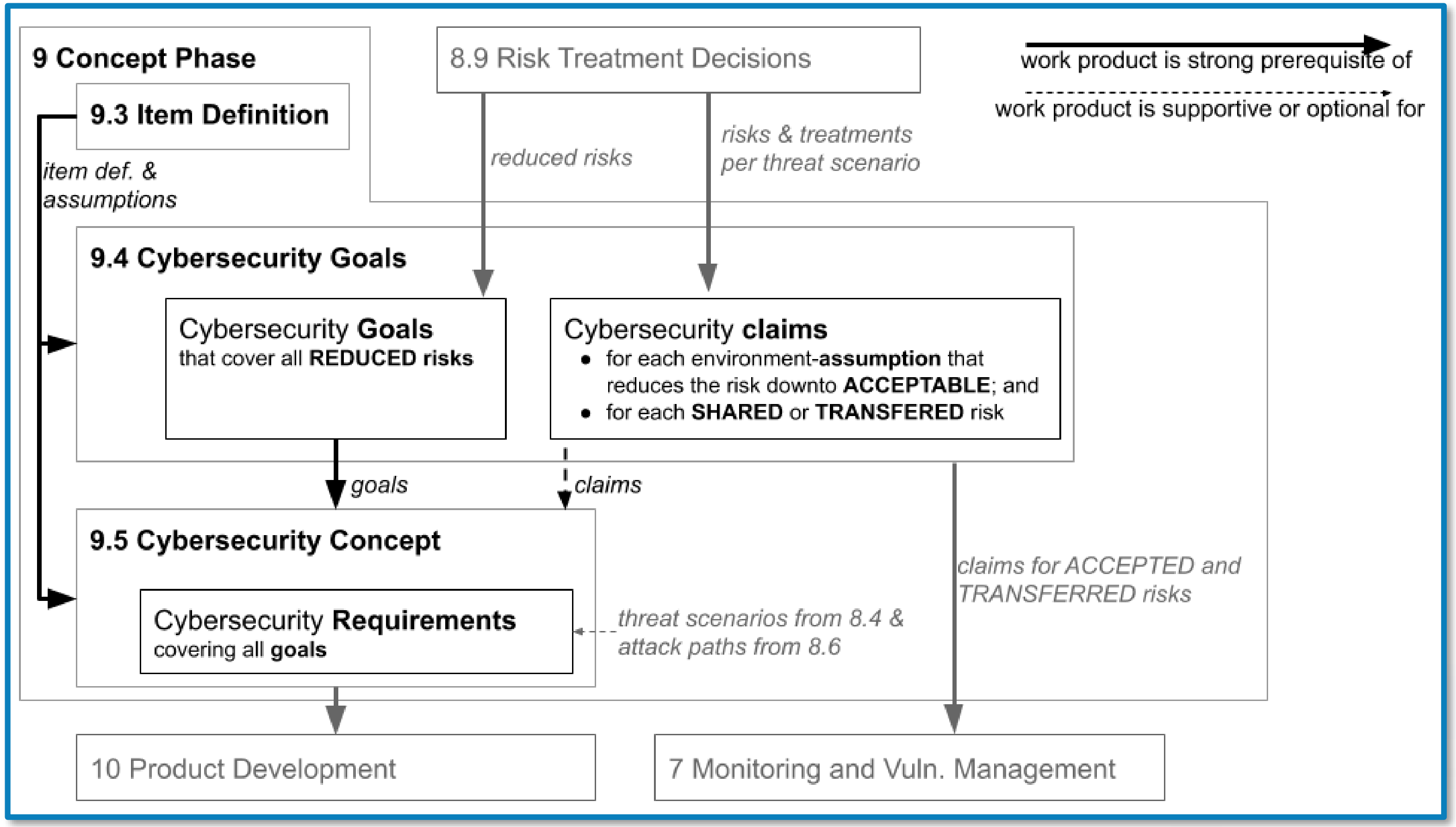
Concept Phase

Key Takeaways: Clause 9

- Consistency is the Underlying Theme
  - Against the Cybersecurity Goals of the Concept
  - Completeness of Controls Towards Item Goals
  - Compatibility to Item

- Cybersecurity Goals (For The Product) Should be Clearly Identified
  - Threat Scenario(s)
  - Impact Rating(s)
  - Attack Path Analysis
  - Attack Feasibility
  - Risk Determination

Clause 9 Process Flow


9 Concept Phase
9.3 Item Definition
item def. & assumptions
8.9 Risk Treatment Decisions
reduced risks
risks & treatments per threat scenario
work product is strong prerequisite of
work product is supportive or optional for
9.4 Cybersecurity Goals
Cybersecurity Goals that cover all REDUCED risks
Cybersecurity claims
• for each environment-assumption that reduces the risk downto ACCEPTABLE; and
• for each SHARED or TRANSFERED risk
goals
claims
9.5 Cybersecurity Concept
Cybersecurity Requirements covering all goals
threat scenarios from 8.4 & attack paths from 8.6
claims for ACCEPTED and TRANSFERRED risks
10 Product Development
7 Monitoring and Vuln. Management

Item = Product or Feature

All Claims MUST be Verified

Risk Transference Requires Claim for Goal(s)

Subject to (Potentially):

- Verification Against Requirements
- Required Reporting of Results

* All figures and charts are original works by GENIVI Security Team

Product Development and Verification (Multi-Phased)

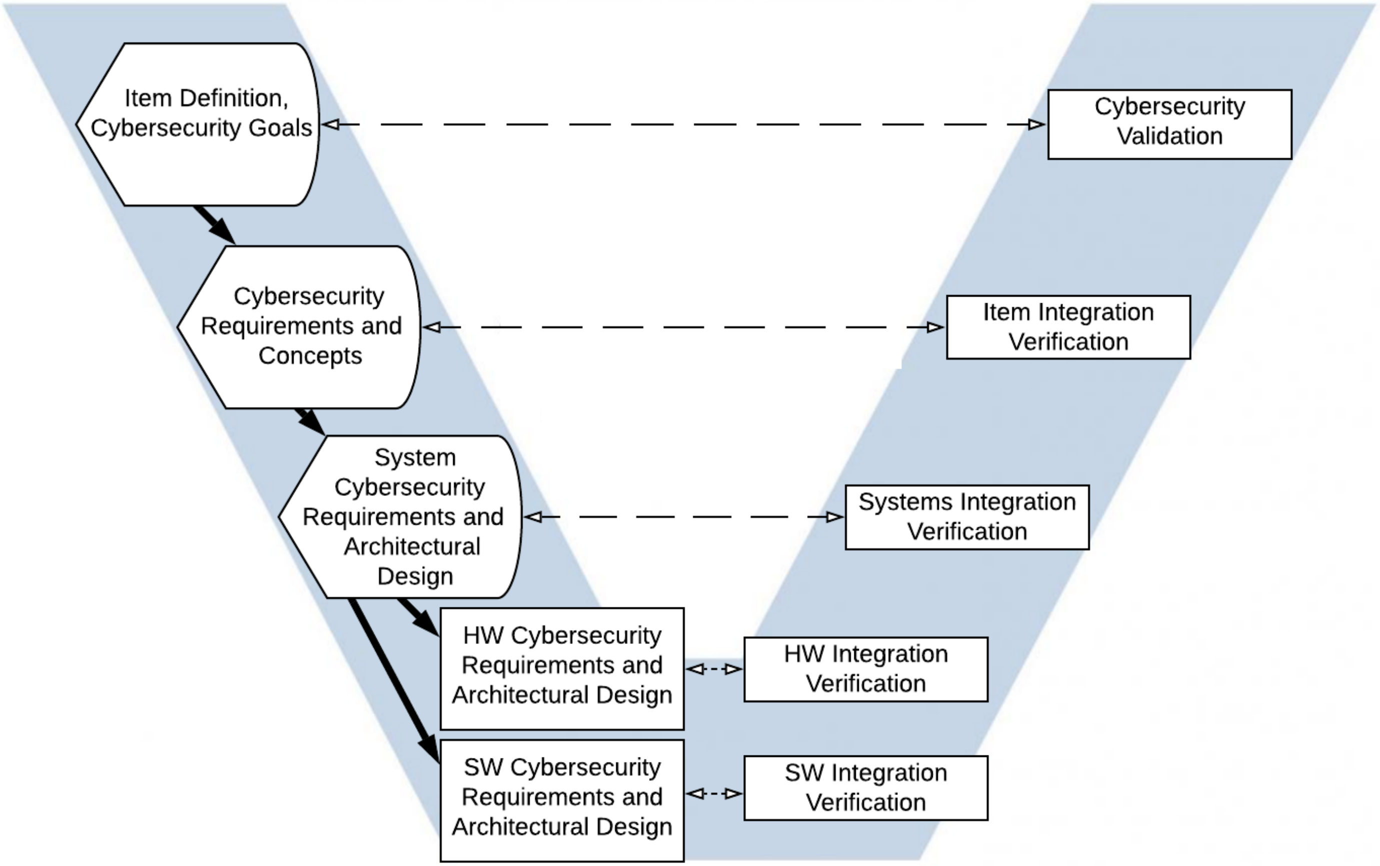
Key Takeaways: Clause 10

- Apply 21434 Ideas To Systems Engineering (V) Model
  - Align Requirements to Cybersecurity Goals of the Concept
  - Allows for Multi-Phase Requirements
  - Refined Design…
- Cybersecurity Requirements and Refined Architectures
  - Defined through Higher Level Goals
  - Refined Architecture Should be Based on Initial Design
  - Post-Development Phases Should Be Included in Requirements
- Verification Activities of All Requirements
  - Against Refined Architecture
  - Against Refined Cybersecurity Requirements
    - Should Include All Phases of Development

Key Takeaways: Clause 11

- Requires Validation of ALL Cybersecurity Claims
  - For Items and Goals (Product vs Organization)
  - Items’ Cybersecurity Requirements Aimed at Cybersecurity Goals
  - Cybersecurity Requirements of the Operational Environment
- Validation Should Confirm:
  - Adequacy of Goals
  - Completeness, Correctness, and Consistency of all Cyber Requirements
  - Any Unintended Operation of Item Against Requirements and Goals
    - Additional Vulnerabilities Uncovered Should be Managed Per Clause (7)
  - Risk Treatment to An Acceptable Level

Clause 10/11 Engineering Flows


Item Definition, Cybersecurity Goals
Cybersecurity Validation
Cybersecurity Requirements and Concepts
Item Integration Verification
System Cybersecurity Requirements and Architectural Design
Systems Integration Verification
HW Cybersecurity Requirements and Architectural Design
HW Integration Verification
SW Cybersecurity Requirements and Architectural Design
SW Integration Verification

Defines Against Known Development Structure

Creates Robust Verification and Validation Plan

Defines Requirements for All Phases of Development

Subject to (Potentially):

- Change Requests
- New Threats/Vulns Updating Verifications
- Required Reporting of Results

* All figures and charts are original works by GENIVI Security Team

Production, Operations and Maintenance, Decommissioning

Key Takeaways: Clauses 12,13,14

- Applies All CS Requirements for Post-Development
  - Goal to Not Introduce Vulnerabilities During Production
  - Production Control Plan for Cybersecurity Requirements
- Handle Incident Response Plans:
  - Remediation Actions
  - Communication Plans
  - Assigned Responsibilities
  - Procedures to Communicate End of Support (Feature or Product)
- Decommissioning:
  - Must Consider All Cybersecurity Plans When Decommissioning Product
    - Must Comply With Clauses 9 and 10

Distributed Cybersecurity Activities

GENIVI®

Key Takeaways: Clause 15

- Applies Plan To Commercial Agreements Between Customer and Suppliers
  - **C**ybersecurity **I**nterface **A**greement for **D**evelopment (CIAD)
    - Document That Defines Interactions, Dependencies, and Responsibilities Between Customer (C) and Supplier (S)
- Quotes Must Adhere to CIAD:
  - Supplier needs:
    - Formal Request to Comply
    - Expectation of Cybersecurity Responsibilities
    - Relevant Cybersecurity Goals or Requirements for the Product or Feature Quoted
- Non-Compliance Requires Notification to Other Party With Resolution Agreement and Action Plan if Applicable

Thank you!

Visit GENIVI:

http://www.genivi.org

http://projects.genivi.org

Contact us:

help@genivi.org