National Security Agency
Cybersecurity Technical Report

Zero Trust Implementation Guideline Primer

January 2026

U/OO/102936-26
PP-25-3613
Version 1.0

Notices and Contact Information

Document change history

Date	Version	Description
January 2026	1.0	Initial publication

Disclaimer of Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats, and to develop and issue cybersecurity specifications and mitigations for National Security Systems, Department of War information systems, and the Defense Industrial Base. This information may be shared broadly to reach all appropriate stakeholders.

Acknowledgements

The National Security Agency (NSA) acknowledges the valuable contribution and support of the Department of War (DoW) Chief Information Officer's Zero Trust (ZT) Portfolio Management Office (PfMO) on this endeavor.

Author(s)

National Security Agency (NSA)
Cybersecurity Directorate

Contact Information

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov
Department of War (DoW) Chief Information Office (CIO) Zero Trust (ZT) Portfolio Management Office (PfMO): osd.zt-pfmo@mail.mil

Executive Summary

Zero Trust (ZT) represents a fundamental enhancement in cybersecurity. Rather than relying on perimeter defenses, ZT emphasizes continuous authentication and authorization of every User/Person Entity (PE), device/Non-Person Entity (NPE), and application, operating under the principles of "never trust, always verify" and "assume breach." This approach is critical for safeguarding sensitive data, systems, and services against increasingly sophisticated cyber threats.

As mandated by Executive Order (EO) 14028, the United States Government (USG) developed several ZT strategies, to achieve ZT. These strategies include frameworks, guidelines, and maturity models designed to assist organizations in implementing ZT. Key foundational documents outlining architecture, maturity models, and guidance supporting this effort include:

- National Institute of Standards and Technology (NIST), Zero Trust Architecture Special Publication (SP) 800-207, August 2020
- The Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model, Version 2.0, January 2022
- The Department of War[1] (DoW) Zero Trust Reference Architecture (ZT RA), Version 2.0, July 2022
- The DoW Zero Trust Strategy, Version 1.0, October 2022

The National Security Agency (NSA), using its Cybersecurity authorities and role as National Manager (NM) for U.S. National Security Systems (NSS), developed the Zero Trust Implementation Guidelines (ZIGs), leveraging NIST and DoW published guidance. The ZIGs are intended to assist the DoW, Defense Industrial Base (DIB), NSS, and affiliated organizations with incorporating ZT principles into their processes, enabling them to achieve Target-level ZT, as described in the DoW ZT Framework from the DoW ZT Strategy.

In close partnership with the DoW CIO, and in an effort to organize the 152 ZT Activities contained within the DoW ZT Strategy, five phases were developed (Discovery, Phase One, and Phase Two, which are Target-level, and Phase Three and Phase Four, which are Advanced-level). These phases are not doctrinal but are a structured approach to organize the ZT Activities. ZT is a framework; therefore in keeping with that model, the

[1] Per EO 14347, the Department of War (DoW) is an authorized secondary title for the Department of Defense (DoD).

phases outlined in the ZIGs are modular and can be aligned to an organization's specific environment.

The current set of ZIGs consist of a Primer and three ZT Implementation Guidelines (Discovery, Phase One, and Phase Two) designed to assist skilled practitioners in adopting and integrating ZT Target-level Capabilities (42) and Target-level Activities (91). ZIGs for Phase Three and Phase Four may be developed at a later time. These guidelines provide a modular structure adhering to the DoW ZT Framework's Pillars, Capabilities, and Activities, as well as NIST SP 800-207, as guidance for implementation. The ZIGs phased implementation approach is as follows:

- Discovery Phase ZIG covers 14 Activities that support 13 Capabilities. The purpose of the Activities within the Discovery Phase ZIG is to collect information about the Component environment(s), such as Data, Applications, Assets, and Services (DAAS), Users/PEs/Non-Person Entities (NPEs), etc.
- Phase One ZIG covers 36 Activities that support 30 Capabilities. Phase One Activities build upon or further refine the Component environment(s) to establish a secure foundation that supports ZT Capabilities.
- Phase Two ZIG covers 41 Activities that support 34 Capabilities. Phase Two Activities mark the beginning of integrating distinct ZT fundamental solutions within the Component environment.

Phase Three and Phase Four ZIGs cover the Advanced-level and may be developed at a later date.

Figure 1: Zero Trust Implementation Guidelines (ZIGs)

Contents

Figures

Tables

Background

EO 14028, *Improving the Nation's Cybersecurity,* mandates USG agencies to adopt a Zero Trust Architecture (ZTA). Specifically, for NSS networks, National Security Memorandum 8 (NSM-8), *Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems,* implements those cybersecurity requirements mandated by EO 14028. NSM-8 focuses on requirements for NSS as they are defined in 44 U.S.C. § 3552(b)(6), as well as all other DoW and Intelligence Community systems, as described in 44 U.S.C § 3553(e)(2) and 3553(e)(3). These directives aim to modernize the nation's cybersecurity posture in response to evolving threats by strengthening digital infrastructure, addressing critical vulnerabilities, bolstering cybersecurity practices, and fostering collaboration between the public and private sectors.

A ZT mindset assumes that all environment traffic, users, devices, and infrastructure may be compromised, necessitating a rigorous authentication and authorization process for all access requests. Implementing these measures enhances the security posture of federal networks by rigorously validating every access request, which prevents unauthorized changes, reduces risk of malicious code insertion, and ensures the integrity of software and supply chains, ultimately strengthening the overall cybersecurity of the United States.

Adopt a Zero Trust Mindset

Adopting a ZT mindset involves fundamentally reassessing and rethinking how cybersecurity is approached within an organization. It augments traditional perimeter-based security models, creating a more dynamic approach that assumes no entity can be trusted by default, regardless of its location, inside or outside the environment.

To effectively address the modern dynamic threat environment, organizations should:

- Implement coordinated and comprehensive system monitoring, management, and defensive operations for continuous protection.
- Continuously verify and validate all resource requests and environment traffic.
- Continuously verify and validate the security posture of all devices and infrastructure.
- Prepare for rapid response and recovery, acknowledging the inherent risk incurred in all access approvals and authorizations to critical resources.

The guiding principles of ZT, outlined in NIST SP 800-207, are the core of a ZTA:

- **Never trust, always verify** – Treat every User/PE/NPE, device, application/workload, and data flow as untrusted. Dynamically authenticate and explicitly approve all activity, adhering to the principle of Least Privilege.
- **Assume breach** – Operate and defend resources under the assumption that an adversary already has presence within the environment. Plan for deny-by-default and heavily scrutinize all users, devices, data flows, and requests. Continuously log, inspect, and monitor all configuration changes, resource accesses, and environment traffic for suspicious activity.
- **Verify explicitly** – Securely and consistently verify access to all resources, using multiple attributes (dynamic and static), to derive confidence levels for contextual access decisions.

Zero Trust Design Concepts

The following are key concepts to address when designing a ZTA:

- **Define mission outcomes** – Derive the ZTA from organization-specific mission requirements that identify the critical DAAS.
- **Architect from the inside out** – First, focus on protecting critical DAAS. Second, secure all paths to access DAAS.
- **Determine who/what needs access to the DAAS to create Access Control policies** – Create security policies and apply them consistently across all environments (e.g., Local Area Network (LAN), Wide Area Network (WAN), endpoint, perimeter, mobile, etc.).
- **Inspect and log all traffic before acting** – Establish comprehensive, complete visibility of all activities across all layers, from endpoints to the environment, to enable analytics that can detect, trace, and make sense of suspicious activity.

ZT is more than an Information Technology (IT) solution; it is a holistic cybersecurity approach. While ZT may leverage technologies or specific products, it is not a singular capability or device. Adopting ZT is a journey that requires integrating capabilities, technologies, solutions, processes, and enablers. This journey necessitates the involvement of stakeholders to ensure alignment and buy-in, a prioritization scheme to focus resources effectively, and a continuous feedback loop for ongoing improvement and adaptation. In support of this holistic cybersecurity approach, the DoW ZT Strategy

outlines four (4) high-level strategic goals for achieving ZT applicable to any Component or Enterprise [1][1]. The goals are:

- ZT cultural adoption
- Secured and defended information systems
- Technology acceleration
- ZT enablement

These goals encompass supporting functions that drive the successful implementation of ZT and address the enablers and governance to support a successful ZTA. The supporting functions included in the DoW ZT Strategy are discussed throughout the ZIGs, with the exception of policy and training, which are outside the scope of the ZIGs and only discussed briefly here.

- **Policy**: Policies are necessary to ensure the DoW ZT Framework is uniformly applied and fully interoperable across the Enterprise. Enterprise-level processes, policies, and resources may need to be developed, redefined, and synchronized across the applicable Components with ZT principles and approaches.
- **Training**: An Enterprise-wide ZT mindset is essential. It guides the design, development, integration, and deployment of IT across the Enterprise and requires a culture where all personnel are aware of, understand, commit to, and are trained to embrace ZT.A training model should be developed that analyzes the skills needed by the Enterprise to accomplish the mission and/or business needs. Adequate training is fundamental to the ZT process and should address various training needs, including:
    - Awareness Training – Incorporate ZT concepts into ongoing security and privacy literacy training. This training should cover core ZT principles, benefits, and practical implications for daily work.
    - Role-Based Training – Identify the specific roles requiring ZT role-based training. This training, tailored for the assigned duties, may be technical or managerial.
    - Developer Provided Training – Require any system developers, system components, or system services within the environment to provide training on the proper use and operation of the implemented security functions or mechanisms to ensure ZT principles are maintained during operational use.

Primer and ZIG Purpose

The purpose of this Primer document is to provide an overview and linkage to the overarching guidance provided by the DoW, CISA, and NIST for achieving a ZTA at the Target-level. The Primer provides direction and guidance for using the ZIGs, which outline the steps to implement the technologies and processes that will enable the Target-level ZT Capabilities, Activities, and Expected Outcomes defined by the DoW ZT Framework. Finally, the Primer describes the methodology used to break down the ZT Activities further so that system owners and practitioners have a deep understanding of how to best utilize the ZIGs.

The Primer is a companion to the ZIGs, which map to the DoW-defined Target-level ZT Implementation. Figure 2 depicts the DoW ZT Framework alignment to the ZIGs by ZT Phase (Discovery, Phase One, Phase Two, Phase Three, Phase Four), Level (Target, Advanced), and the associated Capabilities and Activities included in each document.

The purpose of the Activities within the Discovery Phase ZIG is to collect information about the organization's environment(s), such as DAAS, Users/PEs/NPEs, etc. Phase One Activities build upon or further refine the Component environment(s) to establish a secure foundation that supports ZT Capabilities. Phase Two Activities mark the beginning of integrating distinct ZT fundamental solutions within the Component environment.

ZIGs addressing the Advanced Levels, Phase Three and Phase Four, may be developed at a later date.

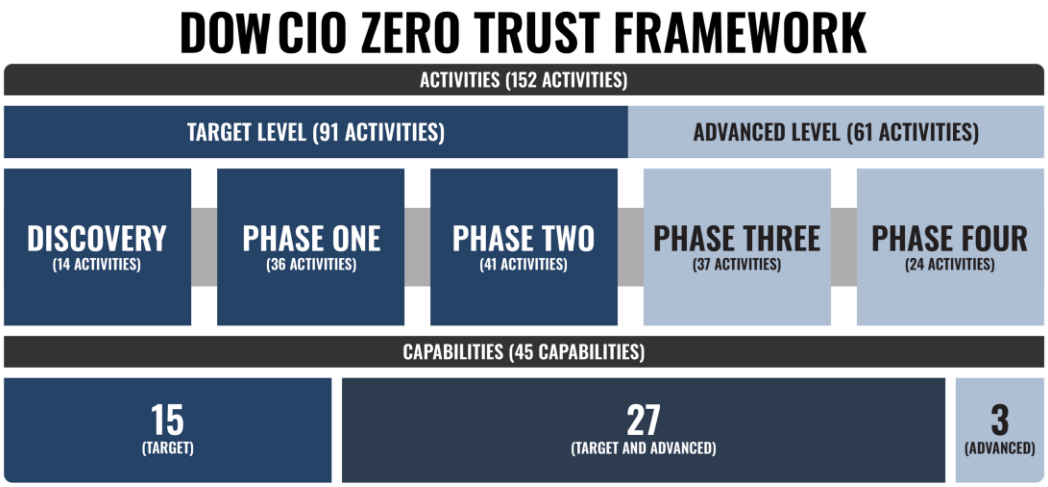

Figure 2: ZIG Alignment to the DoW ZT Framework

Target Audience

The ZIGs are designed to be used by skilled practitioners, individuals, stakeholders, and teams responsible for implementing ZT technical and strategic aspects. They may be used within the DoW, DIB, NSS, industry, academia, and affiliated organizations. The target audience includes the following:

- **Technical Implementers/Skilled Practitioners** – Practitioners managing the technical implementation of ZT enabling technologies and configurations.
- **Enterprise Environment Owners** – Stakeholders responsible for maintaining and securing large-scale IT infrastructures.
- **Cybersecurity Leaders** – Professionals tasked with designing, overseeing, and optimizing cybersecurity measures.
- **External Partners and Vendors** – Collaborators providing technologies, services, and/or expertise to support ZT efforts.

Scope

The Primer and associated ZIGs are designed to guide and support organizations within various environments by providing practical, actionable recommendations to facilitate ZT implementation. These guidelines:

- Explain the historical background and mandates that guide the development of a ZTA.
- Provide direction and guidance for using the associated ZIGs.
- Describe the methodology used to define the relevant Activities and implementation processes within the ZIGs.

In alignment with the current DoW ZT Framework, the ZIGs are most applicable in an IT Enterprise. Future updates may address other contextual environments, including Operational Technology (OT), Defense Critical Infrastructure (DCI), and/or Tactical/Weapons Systems. The ZIGs will continue to be modified as capabilities and technologies advance.

The Primer and associated ZIGs are **not**:

- Prescriptive or mandatory. Organizations should identify their starting points and tailor the capabilities and Activities to their specific needs.
- A one-size-fits-all or step-by-step sequential guide to implementing ZT.
- Vendor-specific. Technologies listed in the Capabilities sections are included for consideration, may not contain all possible technologies, and are vendor agnostic.
- Designed to supersede, impact, or alter any existing authority, law, or policy.

Assumptions

The following assumptions drive the Primer and associated ZIGs:

- The ZIGs are not designed or intended to have a fixed implementation start or end point. Organizations have the flexibility to choose their starting point and tailor the guidance to their specific environment.
- Activities can be implemented concurrently.
- Readers have a foundational understanding of cybersecurity architectures, principles, and their organization's Critical Infrastructure and Key Resources (CIKR).
- Readers possess technical expertise in areas such as Identity and Access Management (IAM), endpoint security, network security, and security analytics.
- Implementing organizations are familiar with ZT, their architecture, and the DoW ZT Framework.
- Personnel have the necessary skills and training to implement Software-Defined Networking (SDN), Development, Security, and Operations (DevSecOps) practices, Artificial Intelligence (AI)/Machine Learning (ML) solutions, data protection capabilities, and security orchestration, including Automation and Orchestration (A&O) and Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipelines. This includes the ability to leverage cloud-based solutions (e.g., Platform as a Service (PaaS)/Software as a Service (SaaS)/Infrastructure as a Service (IaaS)/Anything as a Service (XaaS), etc.) for ZT implementations.
- Future ZIGs will address the ZT Advanced-level and subsequent Phases (Phases Three and Four).

Further Information (Authoritative References)

To fully utilize the ZIGs, practitioners should be familiar with the following authoritative references:

- NIST SP 800-207 Zero Trust Architecture, August 2020
- NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations, September 2020
- NSA/CSS CSI: Embracing a Zero Trust Security Model, Version 1.0, February 2021

- The Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model, Version 2.0, January 2022
- The Department of War Zero Trust Reference Architecture (DoW ZT RA), Version 2.0, July 2022
- The Department of Defense Zero Trust Strategy, Version 1.0, October 2022
- NSA/CSS CSI: Advancing Zero Trust Maturity Throughout the User Pillar, Version 1.1, April 2023
- NSA/CSS CSI: Advancing Zero Trust Maturity Throughout the Device Pillar version 1.0, October 2023
- NSA/CSS CSI: Advancing Zero Trust Maturity Throughout the Network and Environment Pillar, Version 1.0, March 2024
- NSA/CSS CSI: Advancing Zero Trust Maturity Throughout the Data Pillar, Version 1.0, April 2024
- NSA/CSS CSI: Advancing Zero Trust Maturity Throughout the Visibility and Analytics Pillar, Version 1.0, May 2024
- NSA/CSS CSI: Advancing Zero Trust Maturity Throughout the Application and Workload Pillar, Version 1.0, May 2024
- NSA/CSS CSI: Advancing Zero Trust Maturity Throughout the Automation and Orchestration Pillar, Version 1.0, July 2024

As these references are updated or rescinded, the implementation should be reevaluated and revised to comply with the latest laws, policies, and industry best practices.

ZIG Design Methodology

The ZIGs refine the guidance that the DoW ZT Framework provides for ZTA implementation. They closely follow the DoW ZT Framework's structure beginning at the Pillar level within each Phase. The DoW ZT Framework defined Capabilities and associated Activities are further broken down into the implementation process for each Activity.

The ZIG methodology focuses on the framework's Activity Level as the lowest-level element, guiding skilled practitioners in building and tailoring their implementation approach. Each Activity is structured into discrete tasks that are further decomposed into recommended processes and actions to meet the Activity's intent.

The DoW ZT Framework uses Pillars and Capabilities to define the “What” and “Why” of implementing a ZTA. The Activities describe the “Why” and the “How” to achieve these goals.

The ZIGs are intentionally designed with some duplication to ensure that each Capability and Activity can function as a standalone reference. Acronyms are consistently spelled out across sections to promote clarity and modularity. Activity names are italicized throughout the document to enhance visibility and ease of identification.

ZIG Structure

The ZIGs are structured as follows:

Pillars

This section introduces each Pillar pertaining to each Phase of the DoW ZT Framework. The ZT Pillars provide a framework for securing modern IT systems by emphasizing continuous verification, validation, strict access controls, and data protection. Figure 3 shows a graphical description of the DoW ZT Pillars.

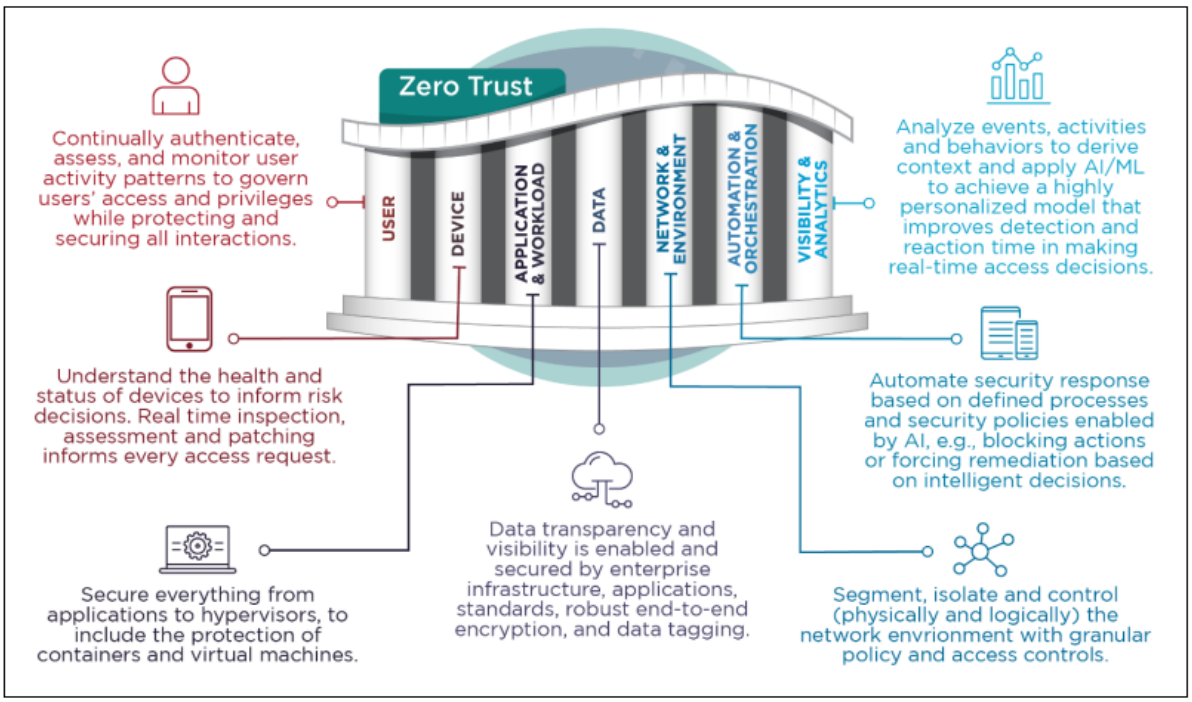

Figure 3: Description of the DoW Zero Trust Pillars

For additional information, see the DoW ZT Framework documents published on the DoW CIO Library, including the Zero Trust Capabilities and Activities, the DoW Zero Trust Strategy, NSA Zero Trust Cybersecurity Information Sheets (CSIs), and the ZT RA [1-11].

Capabilities

This section introduces each Capability associated with each Phase of the DoW ZT Framework. The Capability section precedes the associated Activities and describes each ZT Capability defined by the DoW. It begins with a table similar to Figure 4, which maps to the applicable Pillar and the Capability descriptions. The Pillar and the Capability descriptions shown in Figure 4 are taken from DoW CIO guidance, specifically, the DoW Zero Trust Execution Road Map v 1.1 Data Tables [12]. They are included verbatim, without any changes.

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
1 - User	1.1 - User Inventory
Description	
Regular and Privileged users are identified and integrated into an inventory supporting regular modifications. Applications, software and services that have local users are all part of the inventory and highlighted.	
Impact to ZT	
Users not on the authorized user list will be denied access by policy.	

Figure 4: Sample Capability Table

Following the Capability table are the Scenario, Positive Impacts, and Technology subsections, which relate to the Capability. The Scenario subsection illustrates practical applications, highlighting how the technologies underpinning each Capability can address specific challenges or opportunities. These scenarios are not comprehensive, nor do they serve to assess a system's ZT implementation. They provide examples of practical applications and considerations, helping stakeholders understand the value and impact of adopting a Capability. This approach supports informed decision-making and aligns the Capability with organizational objectives.

The Positive Impacts subsection provides examples of potential benefits an organization may derive from implementing the Capability.

The Technology subsection includes a representative list of technologies that enable the Capability and is not an all-inclusive list of technologies that an organization could consider.

For additional information, see the DoW ZT Framework documents published on the DoW CIO Library, including the Zero Trust Capabilities and Activities, the DoW Zero Trust Strategy, and the ZT RA [1-3].

Activities

This section introduces the Activities associated with each Phase of the DoW ZT Framework. The Activity section begins with the Activity Table, which contains information sourced from the DoW CIO Library's published updates on ZT Capabilities and Activities, current as of this document's publication date. Figure 5 depicts a sample Activity Table, and Table 1 details the source of information for each of the sections of the table.

The terms "Enterprise" and "Component" are used throughout the Activities.

- Enterprise refers to an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency, or, as appropriate, any of its operational elements, etc.). The Enterprise is responsible for providing policies and guidance to those Components that fall under its purview [13].
- Component refers to the organization implementing ZT.

For additional information, see the DoW ZT Framework documents published on the DoW CIO Library, including the Zero Trust Capabilities and Activities, the DoW Zero Trust Strategy, and the ZT RA [3].

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components utilize Enterprise authoritative source of (PE/NPE) identity (PE - AMID, NIS, AFID) and/or establish or augment with local authoritative source. Identity management can be done manually if needed, preparing for automated approach in later stages. Identity source is connected to identity lifecycle management processes (e.g., joiner/mover/leaver/returner, etc.). IT privileged users are clearly identified.	
Predecessor(s)	**Successor(s)**
None	1.2.2
Expected Outcomes	
• Identified managed non-privileged users. • Identified managed privileged users. • Identified applications using their own user account management for non-administrative and administrative accounts. • Identify the authoritative source of identities.	
End State	
Accurately determine and keep track of users who have both the authorization and authentication to access critical systems or resources. This involves regularly reviewing, communicating, and carefully examining the sources of information that provide the true and up-to-date user data.	

Figure 5: Sample Activity Table

Table 1: Activity Table Source of Information

Element	Source	Comment
ID	DoW CIO Library > Defend Against Cyber Attacks > Zero Trust Capabilities and Activities as of 18 Mar 25	
Description		Includes recommended corrections (grammar, capitalization, hyphens, etc.)
Predecessor(s)		
Successor(s)		
Expected Outcomes	DoW CIO Library > Defend Against Cyber Attacks > Zero Trust Capabilities and Activities as of 18 Mar 25	Includes recommended corrections (grammar, capitalization, hyphens, etc.)
End State		Includes recommended corrections (grammar, capitalization, hyphens, etc.)

Considerations

The Considerations subsection clearly explains the prerequisites, challenges, and lessons learned that may influence the successful implementation of each Activity. It highlights processes and applicable documentation and outlines any limitations or dependencies that may affect the execution of specific Activities. By addressing these considerations, the section aims to equip practitioners and decision-makers with the insights needed to effectively plan and adapt the provided guidance to their unique organizational environments.

Implementation

The Implementation subsection provides an actionable roadmap that guides practitioners through the practical execution of each task, ensuring alignment with the overall ZT objectives and facilitating measurable progress toward implementation.

The Implementation subsection defines high-level Tasks and process steps derived from the Activity Description, Expected Outcomes, and End State outlined in the DoW ZT Framework.

Summary

The Summary subsection provides a high-level overview of key considerations and Expected Outcomes for successfully implementing each activity, which are presented in a workflow diagram.

- **Readiness Assessment** – Highlights critical ZT readiness questions to consider before implementing the ZT activity, focusing on organizational readiness.
- **Strategic Insights** – A high-level overview that outlines the intended results and benefits expected after implementing the Activity.
- **Expected Outcomes** – The Expected Outcomes are defined in the DoW ZT Framework. To achieve the Expected Outcomes, organizations should align their execution plans with the DoW ZT Strategy.

Conclusion

ZT operates on the fundamental principle of “never trust, always verify” and that no entity, internal or external, is trusted by default. All data, system, or resource requests must be authenticated and approved based on policy. This modernized cybersecurity framework enhances the ability of environment defenders to secure sensitive data, applications, assets, and services. Continuous monitoring, verification, and validation ensure that cybersecurity measures remain effective and up-to-date, enabling the detection and response to threats that exploit vulnerabilities or gaps in the Enterprise architecture.

The Primer and associated ZIGs were developed to assist skilled practitioners, stakeholders, individuals, and teams responsible for the technical and strategic aspects of ZT implementation across various organizations, including within the DoW, DIB, NSS, and affiliated communities. While they are not a one-size-fits-all approach, the ZIGs provide the tools and guidance to assist in refining ZT implementation plans at the organization’s discretion. As the threat landscape continues to grow and change, these guidelines will be updated to reflect the latest best practices and advancements to achieve a ZT security posture.

Appendix A: Terms and Definitions

Terms and definitions used within all the Zero Trust Implementation Guidelines.

API Standardization
The ability to reach agreement and publish locally, the application programming interface for a commonly used service. Enforcement of compliance in the use of commonly agreed API's.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Access Control
The process of granting or denying specific requests to 1) obtain and use information and related information processing services and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).
Source: NIST Computer Security Resource Center (CSRC) Glossary

Access Control List
A mechanism that implements access control for a system resource by enumerating the identities of the system entities that are permitted to access the resources.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Access Management
Access Management is how an agency authenticates enterprise identities and authorizes appropriate access to protected services.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Active Directory
A Microsoft directory service for the management of identities in Windows domain networks.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Advanced Persistent Threat
An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives which are typically to establish and extend its presence within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Alerts
Data that indicates some trigger or threshold passing event has occurred and which is transmitted from the managed device/service to the managing service. A notification that a specific attack has been detected or directed at an organization's information systems.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Analytics
Information resulting from the systematic analysis of data or statistics. This analysis includes discovering, interpreting, and communicating significant patterns in data.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Application Programming Interface
A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Artificial Intelligence
The capability of computer processes to perform functions that are normally associated with human intelligence such as reasoning, learning and self-improvement.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Attribute-Based Access Control
An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Audit and Accountability
Entails that organizations (i) create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity; and (ii) ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable.
Source: NIST SP 800-12 Revision 1- An Introduction to Information Security

Authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Automation
Ability to create and apply application technology to monitor and control the production and delivery of otherwise manual services.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Availability
Ensuring timely and reliable access to and use of information.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Behavior
Aggregate data from logs and reports that provides packet, flow, file, and other types of information, as well as certain kinds of threat data to figure out whether certain kinds of activity and behavior are likely to constitute a cyberattack.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Big Data
The ability to enable enhanced insight, decision making, and process automation by consuming high-volume, high-velocity and/or high-variety information assets.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Biometrics
A biometric is a measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics. (FIPS 201)
Source: DoD Zero Trust Reference Architecture, Version 2.0

Bring Your Own Device
A non-organization-controlled telework client device.
Source: NIST SP.1800-22 Mobile Device Security: Bring Your Own Device (BYOD)

Business Continuity Plan

The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.
Source: NIST Computer Security Resource Center (CSRC) Glossary

CI/CD Pipeline
A CI/CD pipeline is a component of a broader toolchain that entails continuous integration, version control, automated testing, delivery, and deployment. It automates the integration and delivery of applications and enables organizations to deploy applications quickly and efficiently.
Source: NSA/CISA CSI, Defending Continuous Integration/Continuous Delivery (CI/CD) Environments

Capability
A combination of mutually reinforcing security and privacy controls implemented by technical, physical, and procedural means. Such controls are typically selected to achieve a common information security- or privacy-related purpose.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Certificate Authority
A trusted entity that issues and revokes public key certificates.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Certificate Revocation List
A list of revoked public key certificates created and digitally signed by a certification authority.
Source: Source: NIST Computer Security Resource Center (CSRC) Glossary

Certificate
A set of data that uniquely identifies a public key (which has a corresponding private key) and an owner that is authorized to use the key pair. The certificate contains the owner's public key and possibly other information and is digitally signed by a Certification Authority (i.e., a trusted party), thereby binding the public key to the owner.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Challenge
Additional or secondary question and response from a user to confirm identity or further authenticate.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Chief Information Officer
The senior official that provides advice and other assistance to the head of the agency and other senior management personnel of the agency to ensure that IT is acquired and information resources are managed for the agency in a manner that achieves the agency's strategic goals and information resources management goals; and is responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, the information policies and information resources management responsibilities, including the reduction of information collection burdens on the public.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Cloud Access Security Brokers
A software tool that manages access to secure data with record keeping capabilities that use updated encryption keys and log records to regulate access.
Source: Cybersecurity and Infrastructure Security Agency, United States Digital Service, and Federal Risk and Authorization Management Program, Cloud Security Technical Reference Architecture, Version 2.0

Cloud Security Posture Management
A continuous process of monitoring a cloud environment; identifying, alerting on, and mitigating cloud vulnerabilities; and improving cloud security.
Source: Cybersecurity and Infrastructure Security Agency, United States Digital Service, and Federal Risk and Authorization Management Program, Cloud Security Technical Reference Architecture, Version 2.0

Cloud Service Provider
An external company that provides a platform, infrastructure, applications, and/or storage services for its clients.
Source: Cybersecurity and Infrastructure Security Agency, United States Digital Service, and Federal Risk and Authorization Management Program, Cloud Security Technical Reference Architecture, Version 2.0

Code
Computer instructions and data definitions expressed in a programming language or in a form output by an assembler, compiler, or other translator.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Commercial Off-The-Shelf
Hardware and software IT products that are ready-made and available for purchase by the general public.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Common Access Card
The standard identification for active duty uniformed Service personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel. It is also the principal card used to enable physical access to buildings and controlled spaces, and it provides access to DoD computer network and systems.
Source: DoD Common Access Card

Common Vulnerabilities and Exposures
A list of entries--each containing an identification number, a description, and at least one public reference--for publicly known cybersecurity vulnerabilities.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Communities of Interest
A collaborative group of users (working at the appropriate security level or levels) who exchange information in pursuit of their shared goals, interests, missions, or business processes, and must have a shared vocabulary for the information exchanged. The group exchanges information within and between systems.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Comply-to-Connect
Comply-to-Connect (C2C) is the identification, protection, and detection of DoDIN connected devices to ensure a continuous secure configuration. C2C enables the conduct of Defensive Cyber Operations in response to detected and prevailing threats by providing critical enabling information for the development of a Common Operating Picture. C2C standards are based on a framework of managing access to the network and its information resources by restricting or limiting access to those devices that do not comply with the standards.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Component
The organization implementing ZT.
Source: ZIG Primer

Concept of Operations
Verbal and graphic statement, in broad outline, of an organization’s assumptions or intent in regard to an operation or series of operations of new, modified, or existing organizational systems.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Confidentiality
Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Configuration
The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Configuration Management
A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Container
A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Continuous
Occur periodically without interruption during the ordinary performance of services.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Continuous Authentication
The ability validate network users are the ones who they claim to be throughout an entire session at every step.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Continuous Integration/Continuous Delivery
Continuous Integration/Continuous Delivery (CI/CD) is a development process for quickly building and testing code changes that helps organizations maintain a consistent code base for their applications while dynamically integrating code changes. CI/CD is a key part of the development, security, and operations (DevSecOps) approach that integrates security and automation throughout the development lifecycle.
Source: NSA/CISA CSI, Defending Continuous Integration/Continuous Delivery (CI/CD) Environments

Continuous Monitoring
The ability to determine if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Control Plane
In a Zero Trust environment, there should be a separation (logical or possibly physical) of the communication flows used to control and configure the network and application/service communication flows used to perform the actual work of the organization. This is often broken down to a control plane for network control communication and a data plane for application/service communication flows. The control plane is used by various infrastructure components (both enterprise-owned and from service providers) to maintain and configure assets; judge, grant, or deny access to resources; and perform any necessary operations to set up communication paths between resources. The data plane is used for actual communication between software components.
Source: NIST SP 800-207 Zero Trust Architecture

Controlled Unclassified Information
Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Countermeasures
Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of a system. Synonymous with security controls and safeguards.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Credential
An object or data structure that authoritatively binds an identity, via an identifier or identifiers, and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Credential Management
To manage the life cycle of entity credentials used for authentication.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Cyber Survivability Endorsement
The Joint Staff developed the Cyber Survivability Endorsement (CSE) criteria to ensure joint warfighting systems' requirements are articulated sufficiently, to prevent, mitigate and recover from cyber events by applying a risk-managed approach to countering a capable and determined adversary.
Source: Defense Acquisition University (DAU) Cyber Survivability Endorsement Implementation Guide, Version 2.0

Cyber Threat Intelligence
Cyber threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Cybersecurity Service Provider (CSSP)
A CSSP is an organization that provides one or more cybersecurity services to implement and protect the Department of Defense Information Network (DODIN).
Source: United States Cybersecurity Magazine

Data Catalog
Data Catalog contains descriptions and meta data about the data without itself holding that data.
Source: DoD Zero Reference Architecture, Version 2.0

Data Governance
Set of processes that ensures that data assets are formally managed throughout the enterprise. A data governance model establishes authority, management and decision-making parameters related to the data produced or managed by the enterprise.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Data Lake
A data lake is a centralized repository that allows you to store all your structured and unstructured data at any scale. You can store your data as-is, without having to first structure the data, and run different types of analytics—from dashboards and visualizations to big data processing, real-time analytics, and machine learning to guide better decisions.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Data Loss Prevention
A system's ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g., data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of NSS information.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Data Plane
The data plane is used for communication between software components. This communication channel may not be possible before the path has been established via the control plane. For example, the control plane could be used by the PA and PEP to set up the communication path between the subject and the enterprise resource. The application/service workload would then use the data plane path that was established.
Source: NIST SP 800-207 Zero Trust Architecture

Data Rights Management (DRM)
DRM is a set of access control technologies and policies that proactively detect and protect access to data and proprietary hardware and prevent unauthorized modification or redistribution of protected data.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Data Tagging
The ability to associate a data object with characterizing metadata for a defined purpose.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Defense Industrial Base
The U.S. defense industrial base (DIB) is the network of organizations, facilities, and resources that provides the U.S. government—particularly the Department of Defense (DOD)—with defense-related materials, products, and services.

The DIB encompasses a wide variety of entities, including commercial firms operated on a for-profit basis, not-for-profit research centers and university laboratories, and government-owned industrial facilities. It provides everything from large, technologically sophisticated weapon systems and highly specialized operational support to general commercial products and routine services. By supplying and equipping the armed services, the DIB enables the United States to execute national strategy and develop, maintain, and project military power.
Source: Congress.Gov

Development, Security, Operations
A combination of software engineering methodologies, practices, and tools that unifies software development (Dev), security (Sec), and operations (Ops). It emphasizes collaboration across these disciplines, along with automation and continuous monitoring to support the delivery of secure, high-quality software. DevSecOps integrates security tools and practices into the development pipeline, emphasizes the automation of processes, and fosters a culture of shared responsibility for performance, security, and operational integrity throughout the entire software lifecycle, from development to deployment and beyond.
Source: DoD Enterprise DevSecOps Fundamentals, Version 2.5

Device
A combination of components that function together to serve a specific purpose.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Disaster Recovery Plan
A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Dynamic
Occurring in near-real-time under conditions then present.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Dynamic Policy Enforcement
The ability to adapt policy and configurations, and enforce that change, in near real time based on environmental circumstances and indications of user and network behavior.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Enclave
A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Encryption
Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Encryption at Rest
The ability to protect data from a system compromise or data exfiltration by encrypting data while stored.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Encryption in Transit
The ability to protect data if communications are intercepted while data moves between sites or services. This protection is achieved by encrypting the data before transmission; authenticating the endpoints; and decrypting and verifying the data on arrival.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Endpoint
Endpoint is a role given to any devices capable of initiating or terminating a session on a network. Often described as end-user devices, such as mobile devices, laptops, and desktop machine. Hardware servers in data centers, devices such as zero clients, virtualized systems, and infrastructure equipment (i.e., routers, switches, virtual desktop machine) are also considered endpoints.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Endpoint Agent
Client software installed on a network endpoint that communicates or is controlled by a centralized system.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Endpoint Protection Platform
Safeguards implemented through software to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, antispyware, antiadware, personal firewalls, host-based intrusion detection and prevention systems, etc.).
Source: NIST Computer Security Resource Center (CSRC) Glossary

Enterprise
The governing body that an organization falls under or reports to. The Enterprise is responsible for providing policies and guidance to those Components that fall under its purview.
Source: ZIG Primer

Enterprise Identity Provider
A service which provides state/status determination and access to Identity and Credential information. It may also provide baseline user/NPE access roles.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Executive Order
Legally binding orders given by the President, acting as the head of the Executive Branch, to Federal Administrative Agencies. Executive Orders are generally used to direct federal agencies and officials in their execution of congressionally established laws or policies.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Federal Information Processing Standards (FIPS)
A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology to achieve a common level of quality or some level of interoperability.
Source: NIST Computer Security Resource Center (CSRC) Glossary

File Integrity Monitoring
Detecting any suspicious changes to files in a computer system.
Source: MITRE D3FEND

Geolocation
Determining the approximate physical location of an object, such as a cloud computing server.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Health Insurance Portability and Accountability Act
A federal statute that called on the federal Department of Health and Human Services to establish regulatory standards to protect the privacy and security of individually identifiable health information.
Source: NIST Computer Security Resource Center (CSRC) Glossary

High Availability
A failover feature to ensure availability during device or component interruptions.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Identification and Authentication
The process of establishing the identity of an entity interacting with a system.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Identity
The set of physical and behavioral characteristics by which an individual is uniquely recognizable.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Identity and Access Management
Broadly refers to the administration of individual identities within a system, such as a company, a network or even a country. In enterprise IT, identity management is about establishing and managing the roles and access privileges of individual network users.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Identity Federation
A group of organizations that agree to follow the rules of a trust framework.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Identity Governance and Administration
Identity governance and administration system supports automated service provisioning of access certifications, access requests, password & token management following pre-established governance polies.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Identity Lifecycle Management
The evolution of an identity from creation to deactivation.
Source: GSA Identity Lifecycle Management Playbook, Version 1.3

Identity Management
Identity Management is how an agency collects, verifies, and manages attributes to establish and maintain enterprise identities for employees and contractors.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Identity Provider
The party in a federation transaction that creates an assertion for the subscriber and transmits the assertion to the RP.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Identity as a Service
Identity as a Service (IDaaS) is when a company offers identity, credential, and access management (ICAM) services to customers through a software-as-a-service (SaaS) cloud-service model.
Source: NIST IR 8335 (Initial Public Draft) Announcement

Identity, Credential, and Access Management
Programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and non-person entities (NPEs), bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency's resources. See also attribute-based access control (ABAC).
Source: NIST Computer Security Resource Center (CSRC) Glossary

Impact Levels
The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type, expressed as a value of low, moderate, or high.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Incident Response
The remediation or mitigation of violations of security policies and recommended practices.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Indicators of Compromise
Technical artifacts or observables that suggest that an attack is imminent or is currently underway or that a compromise may have already occurred.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Infrastructure as Code
The process of managing and provisioning an organization's IT infrastructure using machine-readable configuration files, rather than employing physical hardware configuration or interactive configuration tools.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Infrastructure as a Service
The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
Source: NIST Computer Security Resource Center (CSRC) Glossary

Integrity
Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Source: NIST Computer Security Resource Center Glossary

Internet Protocol
Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Internet Protocol Security
A protocol that adds security features to the standard IP protocol to provide confidentiality and integrity services.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Internet of Things
The network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Intrusion Prevention System
A system that can detect an intrusive activity and also attempt to stop the activity, ideally before it reaches its targets.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Inventory
A listing of items including identification and location information.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Just-in-Time
Using the current values of all indicators and analytics as input to a policy decision or enforcement.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Key
A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Key Performance Indicators
A metric of progress toward intended results.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Least Privilege
A security principle that a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Lightweight Directory Access Protocol
The Lightweight Directory Access Protocol, or LDAP, is a directory access protocol.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Logs
Digital information that provides a history of events and states of a specific system or device.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Machine Learning
The development and use of computer systems that adapt and learn from data with the goal of improving accuracy.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Macro-Segmentation
Similar in concept to physical network segmentation, macro-segmentation can be achieved through the application of additional hardware or VLANs.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Maintenance
Any act that either prevents the failure or malfunction of equipment or restores its operating capability.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Mandatory Access Control
An access control policy that is uniformly enforced across all subjects and objects within the boundary of an information system. A subject that has been granted access to information is constrained from doing any of the following: (i) passing the information to unauthorized subjects or objects; (ii) granting its privileges to other subjects; (iii) changing one or more security attributes on subjects, objects, the information system, or system components; (iv) choosing the security attributes to be associated with newly-created or modified objects; or (v) changing the rules governing access control. Organization-defined subjects may explicitly be granted organization-defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all of the above constraints.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Master User Record
A unique representation of a user's accounts, personas, attributes, entitlements, and credentials within an organization.
Source: GSA Identity Lifecycle Management Playbook, Version 1.3

Media Access Control
A unique 48-bit value that is assigned to a particular wireless network interface by the manufacturer.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Metadata
Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).
Source: NIST Computer Security Resource Center (CSRC) Glossary

Micro-Segmentation
Micro-segmentation is the practice of dividing (isolating) the network into small logical segments by enabling granular access control, whereby users, applications, workloads and devices are segmented based on logical, not physical, attributes. This also provides an advantage over traditional perimeter security, as the smaller segments present a reduced attack surface (for malicious actors). In a ZT Architecture, security settings can be applied to different types of traffic, creating policies that limit network and application flows between workloads to those that are explicitly permitted.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Microservices
Small, decoupled components that ideally work independently of the other software components.
Source: GAO Agile Assessment Guide

Mobile Device Management
The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers. MDM is usually implemented through a third-party product that has management features for particular vendors of mobile devices.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Multi-Factor Authentication
Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
Source: NIST Computer Security Resource Center (CSRC) Glossary

National Security Systems
Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Network Access Control
A feature provided by some firewalls that allows access based on a user's credentials and the results of health checks performed on the telework client device.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Next-Generation Firewall
Allows integration of other tools to defend the network against malicious activity.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Non-Person Entity
An entity with a digital identity that acts in cyberspace but is not a human actor. This can include organizations, hardware devices, software applications, and information artifacts.
Source: NIST Computer Security Resource Center (CSRC) Glossary

OpenID Connect
OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol. This specification allows developers to authenticate users across websites and applications without having to own and manage password files. This specification can obtain basic profile information about the end-user in an interoperable and Representational State Transfer (REST)-like manner. OpenID Connect allows clients of all types, including web-based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end-users.
Source: US Department of Veterans Affairs, VA Technical Reference Model v 25.7 [27]

Operating System
The software “master control application” that runs the computer. It is the first program loaded when the computer is turned on, and its main component, the kernel, resides in memory at all times. The operating system sets the standards for all application programs (such as the Web server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Operational Technology
Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Operational Test and Evaluation
The field test, under realistic conditions, of any item (or key component) of weapons, equipment, or munitions for the purpose of determining the effectiveness and suitability of the weapons, equipment, or munitions for use in combat by typical military users, and the evaluation of the results of such tests.
Source: Defense Acquisition University (DAU) Glossary

Patch

A “repair job” for a piece of programming; also known as a “fix”. A patch is the immediate solution to an identified problem that is provided to users; it can sometimes be downloaded from the software maker's Web site. The patch is not necessarily the best solution for the problem, and the product developers often find a better solution to provide when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In many operating systems, a special program is provided to manage and track the installation of patches.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Permission

Authorization to perform some action on a system.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Person Entity

The role a human actor (i.e., User) performs when accessing IT assets with a specific identify.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Personally Identifiable Information

Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Pillars

A Pillar is a key focus area for implementation of Zero Trust controls.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Platform as a Service

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Policy

Statements, rules, or assertions that specify the correct or expected behavior of an entity. For example, an authorization policy might specify the correct access control rules for a software component.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Policy Decision Point

Mechanism that examines requests to access resources and compares them to the policy that applies to all requests for accessing that resource to determine whether specific access should be granted to the particular requester who issued the request under consideration.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Policy Enforcement Point (PEP)
This system is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. The PEP communicates with the Policy Advisor to forward requests and/or receive policy updates from the PA. This is a single logical component in ZTA but may be broken into two different components: the client (e.g., agent on a laptop) and resource side (e.g., gateway component in front of resource that controls access) or a single portal component that acts as a gatekeeper for communication paths.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Policy Information Point
Serves as the retrieval source of attributes, or the data required for policy evaluation to provide the information needed by the policy decision point to make the decisions.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Privileged Access Management
A class of solutions that helps secure, control, manage and monitor privileged access to critical assets.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Privileged User
A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Public Key Infrastructure
A framework that is established to issue, maintain and revoke public key certificates.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Reference Architecture
An authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions.
Source: DoD Reference Architecture Description, Version 1.0

Remote Desktop Protocol
A proprietary network protocol that allows an individual to control the resources and data of a computer over the Internet.
Source: Federal Bureau of Investigation (FBI) Public Service Announcement

Resource
Resources are data, information, performers, materiel, or personnel types that are produced or consumed.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Risk Assessment
The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Role-Based Access Control
Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Rule Set
The capture of policy in a collection of Event/Condition/Action, or other forms of assertive statements, that can be interpreted by an algorithm.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Secure Hash Algorithm
A hash algorithm with the property that it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Secure Shell
A protocol for securely logging into a remote host and executing commands on that host (e.g., administrative commands).
Source: NIST IR7966 Security of Interactive and Automated Access Management Using Secure Shell (SSH)

Secure Sockets Layer
A protocol used for protecting private information during transmission via the Internet. Note: SSL works by using the service public key to encrypt a secret key that is used to encrypt the data that is transferred over the SSL session. Most web browsers support SSL and many web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https:” instead of “http:”. The default port for SSL is 443.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Security Assertion Markup Language
A protocol consisting of XML-based request and response message formats for exchanging security information, expressed in the form of assertions about subjects, between on-line business partners.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Security Content Automation Protocol
A suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated, both to machines and humans.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Security Information and Event Manager
Control log management system that helps filter the types of events and reduce alert fatigue.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Security Orchestration, Automation, and Response
A security strategy that has evolved in recent years to automate the IR process. Some of the state of practice applications of SOAR include threat detection and response, vulnerability prioritization, compliance checks, and security audits with potential applications in many emerging areas, such as IoT management.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Security Technical Implementation Guide
Based on Department of Defense (DoD) policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DoD baseline.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Separation of Duty
Refers to the principle that no user should be given enough privileges to misuse the system on their own. For example, the person authorizing a paycheck should not also be the one who can prepare them. Separation of duties can be enforced either statically (by defining conflicting roles, i.e., roles which cannot be executed by the same user) or dynamically (by enforcing the control at access time). An example of dynamic separation of duty is the two-person rule. The first user to execute a two-person operation can be any authorized user, whereas the second user can be any authorized user different from the first [R.S. Sandhu., and P Samarati, “Access Control: Principles and Practice,” IEEE Communications Magazine 32(9), September 1994, pp. 40-48.]. There are various types of Separation of Duty, an important one is history-based Separation of Duty that regulate for example, the same subject (role) cannot access the same object for variable number of times.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Service Provider
A provider of basic services or value-added services for operation of a network; generally refers to public carriers and other commercial enterprises.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Simple Network Management Protocol (SNMP)
A standard TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates. To work with SNMP, network devices utilize a distributed data store called the Management Information Base (MIB). All SNMP-compliant devices contain a MIB which supplies the pertinent attributes of a device. Some attributes are fixed or "hard-coded" in the MIB, while others are dynamic values calculated by agent software running on the device.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Simple Object Access Protocol
An XML-based protocol for exchanging structured information in a decentralized, distributed environment.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Single Sign-On
An authentication process by which one account and its authenticators are used to access multiple applications in a seamless manner, generally implemented with a federation protocol.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Software Factory
In the DoD, a software factory is defined as a collection of people, tools, and processes that enables teams to continuously deliver value by deploying software to meet the needs of a specific community of end users. It leverages automation to replace manual processes.
Source: DoD Enterprise DevSecOps Fundamentals, Version 2.5

Software as a Service
The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Software Defined Networking
The ability to separate the control and data planes and centrally manage and control the elements in the data plane.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Supply Chain Risk Management
A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplies product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).
Source: NIST Computer Security Resource Center (CSRC) Glossary

System
A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Source: NIST Computer Security Resource Center (CSRC) Glossary

System Administrator
Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures.
Source: NIST Computer Security Resource Center (CSRC) Glossary

System Owner
Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Tactics, Techniques and Procedures
The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Tailoring
The process by which security control baselines are modified by: identifying and designating common controls, applying scoping considerations on the applicability and implementation of baseline controls, selecting compensating security controls, assigning specific values to organization-defined security control parameters, supplementing baselines with additional security controls or control enhancements, and providing additional specification information for control implementation.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Telemetry
Telemetry is the automated collection of measurements or other data at remote points and their automatic transmission to receiving equipment for monitoring.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Token
Something that the Claimant possesses and controls (typically a key or password) that is used to authenticate the Claimant's identity. A portable, user-controlled, physical device (e.g., smart card or memory stick) used to store cryptographic information and possibly also perform cryptographic functions.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Transmission Control Protocol (TCP)
TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees the delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Transport Layer Security (TLS)
An authentication and encryption protocol widely implemented in browsers and Web servers. HTTP traffic transmitted using TLS is known as HTTPS.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Trusted Automated Exchange of Intelligence Information
An application layer protocol for exchanging Cyber Threat Intelligence over HTTPS.
Source: OASIS Cyber Threat Intelligence (CTI) Technical Committee

User Activity Monitoring
The technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing U.S. Government information in order to detect insider threats and to support authorized investigations.
Source: NIST Computer Security Resource Center (CSRC) Glossary

VPN Gateway
Virtual Private Network (VPN) gateways provide secure connectivity between multiple sites, such as on-premises data centers, Virtual Private Cloud (VPC) networks, and VMware Engine private clouds. Traffic is encrypted because the VPN connections traverse the internet. Each VPN gateway can support multiple connections. When you create many connections to the same VPN gateway, all VPN tunnels share the available gateway bandwidth.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Virtual Machine
A software-defined complete execution stack consisting of virtualized hardware, operating system (guest OS), and applications.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Virtual Private Network
A virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and IP information transmitted between networks or between different nodes on the same network.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Vulnerability Management
An ISCM capability that identifies vulnerabilities [Common Vulnerabilities and Exposures (CVEs)] on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Zero Trust
A collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Zero Trust Architecture
An enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Appendix B: Abbreviations and Acronyms

The following provides a complete list of abbreviated terms and acronyms used within all Zero Trust Implementation Guidelines.

A&O	Automation and Orchestration
ABAC	Attribute-Based Access Control
ACL	Access Control List
ADC	Application Delivery Controller
AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
AppSec	Application Security
APT	Advanced Persistent Threat
ASTO	Application Security Testing Orchestration
ATO	Authorization to Operate
AUP	Acceptable Use Policy
AV	Antivirus
B/C/P/S	Base/Camp/Post/Station
BCP	Business Continuity Planning
BYOD	Bring Your Own Device
C2C	Comply-to-Connect
CA	Certificate Authority
CaC	Configuration as Code
CAC	Common Access Card
CASB	Cloud Access Security Broker
cATO	Continuous Authorization to Operate
CBA	Capabilities-Based Assessment
CCPA	California Consumer Privacy Act
CERT	Computer Emergency Response Team
CFI	Control Flow Integrity
CI/CD	Continuous Integration/Continuous Delivery (or Deployment)
CIA	Confidentiality, Integrity, and Availability
CIB	Configuration Item Baseline
CIKR	Critical Infrastructure and Key Resources
CIO	Chief Information Office
CISA	Cybersecurity and Infrastructure Security Agency
CMDB	Configuration Management Database
CMS	Content Management System
CNDSP	Computer Network Defense Service Provider
COI	Communities of Interest

CONOPS	Concept of Operations
COOP	Continuity of Operations
COTS	Commercial Off-The-Shelf
CP	Certificate Policies
CPS	Certification Practice Statement
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRS	Cyber Risk Scoring
CRUD	Create, Read, Update, and Delete
C-SCRM	Cybersecurity Supply Chain Risk Management
C-SCRM	Cybersecurity Supply Chain Risk Management
CSE	Cyber Survivability Endorsement
CSF	Cybersecurity Framework
CSI	Cybersecurity Information Sheet
CSP	Cloud Service Provider
CSPM	Cloud Security Posture Management
CSSP	Cybersecurity Service Provider
CTI	Cyber Threat Intelligence
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposure
CyberOps	Cyber Operations
DAAS	Data, Applications, Assets, and Services
DAST	Dynamic Application Security Testing
DB	Database
DBAC	Discretionary-Based Access Control
DC	Domain Controller
DCI	Defense Critical Infrastructure
DCN	Data Collection Node
DDoS	Distributed Denial-of-Service
DEP	Data Execution Prevention
DevOps	Development and Operations
DevSecOps	Development, Security, and Operations
DIB	Defense Industrial Base
DISA	Defense Information Systems Agency
DiT	Data in Transit
DiU	Data in Use
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DoD	Department of Defense
DoW	Department of War (authorized secondary title for the DoD)

DoW CIO	Department of War Chief Information Office (formerly DoD CIO)
DPI	Deep Packet Inspection
DPIV	Digital Personal Identity Verification
DPP	Data Privacy and Protection
DRM	Data Rights Management
DRP	Disaster Recovery Plan
EAM	Entity Activity Monitoring
ECA	External Certification Authority
ECDSA	Elliptic Curve Digital Signature Algorithm
EDM	Enterprise Device Management
EDR	Endpoint Detection and Response
EO	Executive Order
EPP	Endpoint Protection Platform
ETL	Extract, Transform, Load
FAM	File Activity Monitoring
FIDO	Fast Identity Online
FIM	File Integrity Monitoring
FIPS	Federal Information Processing Standards
FPKI	Federal Public Key Infrastructure
FW	Firewall
FWaaS	Firewall as a Service
GDPR	General Data Protection Regulation
GO	Global Orchestrator
GPU	Graphics Processing Unit
GRC	Governance, Risk, and Compliance
HaCC	Hosting and Computer Center
HCI	Hyperconverged Infrastructure
HEC	Hypertext Transfer Protocol (HTTP) Event Collector
HIPAA	Health Insurance Portability and Accountability Act
HIPS	Host-Based Intrusion Prevention Systems
HR	Human Resources
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/A/RBAC	Identity, Attribute, Role-Based Access Control
I/O	Input/Output
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	Identity and Access Management
IAVM	Information Assurance Vulnerability Management

IBAC	Identity-Based Access Control
ICAM	Identity, Credential, and Access Management
ICD	Interface Control Document
IC-TDF	Intelligence Community-Trusted Data Format
ID	Identification
IDaaS	Identity as a Service
IdM	Identity Management
IdP	Identity Provider
IDS	Intrusion Detection System(s)
IG	Installation Gateway
IGA	Identity Governance and Administration
ILM	Identity Lifecycle Management
IoC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPC	Inter-Process Communication
IPS	Intrusion Prevention System(s)
IPsec	Internet Protocol Security
IPv6	Internet Protocol Version 6
IR	Incident Response
ISA	Information Sharing Agreement
ISAC	Information Sharing and Analysis Center
ISN	Installation Service Node
IT	Information Technology
ITAM	Information Technology Asset Management
ITOM	Information Technology Operations Management
ITSM	Information Technology Service Management
JEA	Just Enough Administration
JIT	Just-In-Time
JSON	JavaScript Object Notation
JWT	JavaScript Object Notation (JSON) Web Tokens
KMS	Key Management System
KPI	Key Performance Indicator
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MDM	Mobile Device Management
MDR	Managed Detection and Response
MEF	Mission Essential Functionality
MFA	Multi-Factor Authentication

ML	Machine Learning
MSP	Managed Service Provider
mTLS	mutual Transport Layer Security
NAC	Network Access Control
NETCONF	Network Configuration
NetOps	Network Operations
NextGen AV	Next-Generation Antivirus
NFV	Network Function Virtualization
NGFW	Next-Generation Firewall
NG-IPS	Next-Generation Intrusion Prevention System
NIST	National Institute of Standards and Technology
NM	National Manager
NPE	Non-Person Entity
NSA	National Security Agency
NSM	National Security Memorandum
NSS	National Security Systems
NTA	Network Traffic Analysis
OAuth	Open Authorization
OCSP	Online Certificate Status Protocol
OIDC	OpenID Connect
OLTP	Online Transaction Processing
OMB	Office of Management and Budget
OS	Operating System
OSINT	Open-Source Intelligence
OSS	Operations Support System
OT	Operational Technology
OT&E	Operational Test and Evaluation
OTP	One-Time Password
OWASP	Open Worldwide Application Security Project
PA	Policy Administrator
PaaS	Platform as a Service
PAM	Privileged Access Management
PAP	Policy Administration Point
PBAC	Policy-Based Access Control
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PDP	Policy Decision Point
PE	Person Entity
PEP	Policy Enforcement Point
PfMO	Portfolio Management Office

PHI	Protected Health Information
PID	Process Identifier
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIP	Policy Information Point
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PKI	Public Key Infrastructure
PPE	Poisoned Pipeline Execution
PPSM	Ports, Protocols, and Services Management
PQC	Post-Quantum Cryptography
PQE	Post-Quantum Encryption
PS	Personnel Security
RA	Reference Architecture
RAM	Random-Access Memory
RASP	Runtime Application Self-Protection
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
REST	Representational State Transfer
REST API	Representational State Transfer Application Programming Interface
RFP	Request for Proposal
RPA	Robotic Process Automation
RPO	Recovery Point Objective
RSA	Rivest-Shamir-Adleman
RTO	Recovery Time Objective
SA	System Administrator
SaaS	Software as a Service
SALC	Software Acquisition Life Cycle
SAM	Software Asset Management
SAML	Security Assertion Markup Language
SAST	Static Application Security Testing
SBOM	Software Bills of Material
SCA	Software Composition Analysis
SCAP	Security Content Automation Protocol
SCIM	System for Cross-domain Identity Management
SCRM	Supply Chain Risk Management
SDC	Software-Defined Compute
SDLC	Software Development Lifecycle
SDN	Software-Defined Networking
SDS	Software-Define Storage

SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SID	Security Identifier
SIEM	Security Incident and Event Manager
SLA	Service Level Agreement
SMART	Specific, Measurable, Achievable, Relevant, and Time-bound
SME	Subject Matter Expert
SNMP	Simple Network Management Protocol
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SOP	Standard Operating Procedure
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
STIG	Security Technical Implementation Guide
STIX	Structured Threat Information eXpression
Syslog	System Log
T&E	Testing and Evaluation
TAXII	Trusted Automated Exchange of Intelligence Information
TCP	Transmission Control Protocol
TEE	Trusted Execution Environment
TIP	Threat Intelligence Platform
TLS	Transport Layer Security
TPU	Tensor Processing Unit
TTP	Tactics, Techniques and Procedures
UAM	User Activity Monitoring
UAT	User Acceptance Testing
UEBA	User and Entity Behavior Analytics
UEDM	Unified Endpoint and Device Management
UEM	Unified Endpoint Management
USB	Universal Serial Bus
USG	United States Government
VA	Validation Authority
VAULTIS	Visible, Assessable, Understandable, Linked, Trusted, Interoperable, and Secure
VDP	Vulnerability Disclosure Program
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMP	Vulnerability Management Program
VPN	Virtual Private Network

VRF	Virtual Routing and Forwarding
VXLAN	Virtual Extensible Local Area Network
WAF	Web Application Firewall
WAN	Wide Area Network
X.509	International Public Key Certificate Standard for secure signatures and web browsers
XaaS	Anything as a Service
XDR	Extended Detection and Response
XML	Extensible Markup Language
YAML	Yet Another Markup Language
ZIG	Zero Trust Implementation Guideline
ZT	Zero Trust
ZTA	Zero Trust Architecture
ZTDF	Zero Trust Data Format
ZTP	Zero-Touch Provisioning

Appendix C: References

[1] Department of War Office of the Chief Information Officer. "Department of Defense Zero Trust Strategy, Version 1.0." 2022. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[2] Department of War Office of the Chief Information Officer. "Department of Defense Zero Trust Capabilities and Activities." 2025. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-CapabilitiesActivities.pdf?ver=-o9HgcID4LQHccIGjNQtiw%3d%3d

[3] Department of War. "Zero Trust Reference Architecture, Version 2.0." 2022. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[4] National Security Agency. "CSI: Embracing a Zero Trust Security Model." 2021. Available: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

[5] National Security Agency. "CSI: Advancing Zero Trust Maturity Throughout the User Pillar." 2023. Available: https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI_Zero_Trust_User_Pillar_v1.1.PDF

[6] National Security Agency. "CSI: Advancing Zero Trust Maturity Throughout the Device Pillar." 2023. Available: https://media.defense.gov/2023/Oct/19/2003323562/-1/-1/0/CSI-DEVICE-PILLAR-ZERO-TRUST.PDF

[7] National Security Agency. "CSI: Advancing Zero Trust Maturity Throughout the Application & Workload Pillar." 2024. Available: https://media.defense.gov/2024/May/22/2003470825/-1/-1/0/CSI-APPLICATION-AND-WORKLOAD-PILLAR.PDF

[8] National Security Agency. "CSI: Advancing Zero Trust Maturity Throughout the Data Pillar." 2024. Available: https://media.defense.gov/2024/Apr/09/2003434442/-1/-1/0/CSI_DATA_PILLAR_ZT.PDF

[9] National Security Agency. "CSI: Advancing Zero Trust Maturity Throughout the Network & Environment Pillar." 2024. Available: https://media.defense.gov/2024/Jul/10/2003500250/-1/-1/0/CSI-ZT-AUTOMATION-ORCHESTRATION-PILLAR.PDF

[10] National Security Agency. "CSI: Advancing Zero Trust Maturity Throughout the Automation & Orchestration Pillar." 2024. Available: https://media.defense.gov/2024/Jul/10/2003500250/-1/-1/0/CSI-ZT-AUTOMATION-ORCHESTRATION-PILLAR.PDF

[11] National Security Agency. "CSI: Advancing Zero Trust Maturity Throughout the Visibility & Analytics Pillar." 2024. Available: https://media.defense.gov/2024/May/30/2003475230/-1/-1/0/CSI-VISIBILITY-AND-ANALYTICS-PILLAR.PDF

[12] Department of War Office of the Chief Information Officer. "Zero Trust Execution Roadmap, Version 1.1." 2024. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-ExecutionRoadmap-v1.1.pdf

[13] National Institute of Standards and Technology. "Computer Security Resource Center Glossary." 2021. Available: https://csrc.nist.gov/glossary

[14] National Institute of Standards and Technology. "An Introduction to Information Security, NIST Special Publication 800-12r1." 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

[15] National Institute of Standards and Technology. "Mobile Device Security: Bring Your Own Device (BYOD), NIST Special Publication 1800-22." 2023. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-22.pdf

[16] National Security Agency and Cybersecurity and Infrastructure Security Agency. "Defending Continuous Integration/Continuous Delivery (CI/CD) Environments." 2023. Available: https://media.defense.gov/2023/Jun/28/2003249466/-1/-1/0/CSI_DEFENDING_CI_CD_ENVIRONMENTS.PDF

[17] Cybersecurity and Infrastructure Agency. "Cloud Security Technical Reference Architecture." 2022. Available: https://www.cisa.gov/sites/default/files/2023-02/cloud_security_technical_reference_architecture_2.pdf

[18] Department of War. "Common Access Card (CAC)." n.d. Available: https://www.cac.mil/Common-Access-Card/

[19] National Institute of Standards and Technology. "Zero Trust Architecture, NIST Special Publication 800-207." 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[20] Defense Acquisition University. "Cyber Survivability Endorsement Implementation Guide." n.d. Available: https://www.dau.edu/sites/default/files/Migrated/CopDocuments/Guide%20-%20Cyber%20Survivability%20Endorsement%20Implementation.pdf (accessed.

[21] United States Cybersecurity Magazine. "Department of Defense (DOD) Cybersecurity Service Providers (CSSPs): A Unique Component of DOD's Defense–in–Depth Strategy." n.d. Available: https://www.uscybersecurity.net/dod/

[22] Congressional Research Service. "The U.S. Defense Industrial Base: Background and Issues for Congress." 2024. Available: https://www.congress.gov/crs-product/R47751

[23] MITRE. "MITRE D3FEND." 2025. Available: https://d3fend.mitre.org

[24] General Services Administration. "Identity Lifecyle Management Playbook." 2024. Available: https://www.idmanagement.gov/playbooks/ilm/#stage-2---provisioning--identity-governance-administration-iga

[25] National Institute of Standards and Technology. "Identity as a Service for Public Safety Organizations, NIST IR 8335." 2021. Available: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8335-draft.pdf

[26] Government Accountability Office. "Agile Assessment Guide: Best Practices for Adoption and Implementation." 2023. Available: https://www.gao.gov/assets/d24105506.pdf

[27] Department of Veterans Affairs. "Open Identifier (OpenID) Connect, VA Technical Reference Model, Version 25.7." 2025. Available: https://www.oit.va.gov/Services/TRM/StandardPage.aspx?tid=6769#

[28] Defense Acquisition University. "Defense Acquisition University Glossary." n.d. Available: https://www.dau.edu/glossary

[29] Department of War Office of the Chief Information Officer. "DoD Reference Architecture Description." 2010. Available: https://dodcio.defense.gov/Portals/0/Documents/Ref_Archi_Description_Final_v1_18Jun10.pdf

[30] Federal Bureau of Investigation. "Cyber Actors Increasingly Exploit the Remote Desktop Protocol to Conduct Malicious Activity." 2018. Available: https://www.ic3.gov/PSA/2018/PSA180927#:~:text=Definition,making%20intrusions%20difficult%20to%20detect

[31] National Institute of Standards and Technology. "Security of Interactive and Automated Access Management Using Secure Shell (SSH), NIST IR 7966." 2015. Available: https://nvlpubs.nist.gov/nistpubs/ir/2015/nist.ir.7966.pdf

[32] OASIS. "Introduction to TAXII." 2024. Available: https://oasis-open.github.io/cti-documentation/taxii/intro.html

Appendix D: Activity Implementation Task Diagrams (All Phases)

The Department of War (DoW) Chief Information Office (CIO) Zero Trust (ZT) Framework defines 152 Activities (91 Target-level) that describe how organizations can implement ZT. The relationship between the implementation of these Activities is identified through DoW-defined predecessors and successors for each Activity. These Zero Trust Implementation Guidelines (ZIGs) provide a set of Implementation Tasks associated with DoW-defined ZT Activities to accomplish the Expected Outcomes and Capability intents.

In the ZIGs, the Activities feature multiple tasks, with several predecessors and successors, leading to a complex and intricate implementation process. Additionally, dependency and constraint relationships between tasks within a single Activity or across different Activities add to this complexity. The following Activity Task Diagrams provide a non-linear, illustrative example of a one-to-one visualization of the Activity, beginning on the left with any defined predecessors, followed by the Activity tasks as outlined in the applicable Activity, and ending on the right with defined successors. A filled in circle at the beginning indicates that there is/are no DoW-defined predecessor(s) and a non-filled in circle at the end indicates there is/are no DoW-defined successor(s) for that particular Activity. The diagrams provide a standardized visual representation for navigating the implementation process. Appendix D begins with a linear graphic illustrating the Pillars and Activities, by both Pillar and Phase. This diagram serves as a reference guide to the subsequent Activity Task Diagrams.

Zero Trust Target Level Activities

Pillar	Discovery	Phase I	Phase II
USER	1.1.1 Inventory User	1.3.1 Organizational MFA & IdP 1.4.1 Implement System and Migrate Privileged Users Pt. 1 1.5.1 Organization Identity Lifecycle Management 1.7.1 Deny User by Default Policy 1.8.1 Single Authentication	1.2.1 Implement App-Based Permissions per Enterprise 1.2.2 Rule-Based Dynamic Access Pt. I 1.4.2 Implement System and Migrate Privileged Users Pt. 2 1.5.2 Enterprise Identity Lifecycle Management Pt. 1 1.6.1 Implement UEBA & UAM Tooling 1.8.2 Periodic Authentication 1.9.1 Enterprise PKI & IdP Pt. 1
DEVICE	2.1.1 Device Health Tool Gap Analysis 2.3.4 Integrate NextGen AV Tools w/C2C	2.1.2 NPE & PKI, Device Under Management 2.4.1 Deny Device by Default Policy 2.5.1 Implement Asset, Vulnerability, & Patch Management Tools 2.6.1 Implement UEDM or Equivalent Tools 2.6.2 Enterprise Device Management Pt. 1 2.7.1 Implement EDR Tools & Integrate w/C2C	2.1.3 Enterprise IdP Part 1 2.2.1 Implement C2C/Compliance-Based Network Authorization Pt. 1 2.3.3 Implement Application Control & FIM Tools 2.4.2 Managed & Limited BYOD & IoT Support 2.6.3 Enterprise Device Management Pt. 2 2.7.2 Implement XDR Tools & Integrate w/C2C Pt. 1
APPLICATION & WORKLOAD	3.1.1 Application/Code Identification	3.2.1 Build DevSecOps Software Factory Pt. 1 3.2.2 Build DevSecOps Software Factory Pt. 2 3.3.1 Approved Binaries/Code 3.3.2 Vulnerability Management Program Pt. 1 3.4.1 Resource Authorization Pt. 1 3.4.3 SDC Resource Authorization Pt. 1	3.2.3 Automate Application Security & Code Remediation Pt. 1 3.3.3 Vulnerability Management Program Pt. 2 3.3.4 Continual Validation 3.4.2 Resource Authorization Pt. 2 3.4.4 SDC Resource Authorization Pt. 2
DATA	4.1.1 Data Analysis 4.4.1 DLP Enforcement Point Logging & Analysis 4.4.2 DRM Enforcement Point Logging & Analysis	4.2.1 Define Data Tagging Standards 4.2.2 Interoperability Standards 4.3.1 Implement Data Tagging & Classification Tools 4.4.3 File Activity Monitoring Pt. 1 4.5.1 Implement DRM and Protection Tools Pt. 1 4.6.1 Implement Enforcement Points	4.2.3 Develop SDS Policy 4.3.2 Manual Data Tagging Pt. 1 4.4.4 File Activity Monitoring Pt. 2 4.5.2 Implement DRM & Protection Tools Pt. 2 4.5.3 DRM Enforcement via Data Tags & Analytics Pt. 1 4.6.2 DLP Enforcement via Data Tags & Analytics Pt. 1 4.7.1 Integrate DAAS Access w/SDS Policy Pt. 1 4.7.4 Integrate Solution(s) & Policy w/Enterprise IdP Pt. 1
NETWORK & ENVIRONMENT	5.1.1 Define Granular Control Access Rules & Policies Pt. 1 5.2.1 Define SDN APIs	5.1.2 Define Granular Control Access Rules & Policies Pt. 2 5.2.2 Implement SDN Programmable Infrastructure 5.3.1 Datacenter Macro-Segmentation 5.4.1 Implement Micro-Segmentation	5.2.3 Segment Flows into Control, Management, & Data Planes 5.3.2 B/C/P/S Macro-Segmentation 5.4.2 Application & Device Micro-Segmentation 5.4.4 Protect Data in Transit
AUTOMATION & ORCHESTRATION	6.1.1 Policy Inventory & Development 6.2.1 Task Automation Analysis 6.5.1 Response Automation Analysis 6.6.1 Tool Compliance Analysis	6.1.2 Organization Access Profile 6.5.2 Implement SOAR Tools 6.6.2 Standardized API Calls & Schemas Pt. 1 6.7.1 Workflow Enrichment Pt. 1	6.1.3 Enterprise Security Profile Pt. 1 6.2.2 Enterprise Integration & Workflow Provisioning Pt. 1 6.3.1 Implement Data Tagging & Classification ML Tools 6.6.3 Standardized API Calls & Schemas Pt. 2 6.7.2 Workflow Enrichment Pt. 2
VISIBILITY & ANALYTICS	7.1.1 Scale Considerations	7.1.2 Log Parsing 7.2.1 Threat Alerting Pt. 1 7.2.4 Asset ID & Alert Correlation 7.3.1 Implement Analytics Tools 7.5.1 Cyber Threat Intelligence Program Pt. 1	7.1.3 Log Analysis 7.2.2 Threat Alerting Pt. 2 7.2.5 User & Device Baselines 7.3.2 Establish User Baseline Behavior 7.4.1 Baseline & Profiling Pt. 1 7.5.2 Cyber Threat Intelligence Program Pt. 2

Target Activities: 91

Figure D-1: Target-level Activities by Pillar

Activity 1.1.1 Inventory User

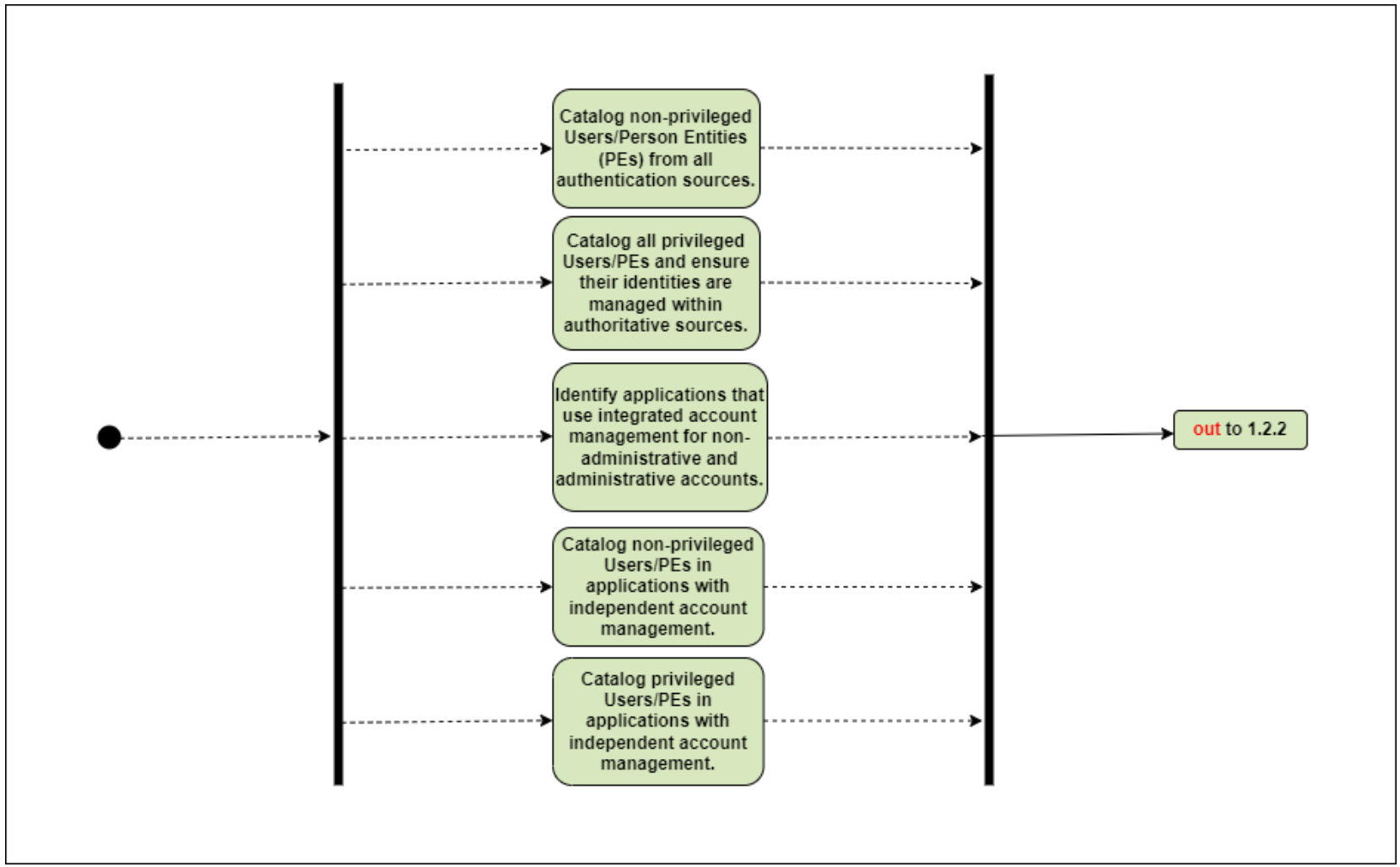

Figure D- 2: Implementation Tasks for Activity 1.1.1 — Inventory User

Activity 1.2.1 Implement Application-Based Permissions per Enterprise

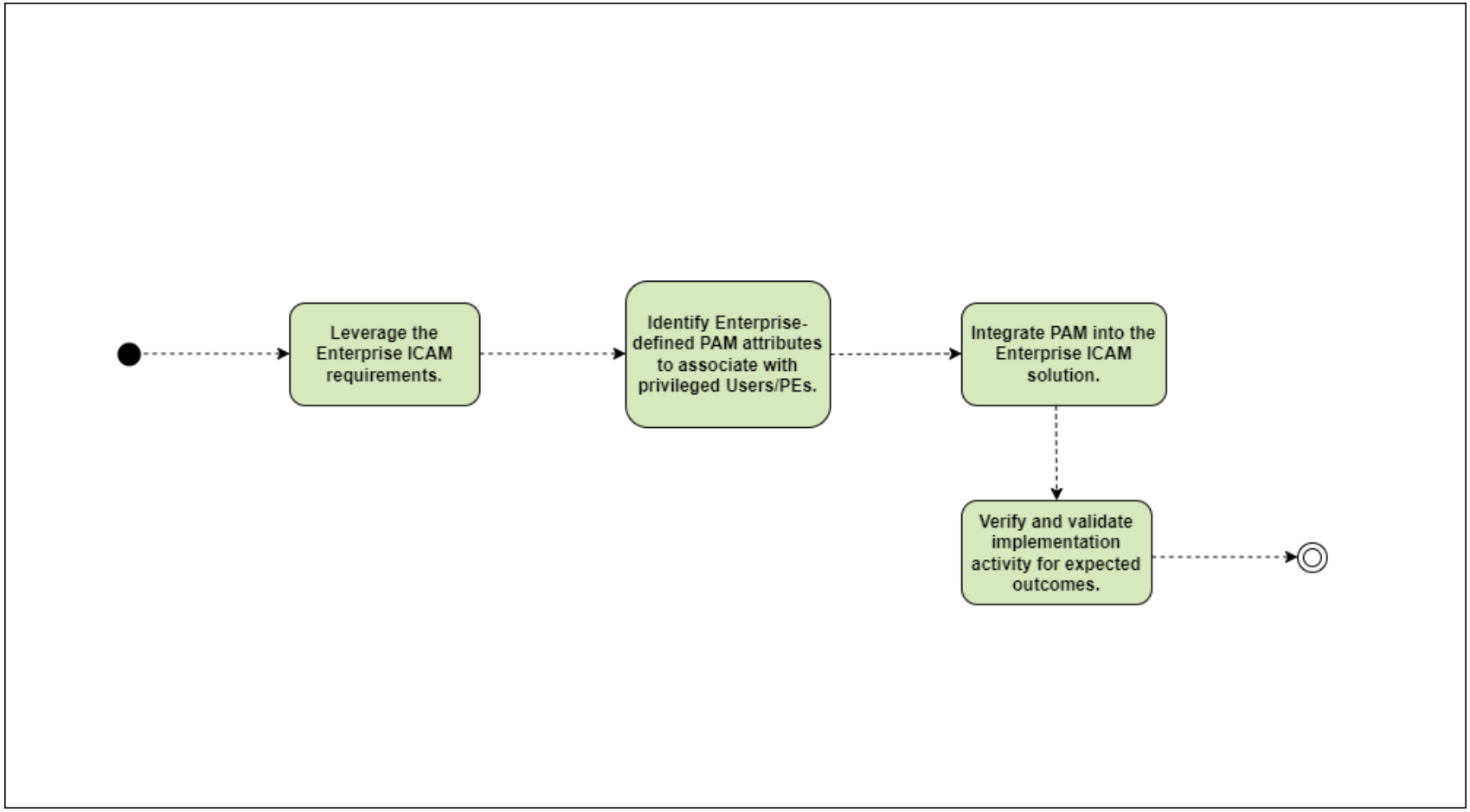

Figure D- 3: Implementation Tasks for Activity 1.2.1 — Implement Application-Based Permissions per Enterprise

Activity 1.2.2 Rule-Based Dynamic Access Part 1

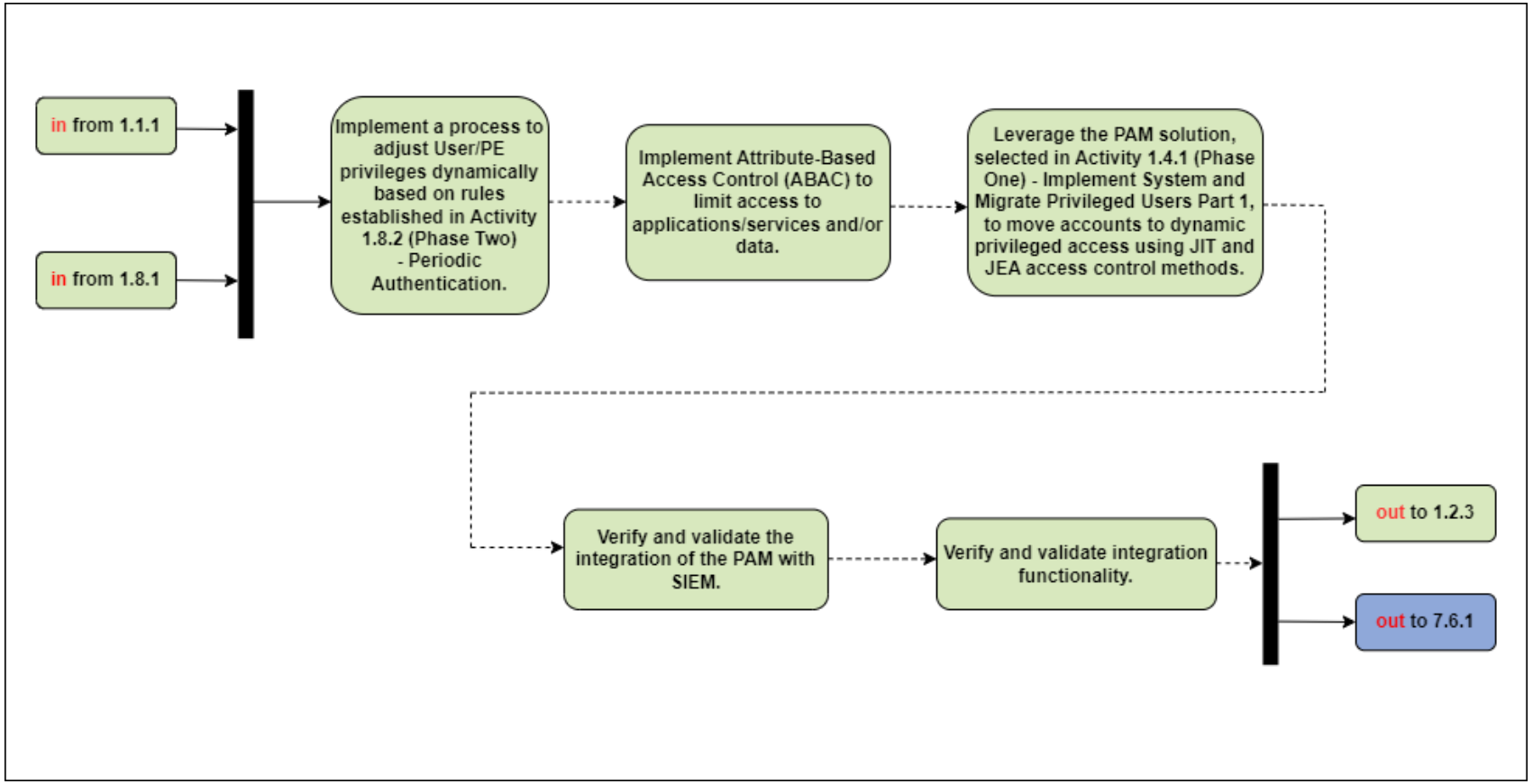

Figure D- 4: Implementation Tasks for Activity 1.2.2 — Rule-Based Dynamic Access Part 1

Activity 1.3.1 Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)

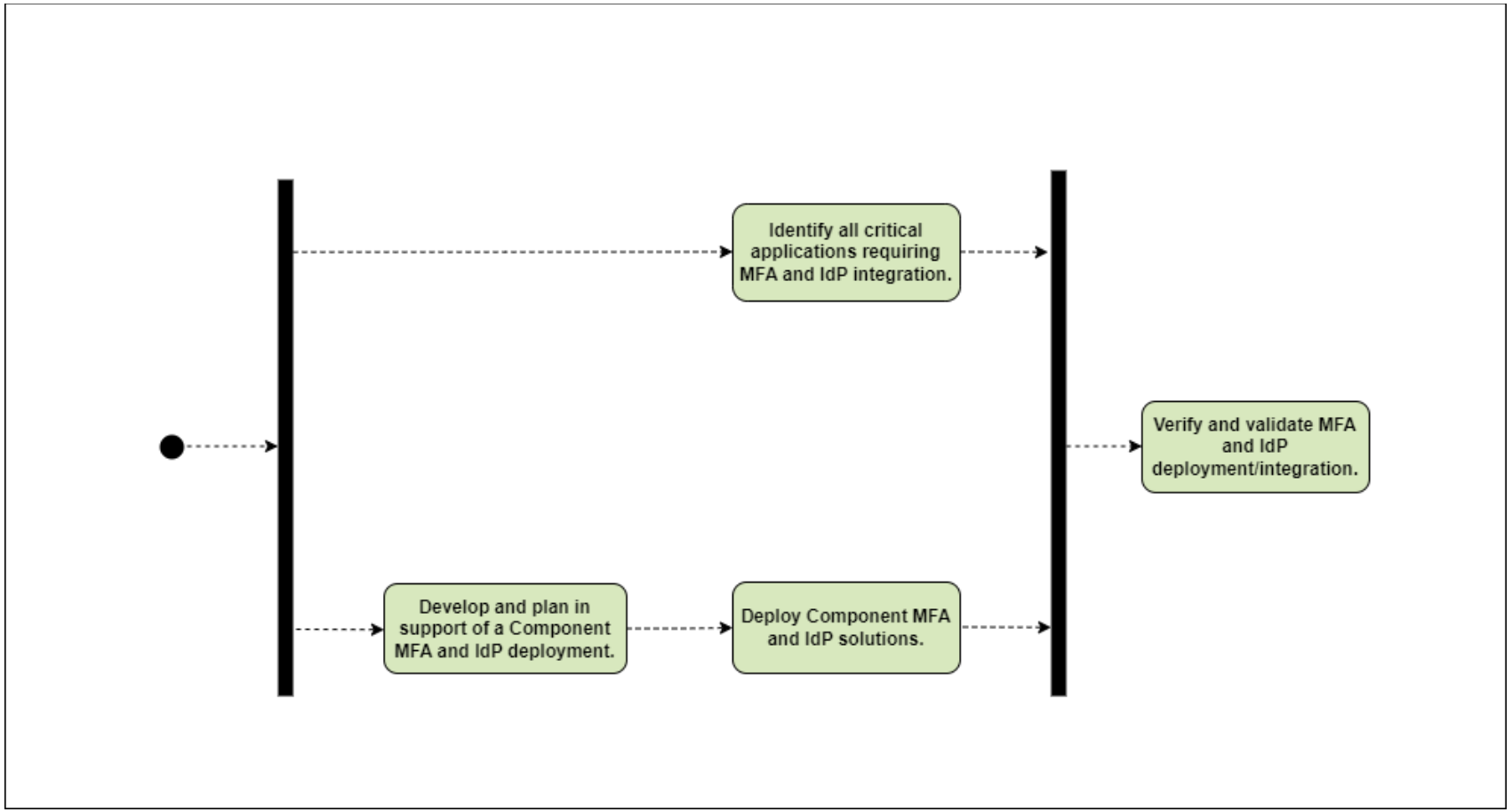

Figure D- 5: Implementation Tasks for Activity 1.3.1 — Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)

Activity 1.4.1 Implement System and Migrate Privileged Users Part 1

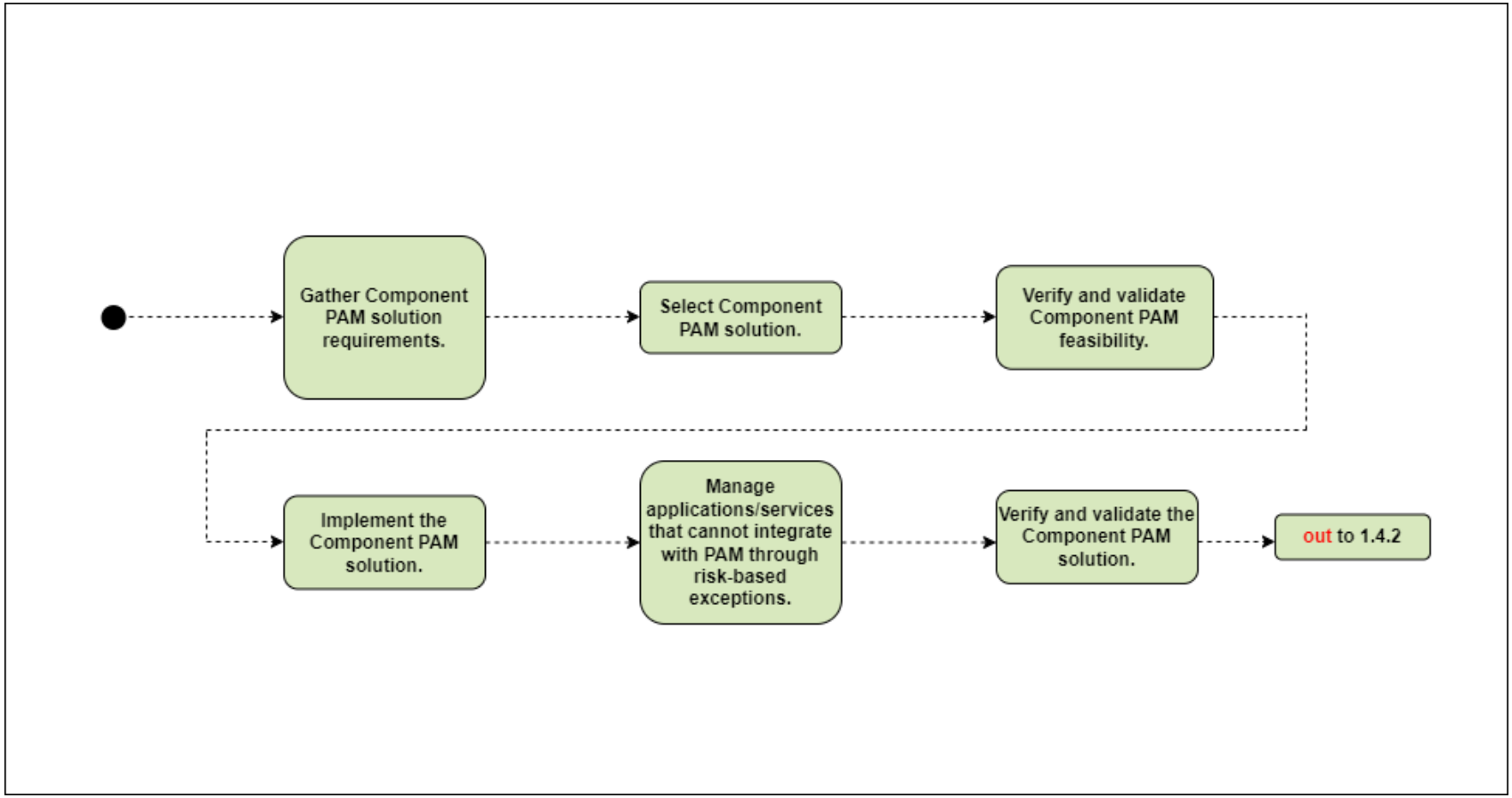

Figure D- 6: Implementation Tasks for Activity 1.4.1 — Implement System and Migrate Privileged Users Part 1

Activity 1.4.2 Implement System and Migrate Privileged Users Part 2

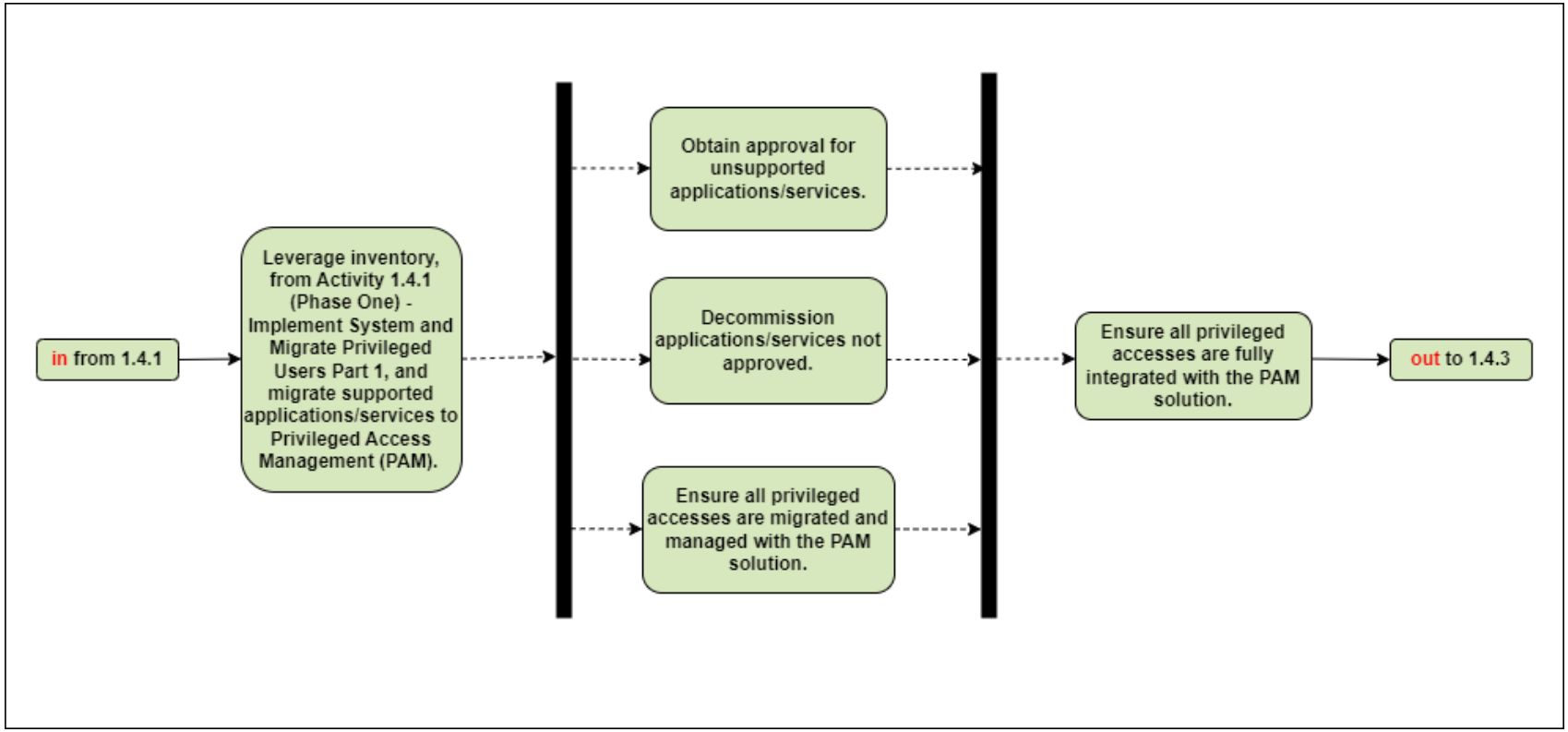

Figure D- 7: Implementation Tasks for Activity 1.4.2 — Implement System and Migrate Privileged Users Part 2

Activity 1.5.1 Organizational Identity Lifecycle Management (ILM)

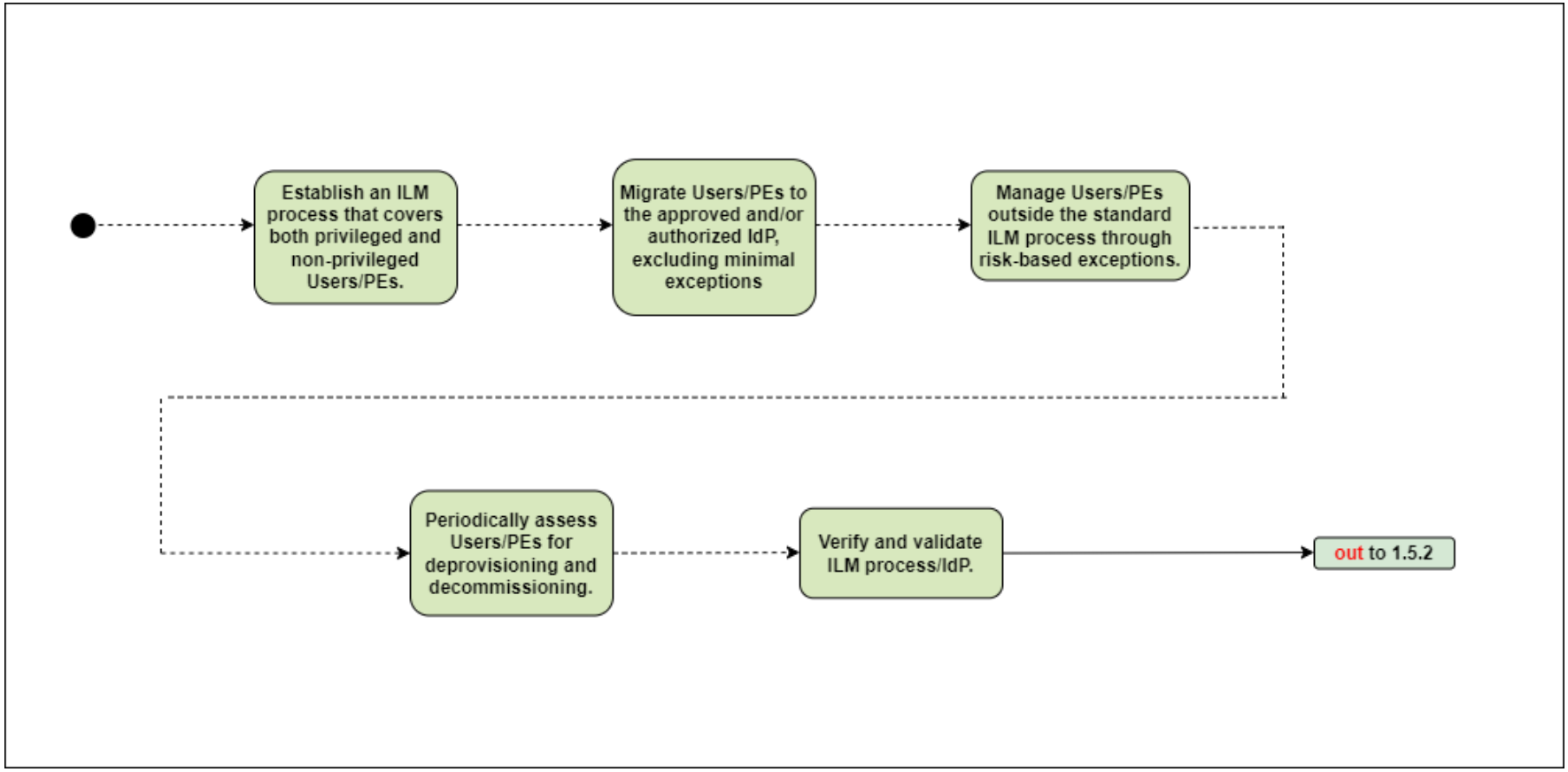

Figure D- 8: Implementation Tasks for Activity 1.5.1 — Organizational Identity Lifecycle Management (ILM)

Activity 1.5.2 Enterprise Identity Lifecycle Management (ILM) Part 1

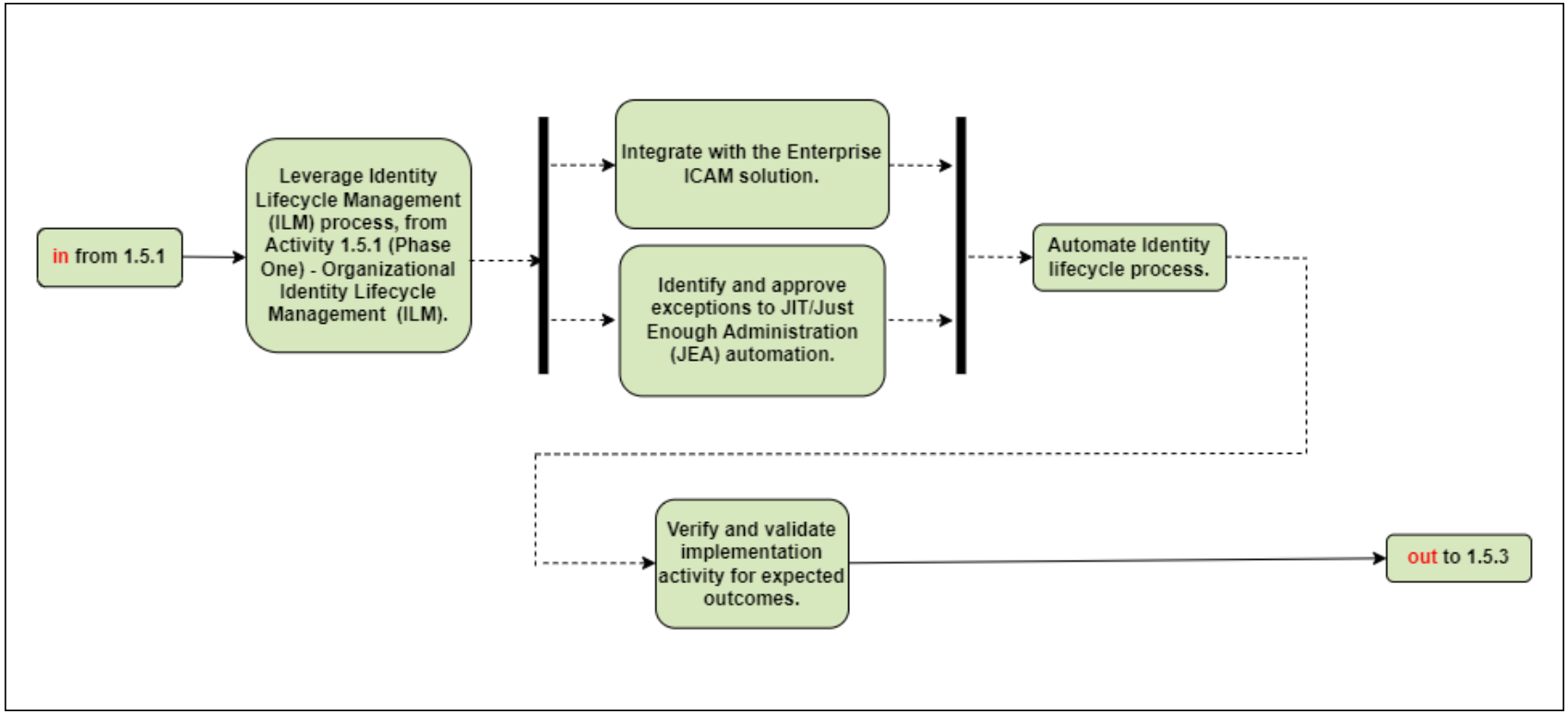

Figure D- 9: Implementation Tasks for Activity 1.5.2 — Enterprise Identity Lifecycle Management (ILM) Part 1

Activity 1.6.1 Implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) Tooling

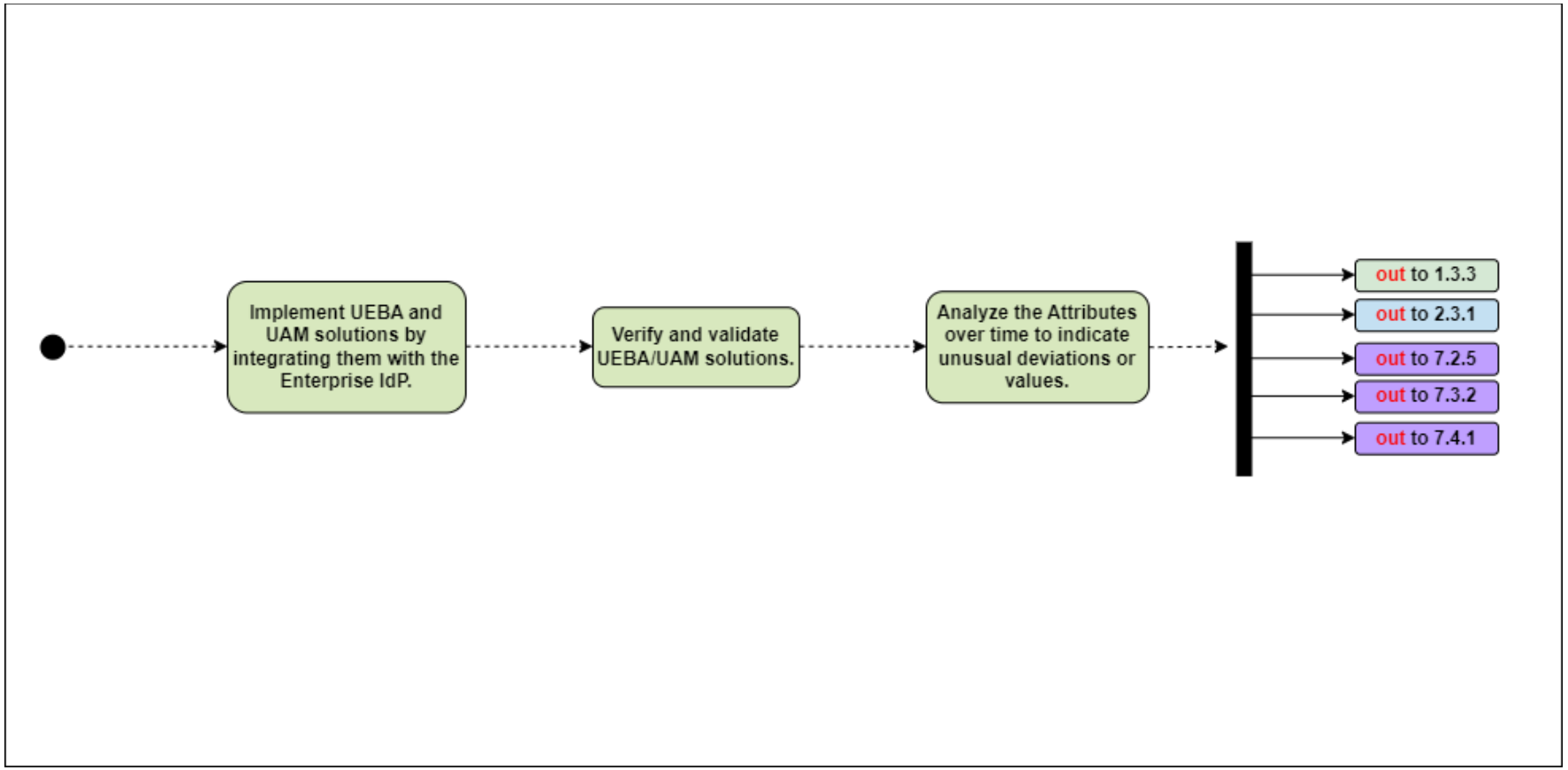

Figure D- 10: Implementation Tasks for Activity 1.6.1 — Implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) Tooling

Activity 1.7.1 Deny User by Default Policy

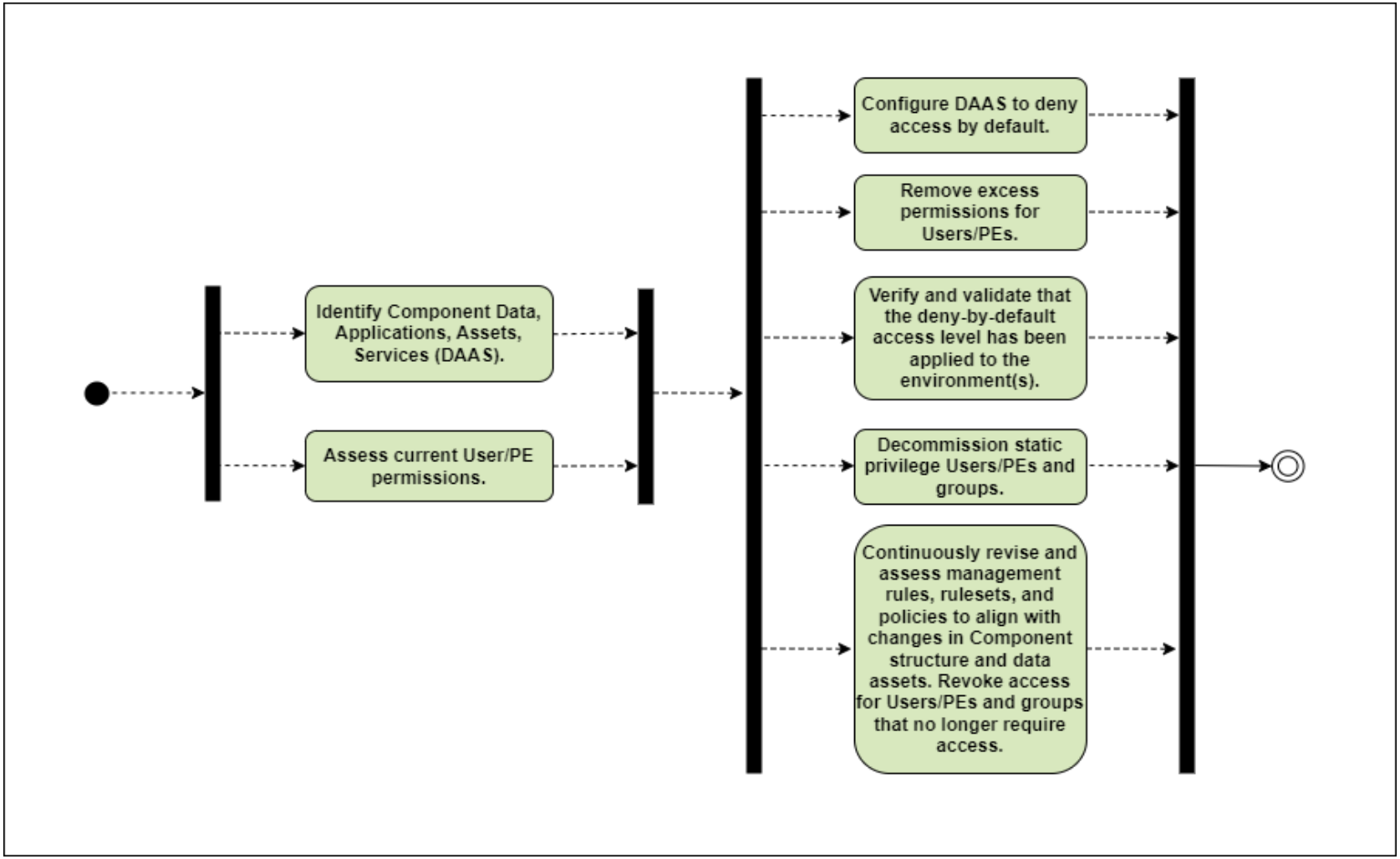

Figure D- 11: Implementation Tasks for Activity 1.7.1 — Deny User by Default Policy

Activity 1.8.1 Single Authentication

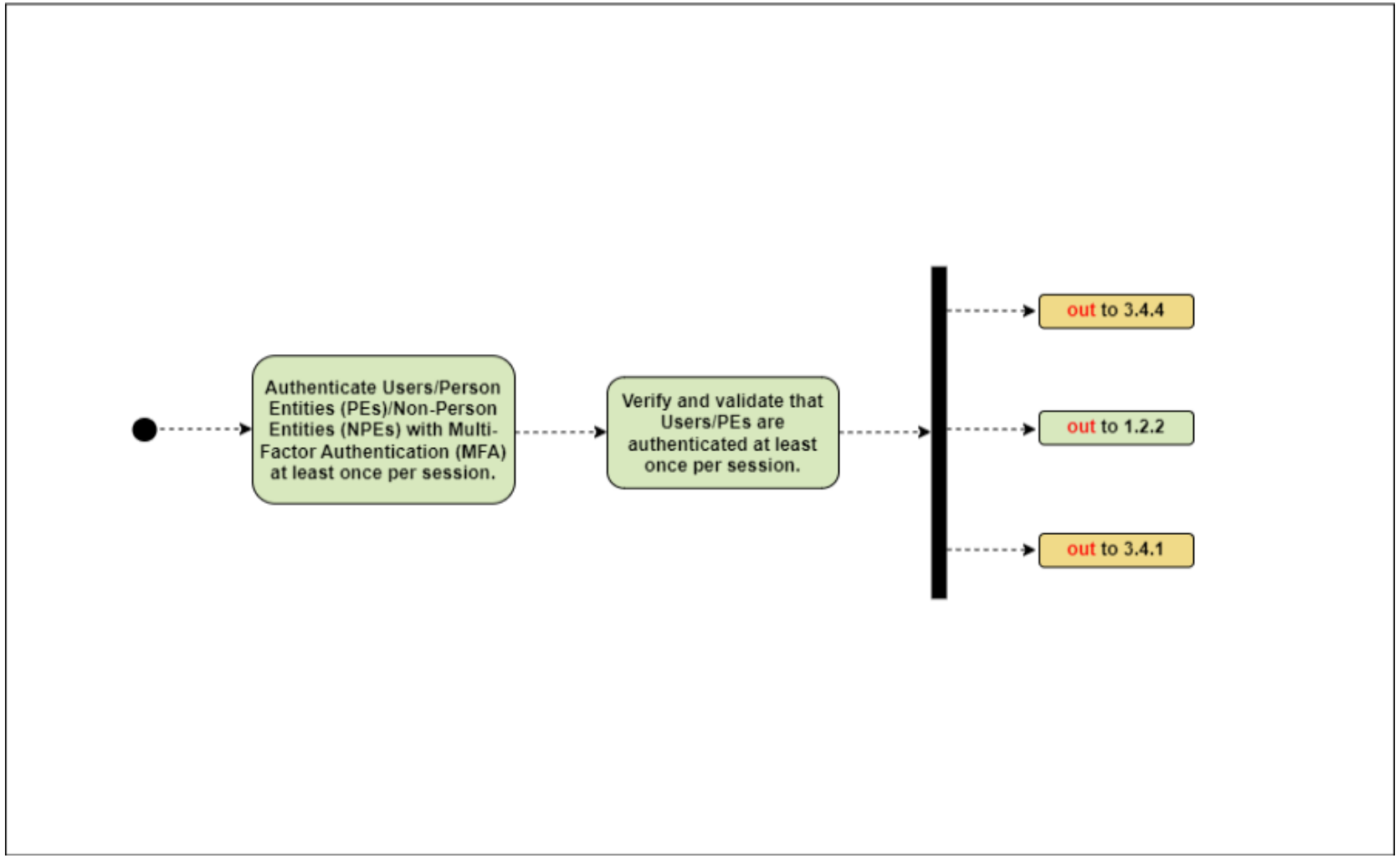

Figure D- 12: Implementation Tasks for Activity 1.8.1 — Single Authentication

Activity 1.8.2 Periodic Authentication

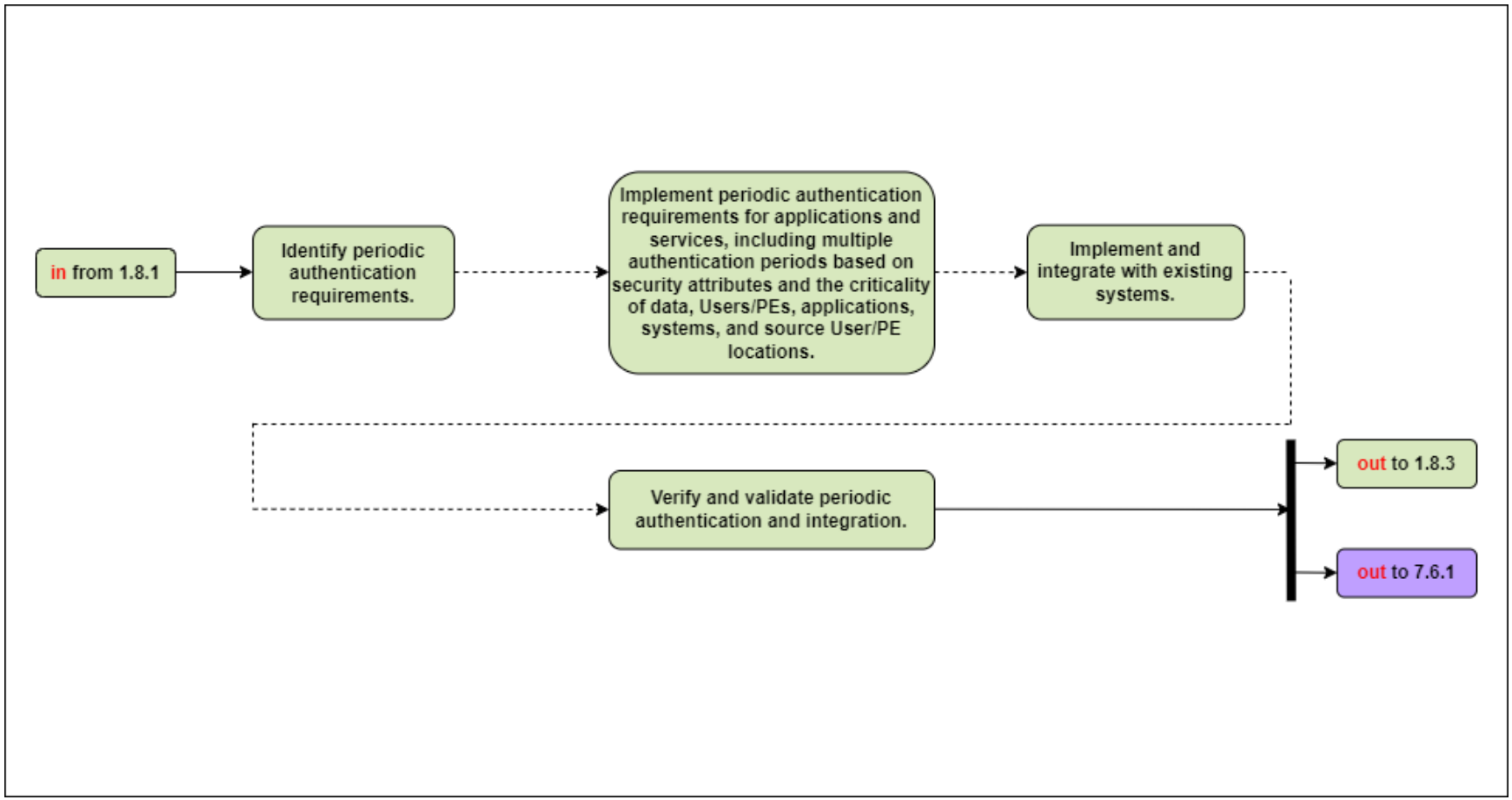

Figure D- 13: Implementation Tasks for Activity 1.8.2 — Periodic Authentication

Activity 1.9.1 Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1

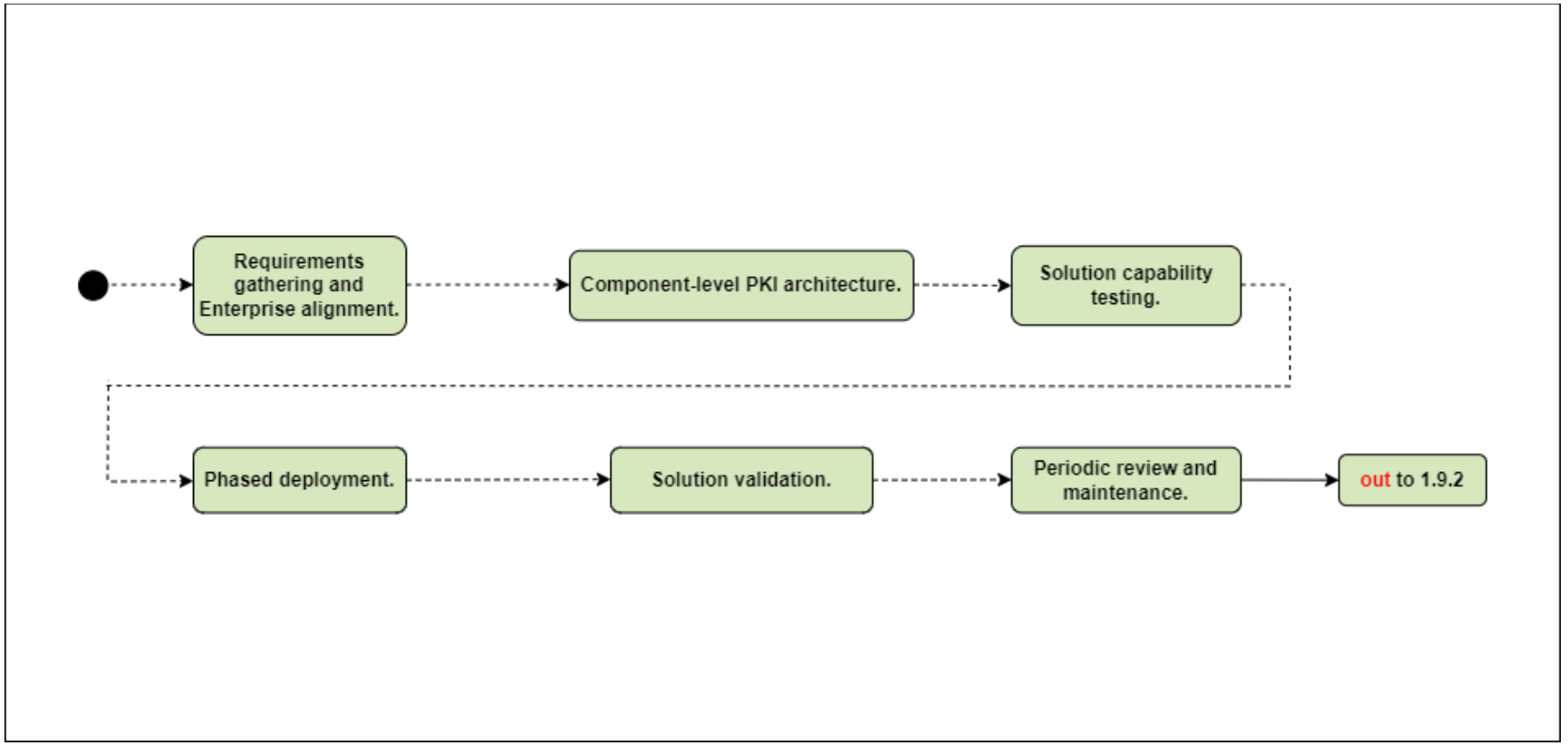

Figure D- 14: Implementation Tasks for Activity 1.9.1 — Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1

Activity 2.1.1 Device Health Tool Gap Analysis

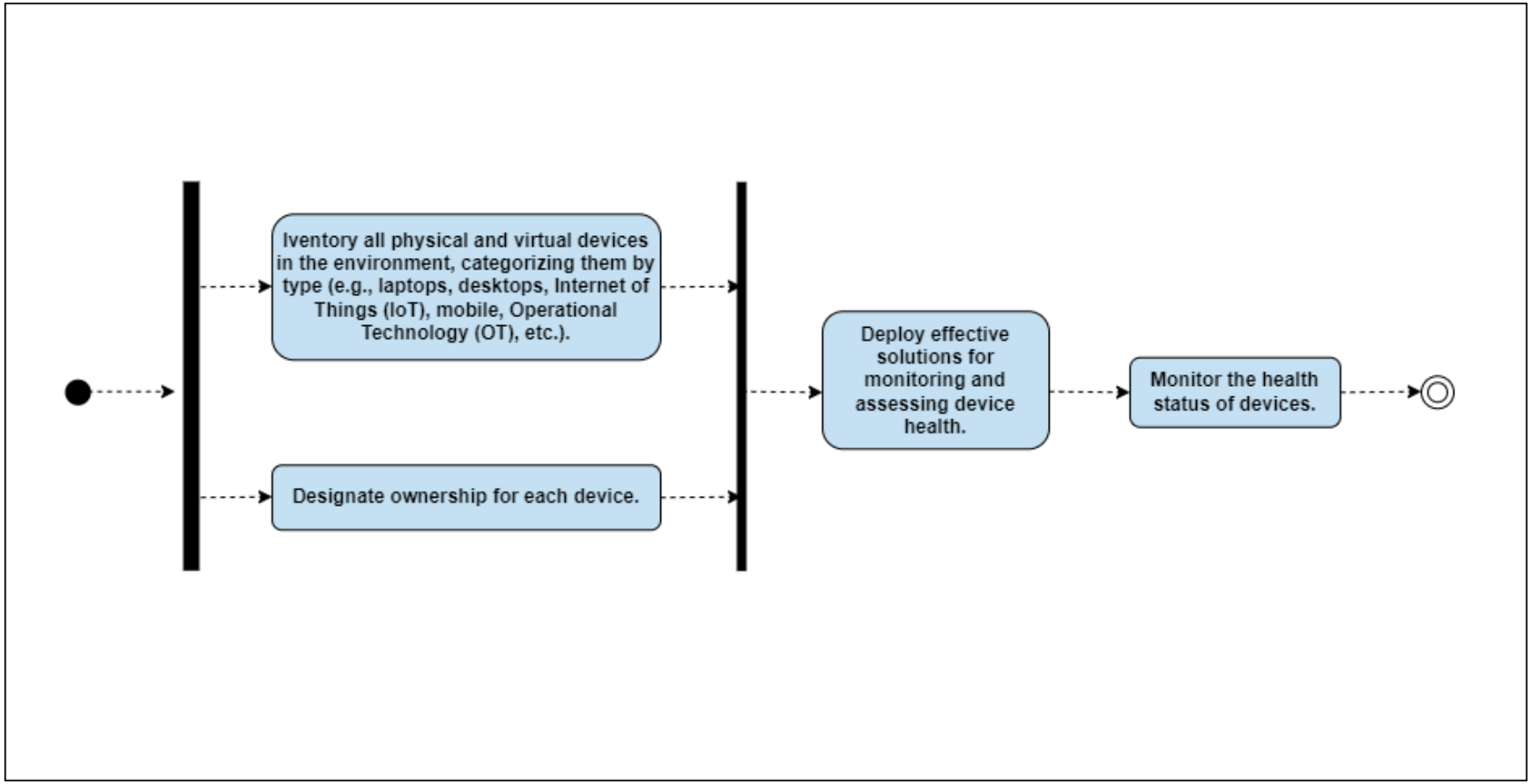

Figure D- 15: Implementation Tasks for Activity 2.1.1 — Device Health Tool Gap Analysis

Activity 2.1.2 Non-Person Entity (NPE) and Public Key Infrastructure (PKI), Device Under Management

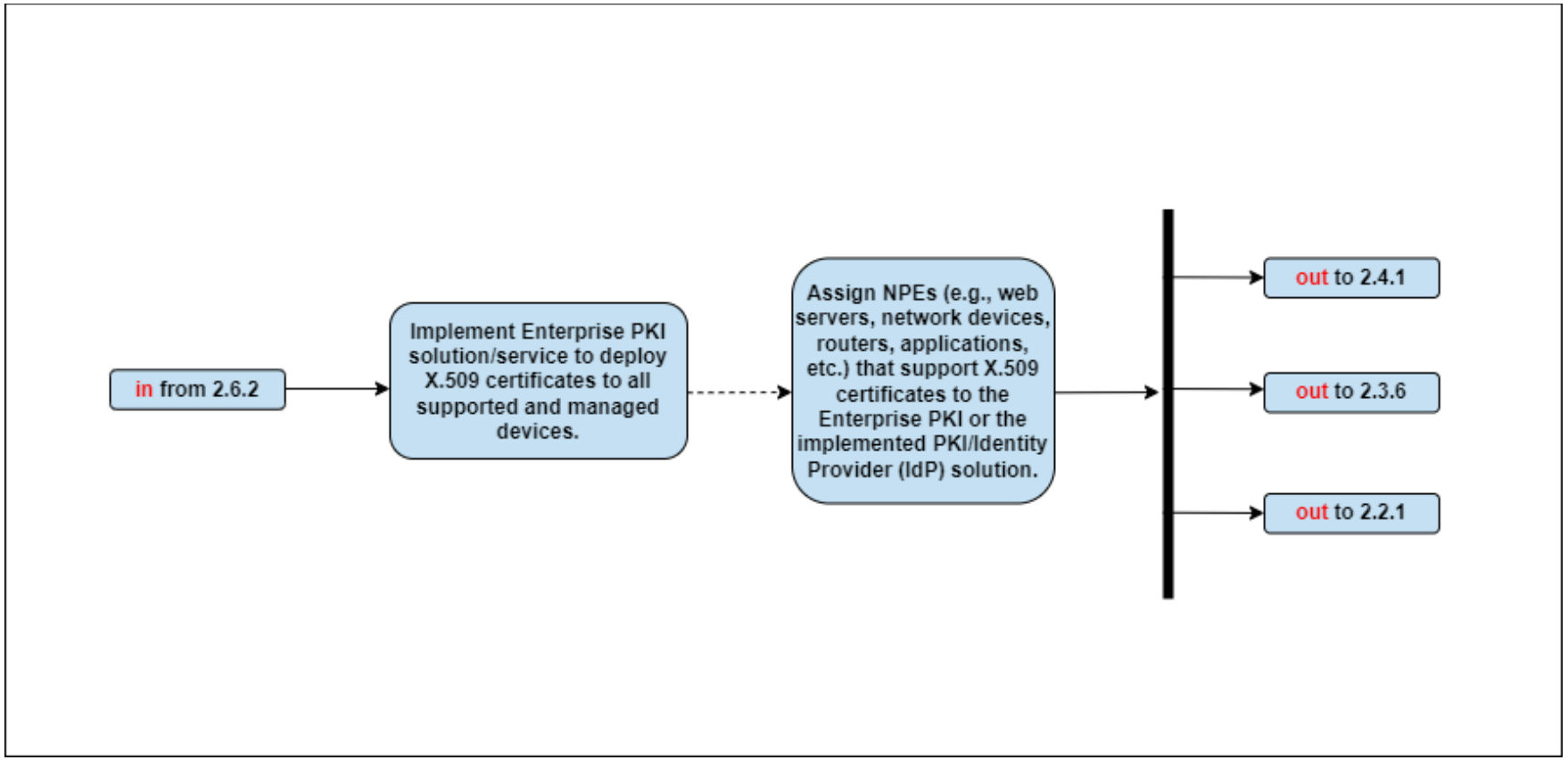

Figure D- 16: Implementation Tasks for Activity 2.1.2 — Non-Person Entity (NPE) and Public Key Infrastructure (PKI), Device Under Management

Activity 2.1.3 Enterprise Identity Provider (IdP) Part 1

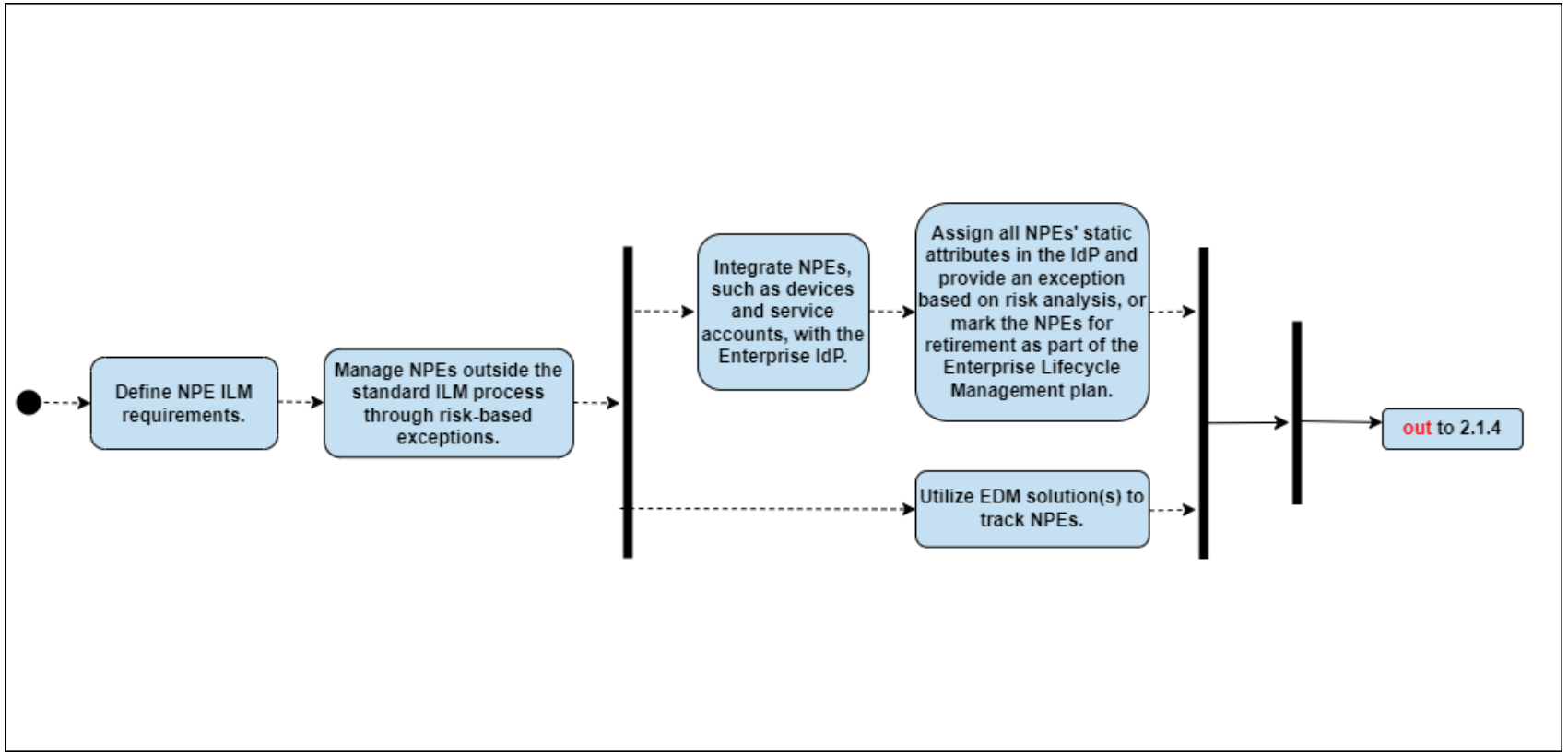

Figure D- 17: Implementation Tasks for Activity 2.1.3 — Enterprise Identity Provider (IdP) Part 1

Activity 2.2.1 Implement Comply-to-Connect (C2C) and Compliance-Based Network Authorization Part 1

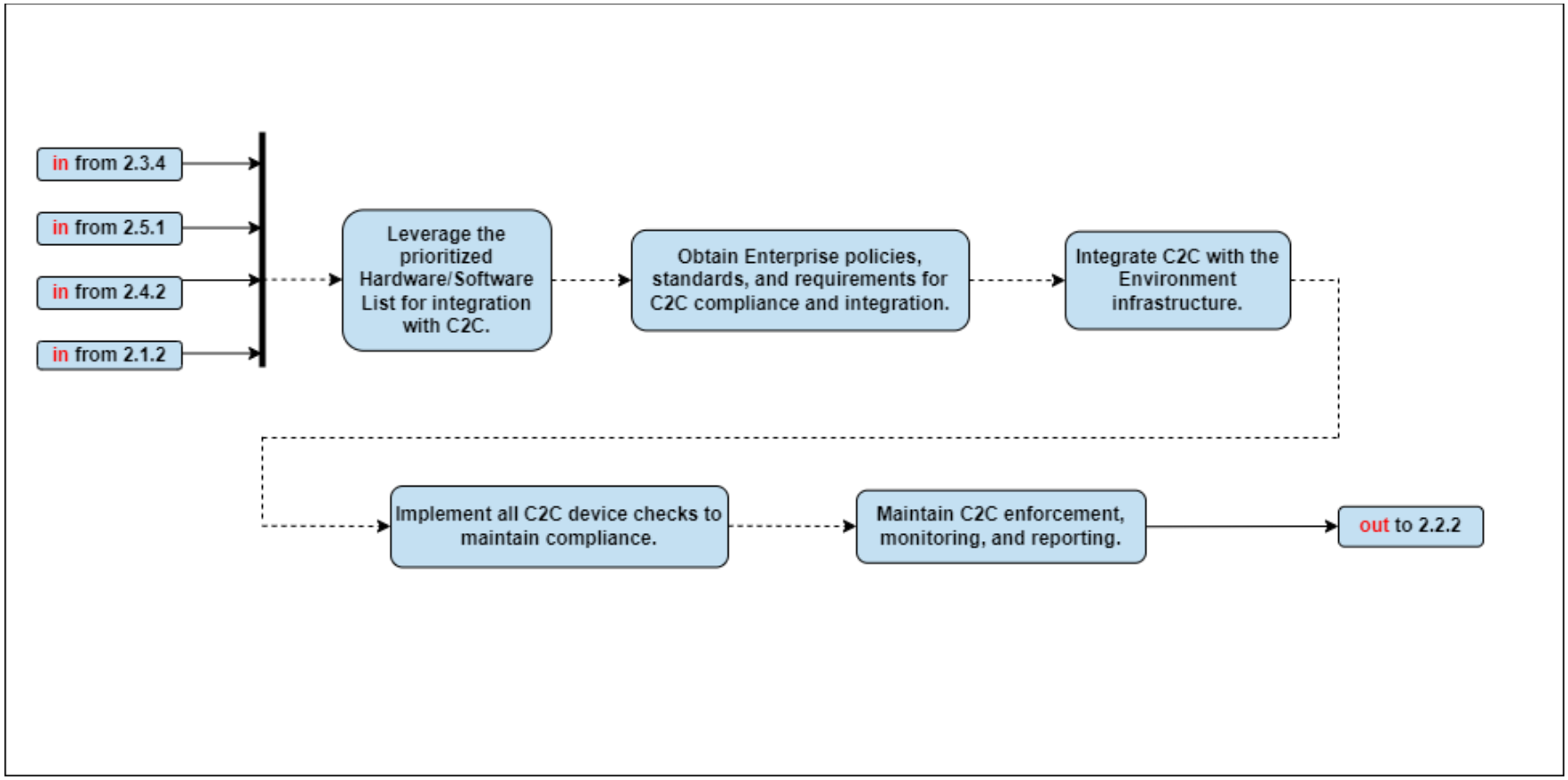

Figure D- 18: Implementation Tasks for Activity 2.2.1 — Implement Comply-to-Connect (C2C) and Compliance-Based Network Authorization Part 1

Activity 2.3.3 Implement Application Control and File Integrity Monitoring (FIM) Tools

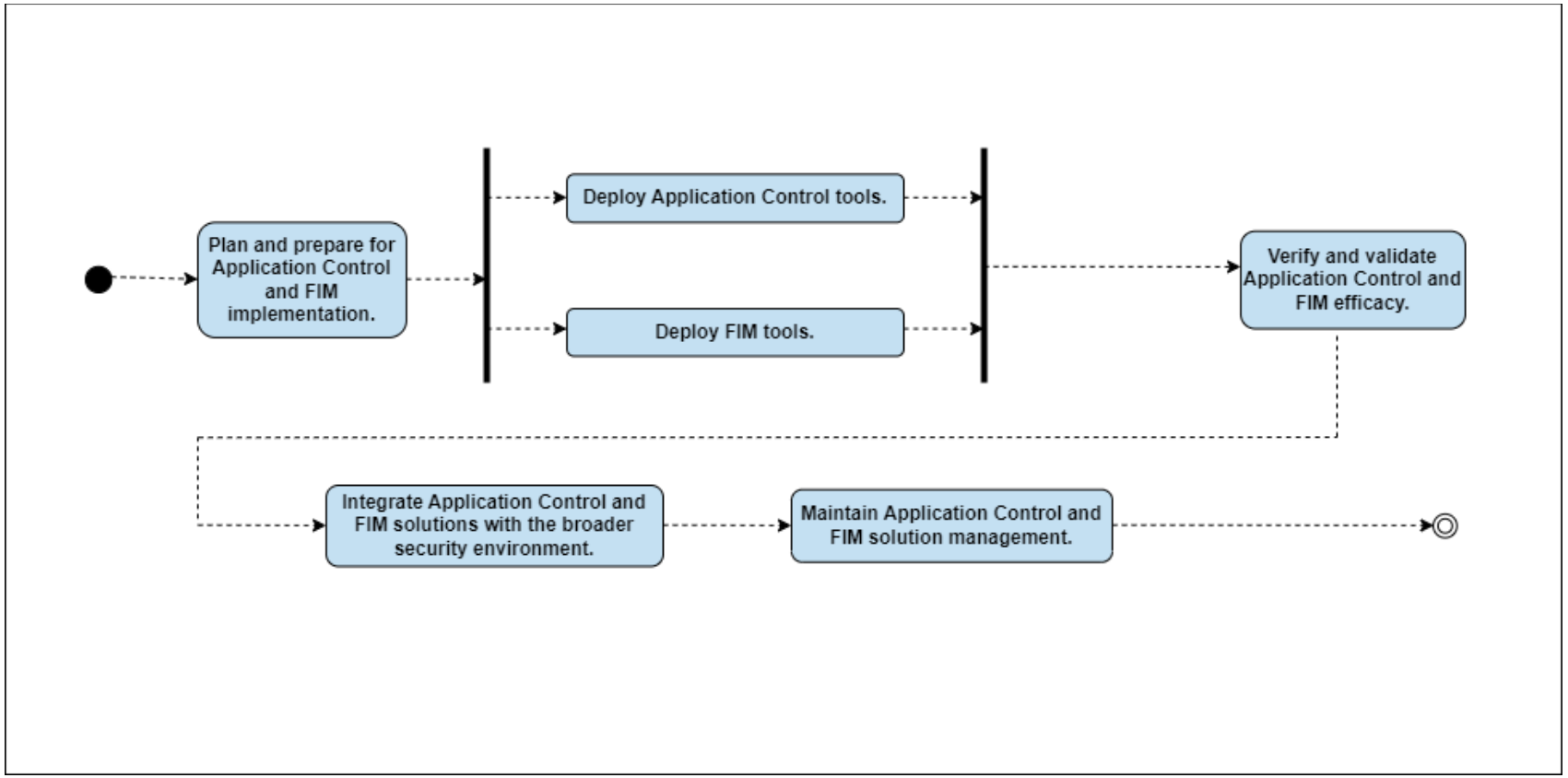

Figure D- 19: Implementation Tasks for Activity 2.3.3 — Implement Application Control and File Integrity Monitoring (FIM) Tools

Activity 2.3.4 Integrate Next-Generation Antivirus (NextGen AV) Tools with Comply-to-Connect (C2C)

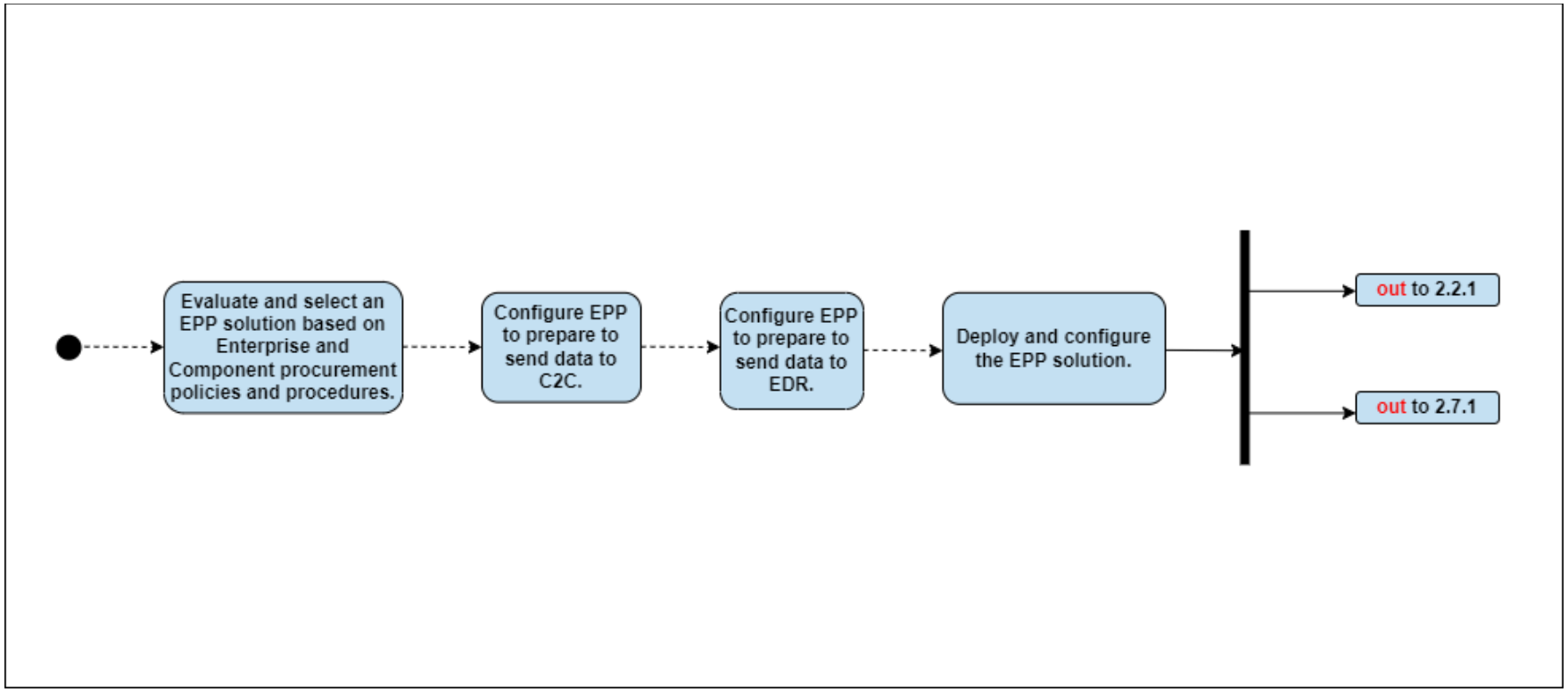

Figure D- 20: Implementation Tasks for Activity 2.3.4 — Integrate Next-Generation Antivirus (NextGen AV) Tools with Comply-to-Connect (C2C)

Activity 2.4.1 Deny Device by Default Policy

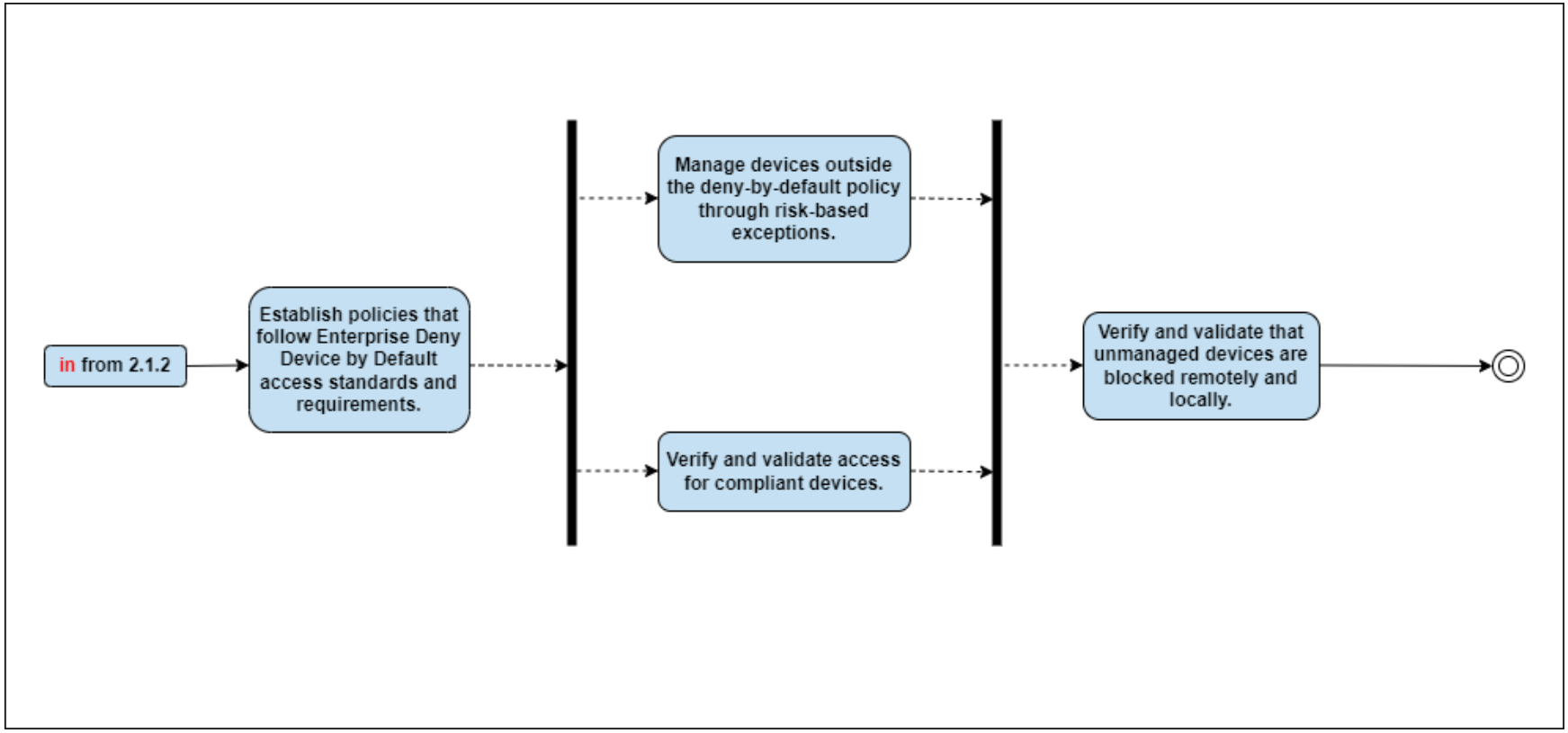

Figure D- 21: Implementation Tasks for Activity 2.4.1 — Deny Device by Default Policy

Activity 2.4.2 Managed and Limited Bring Your Own Device (BYOD) and Internet of Things (IoT) Support

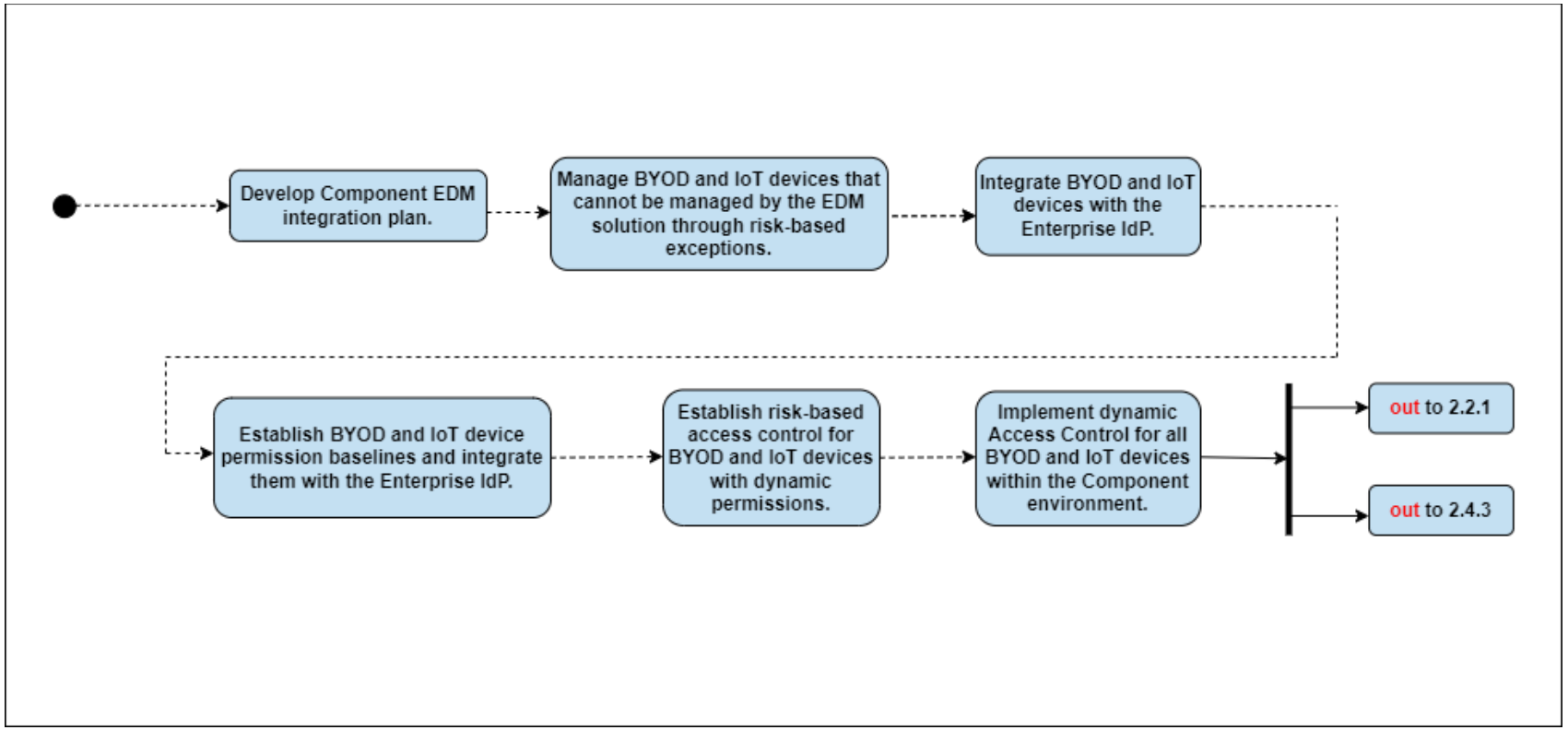

Figure D- 22: Implementation Tasks for Activity 2.4.2 — Managed and Limited Bring Your Own Device (BYOD) and Internet of Things (IoT) Support

Activity 2.5.1 Implement Asset, Vulnerability, and Patch Management Tools

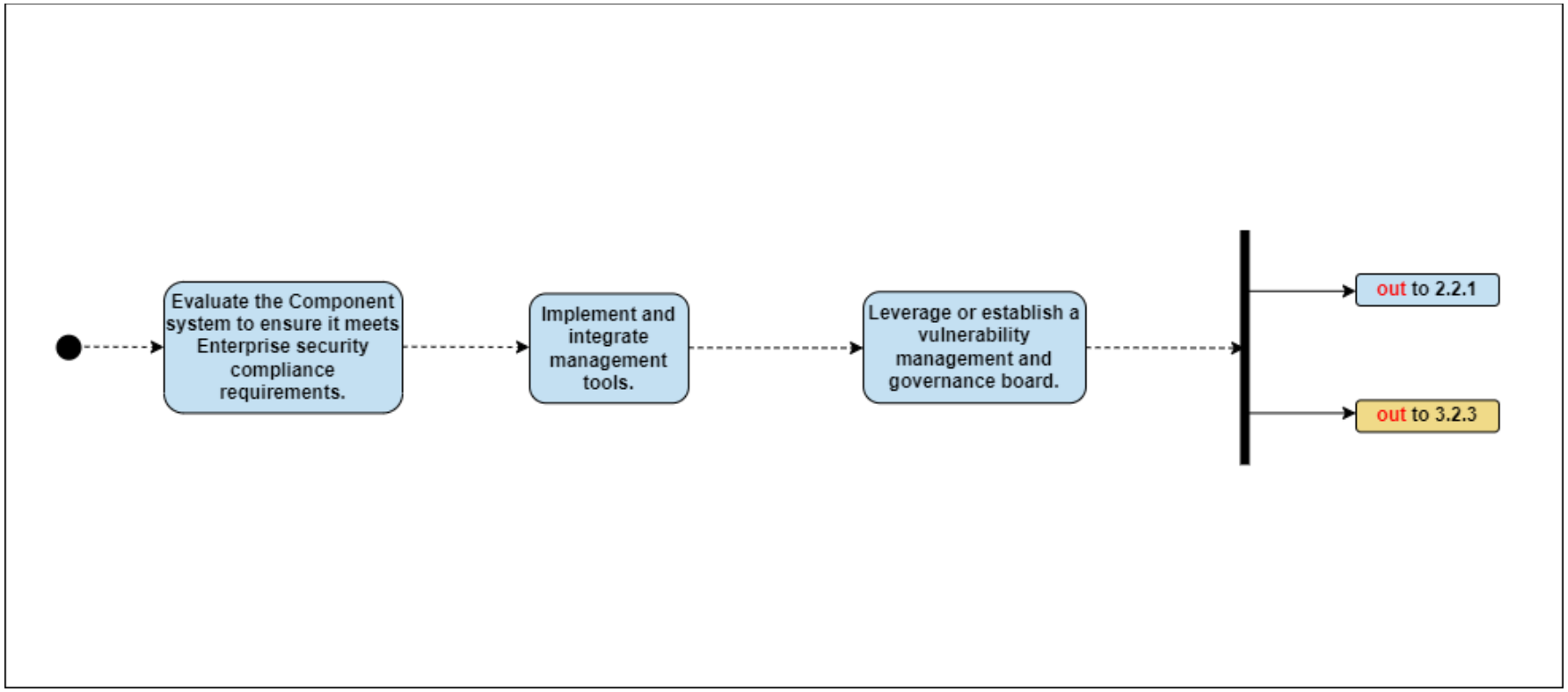

Figure D- 23: Implementation Tasks for Activity 2.5.1 — Implement Asset, Vulnerability, and Patch Management Tools

Activity 2.6.1 Implement Unified Endpoint and Device Management (UEDM) or Equivalent Tools

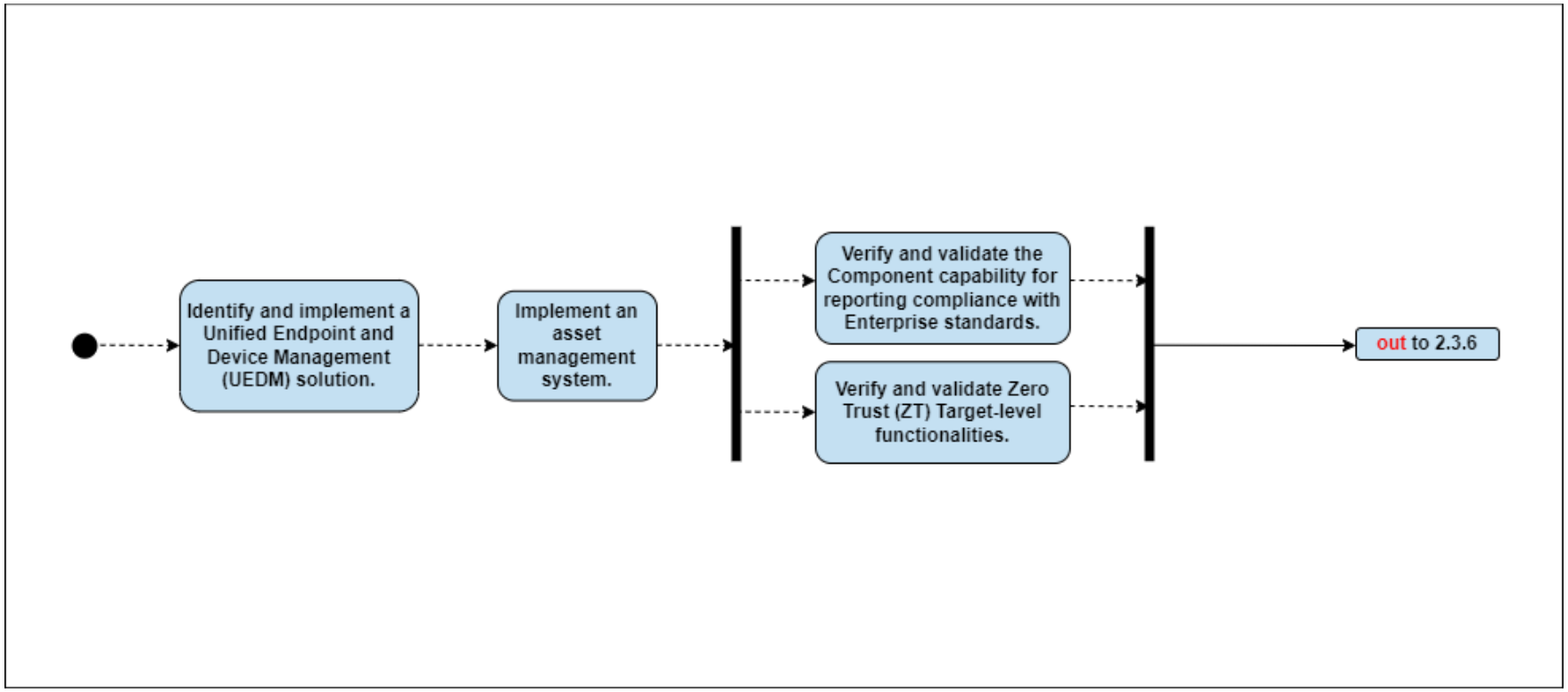

Figure D- 24: Implementation Tasks for Activity 2.6.1 — Implement Unified Endpoint and Device Management (UEDM) or Equivalent Tools

Activity 2.6.2 Enterprise Device Management (EDM) Part 1

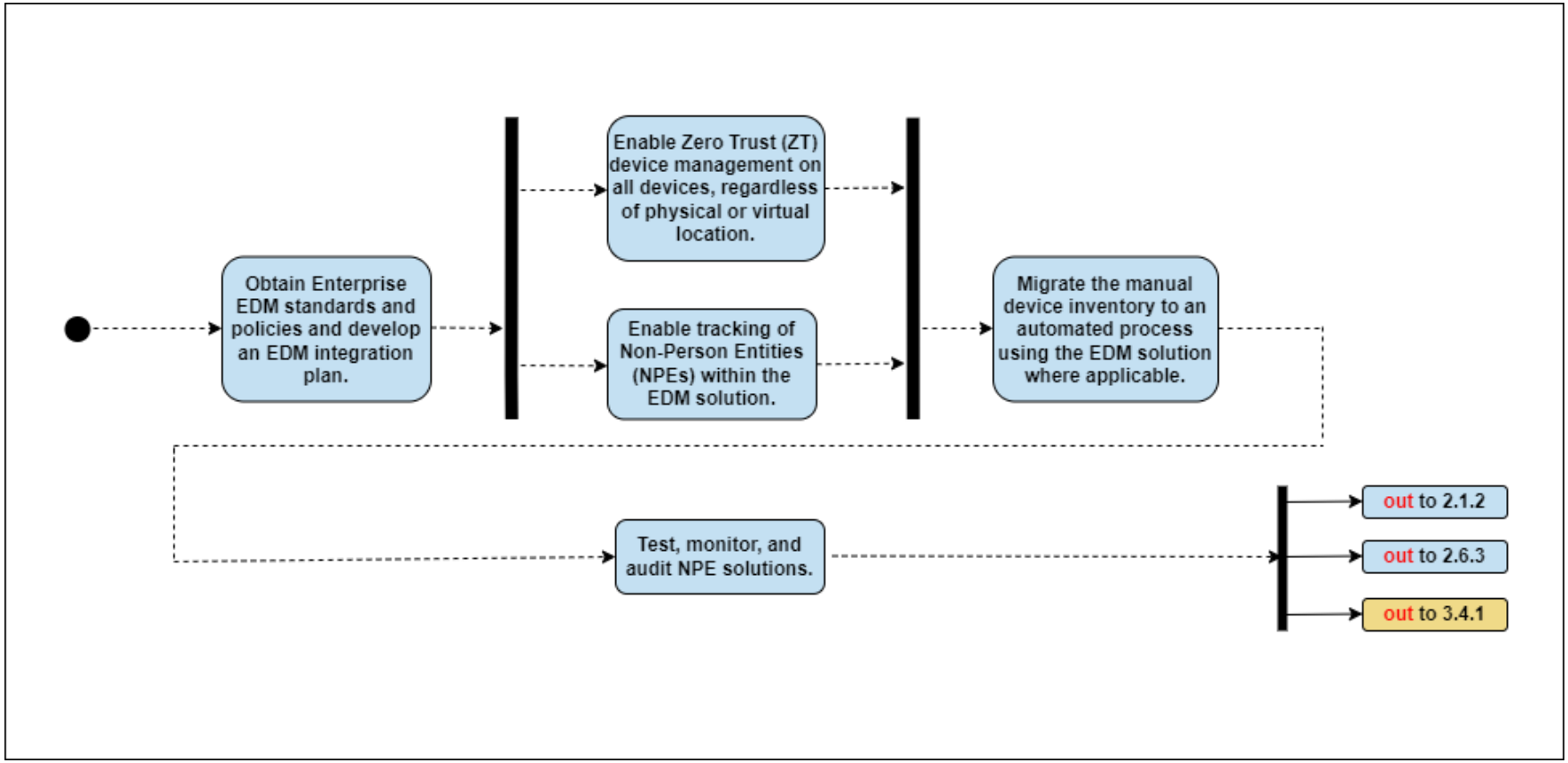

Figure D- 25: Implementation Tasks for Activity 2.6.2 — Enterprise Device Management (EDM) Part 1

Activity 2.6.3 Enterprise Device Management (EDM) Part 2

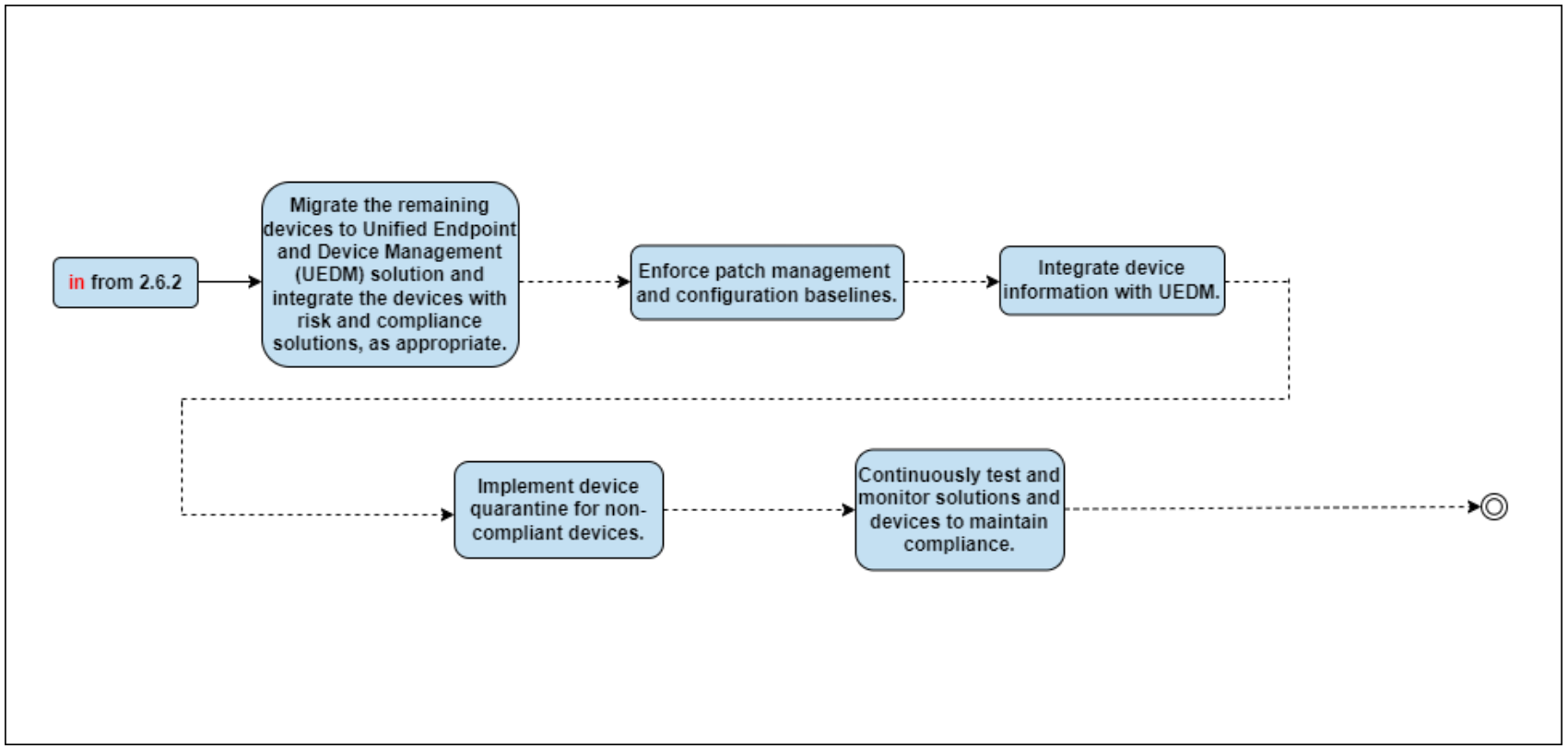

Figure D- 26: Implementation Tasks for Activity 2.6.3 — Enterprise Device Management (EDM) Part 2

Activity 2.7.1 Implement Endpoint Detection and Response (EDR) Tools and Integrate with Comply-to-Connect (C2C)

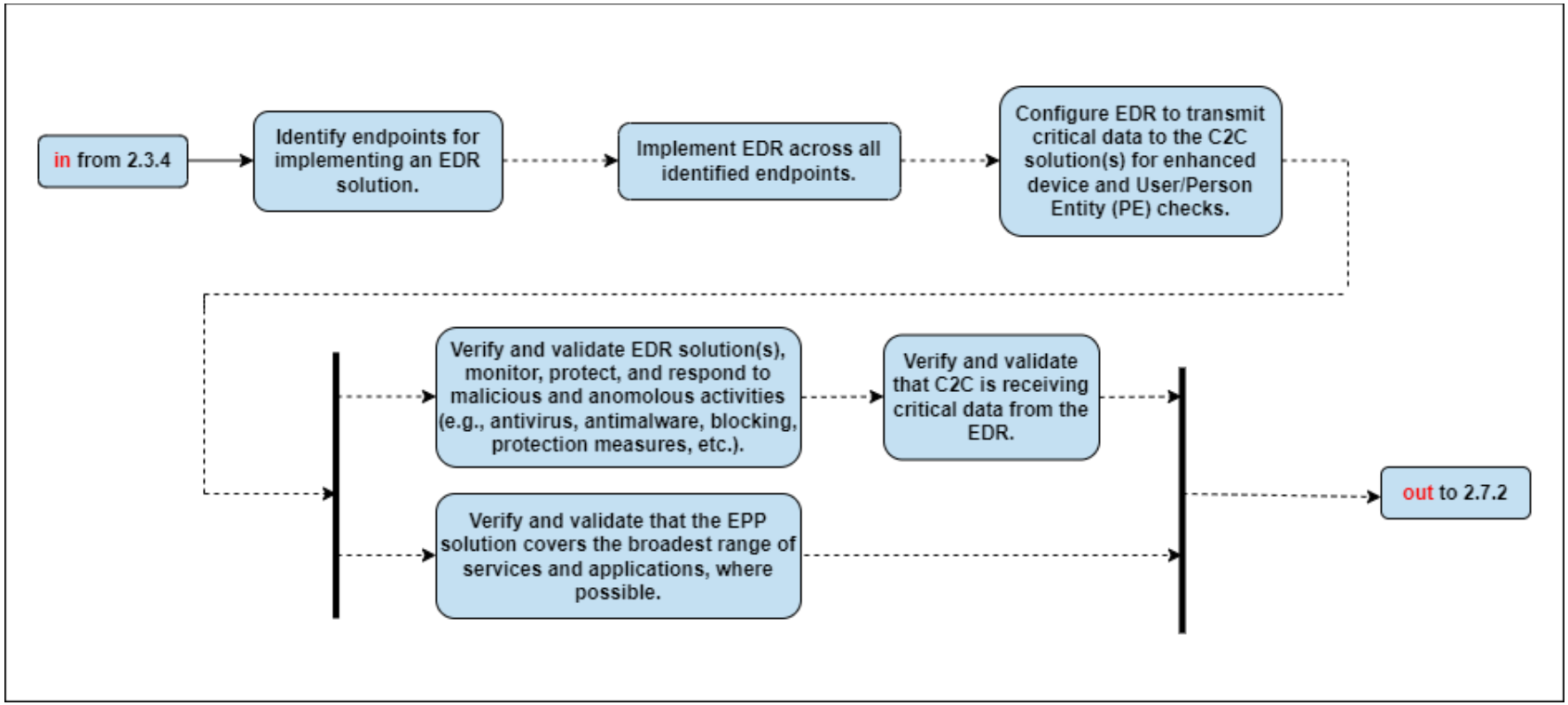

Figure D- 27: Implementation Tasks for Activity 2.7.1 — Implement Endpoint Detection and Response (EDR) Tools and Integrate with Comply-to-Connect (C2C)

Activity 2.7.2 Implement Extended Detection and Response (XDR) Tools and Integrate with Comply-to-Connect (C2C) Part 1

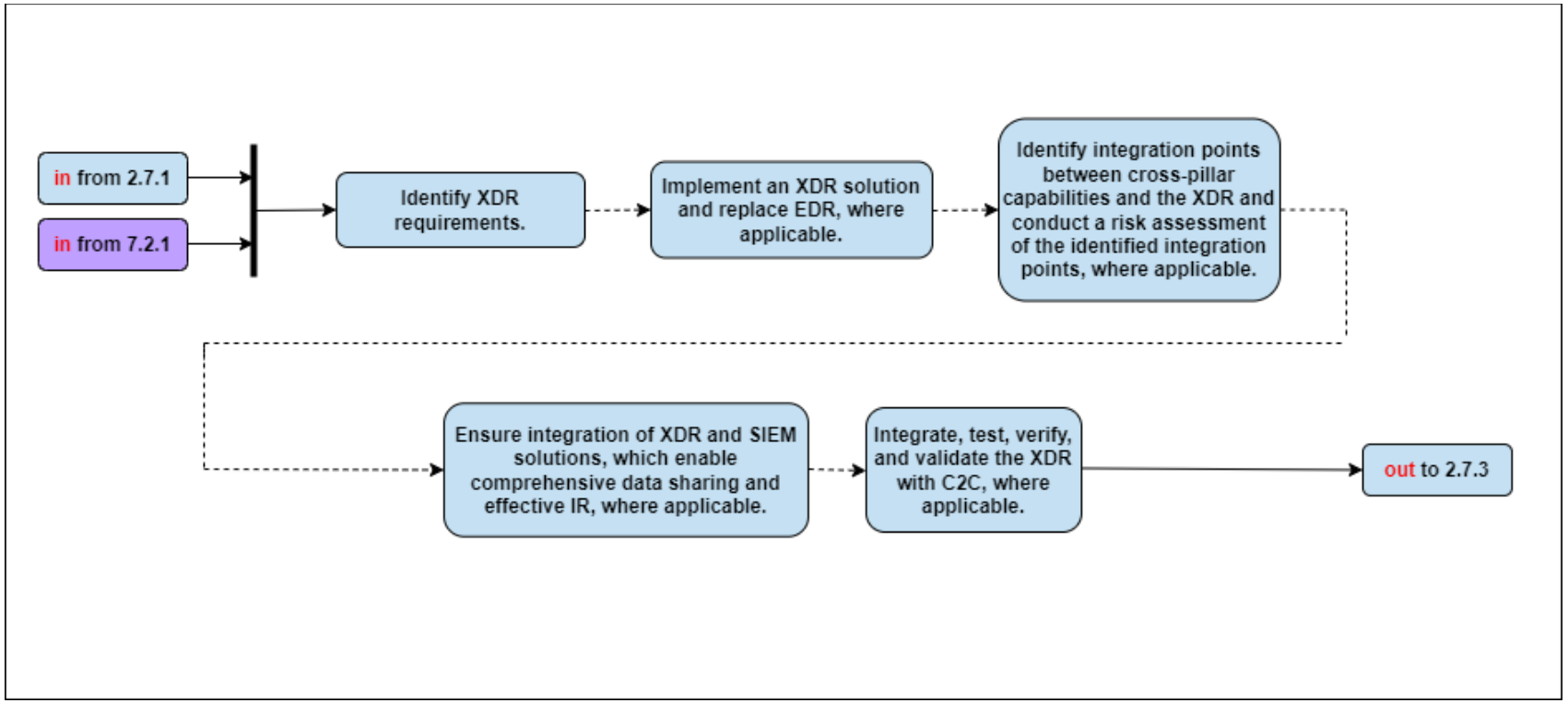

Figure D- 28: Implementation Tasks for Activity 2.7.2 — Implement Extended Detection and Response (XDR) Tools and Integrate with Comply-to-Connect (C2C) Part 1

Activity 3.1.1 Application and Code Identification

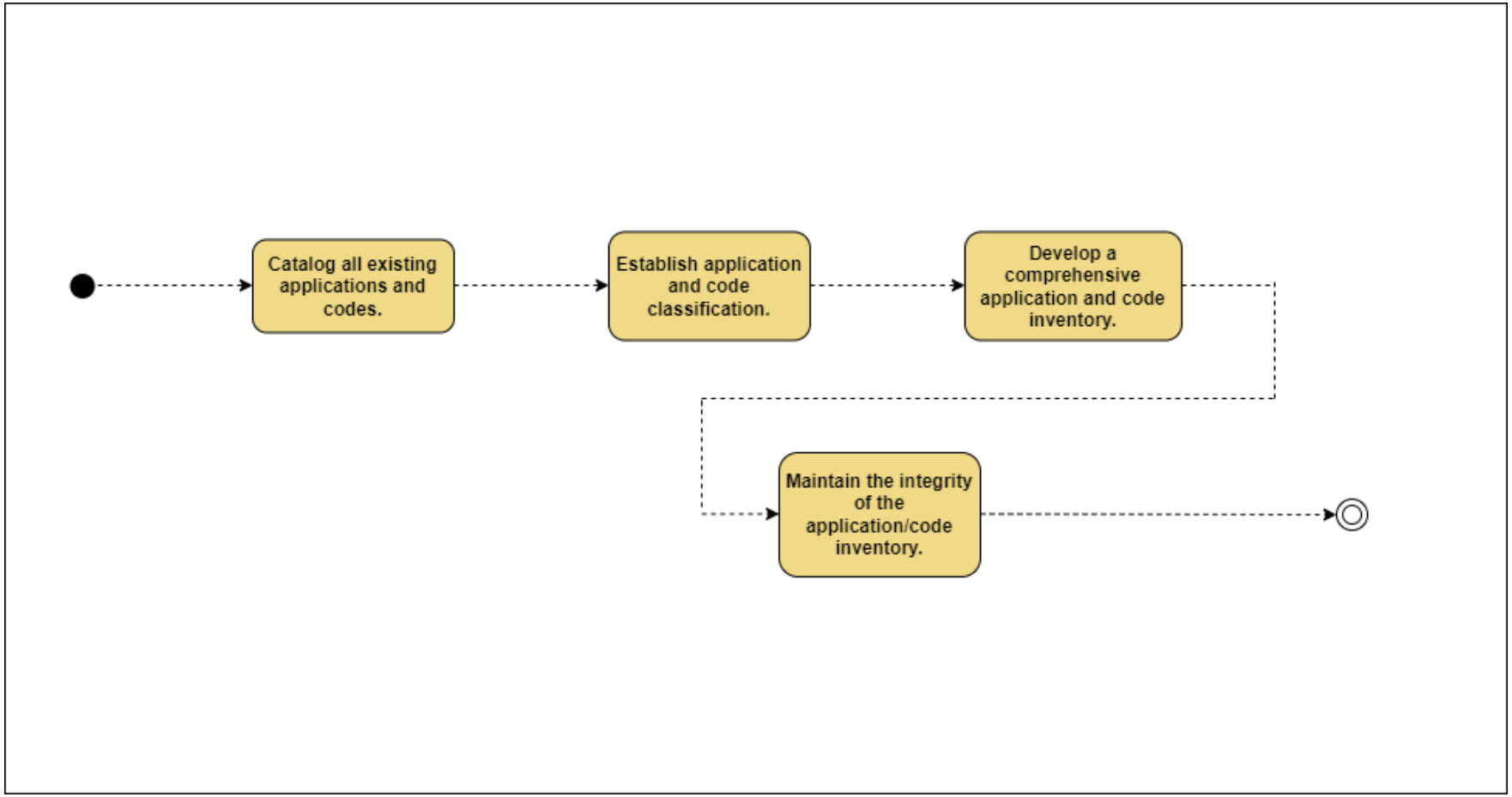

Figure D- 29: Implementation Tasks for Activity 3.1.1 — Application and Code Identification

Activity 3.2.1 Build Development, Security, and Operations (DevSecOps) Software Factory Part 1

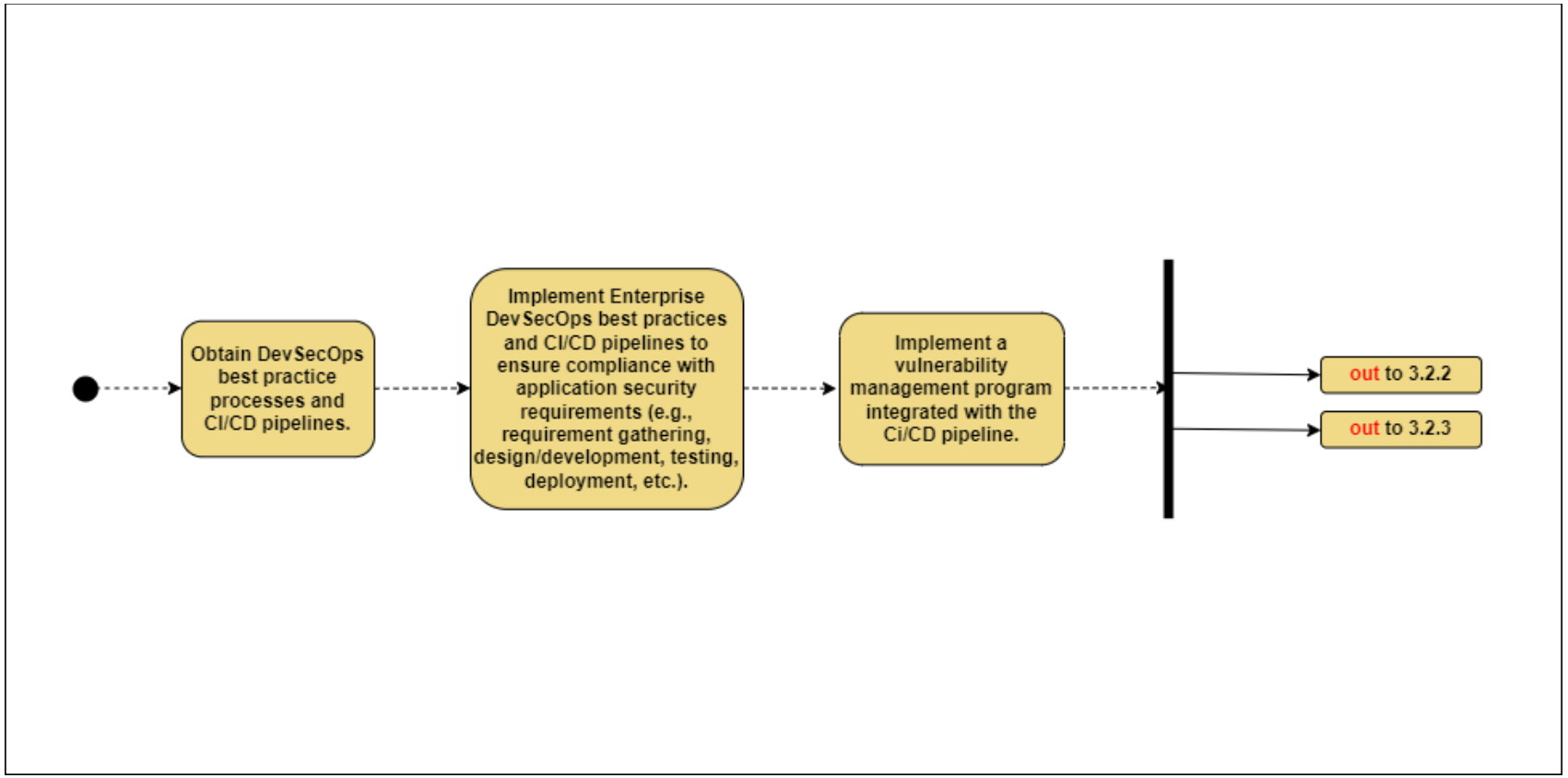

Figure D- 30: Implementation Tasks for Activity 3.2.1 — Build Development, Security, and Operations (DevSecOps) Software Factory Part 1

Activity 3.2.2 Build Development, Security, and Operations (DevSecOps) Software Factory Part 2

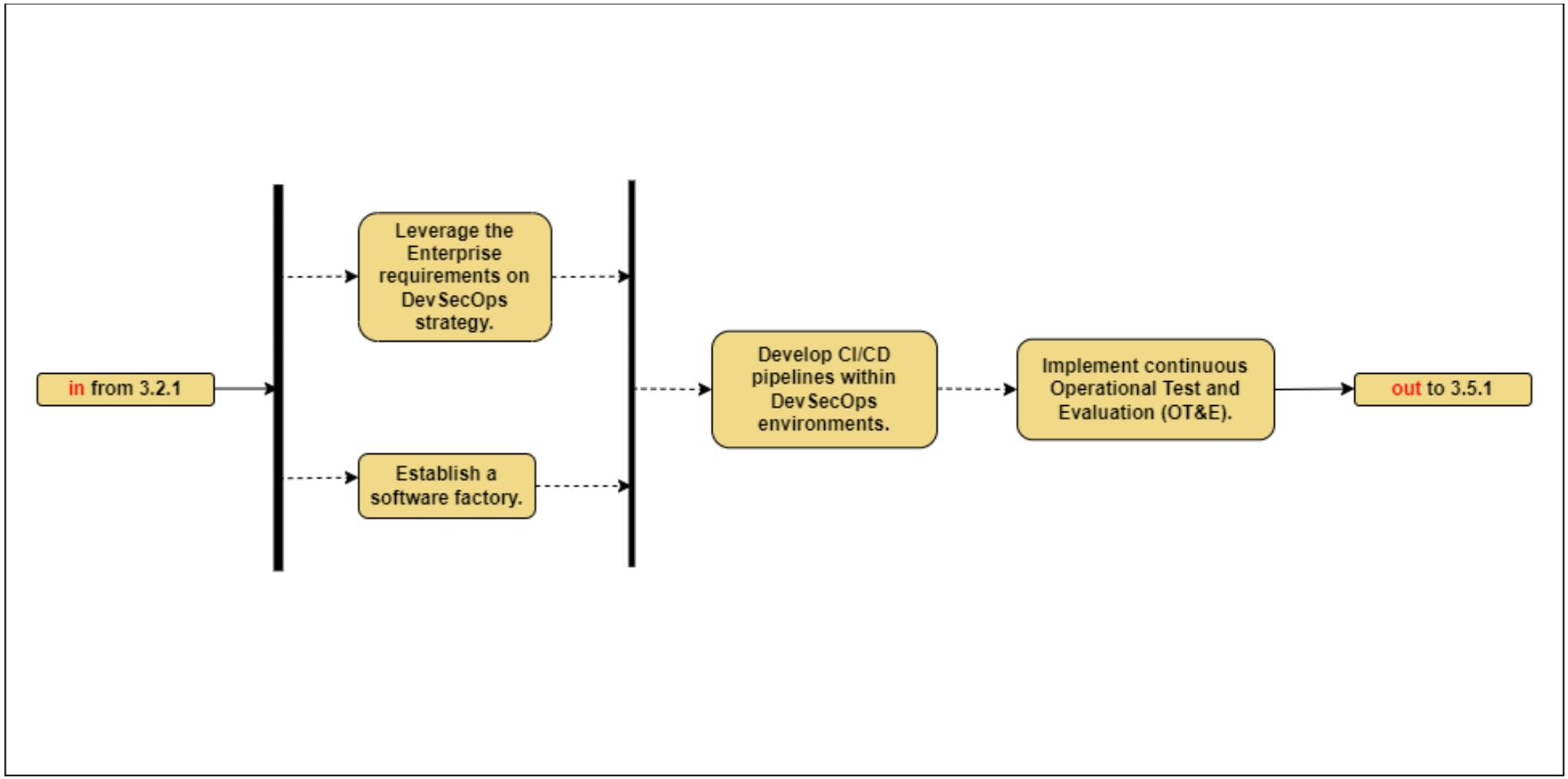

Figure D- 31: Implementation Tasks for Activity 3.2.2 — Build Development, Security, and Operations (DevSecOps) Software Factory Part 2

Activity 3.2.3 Automate Application Security and Code Remediation Part 1

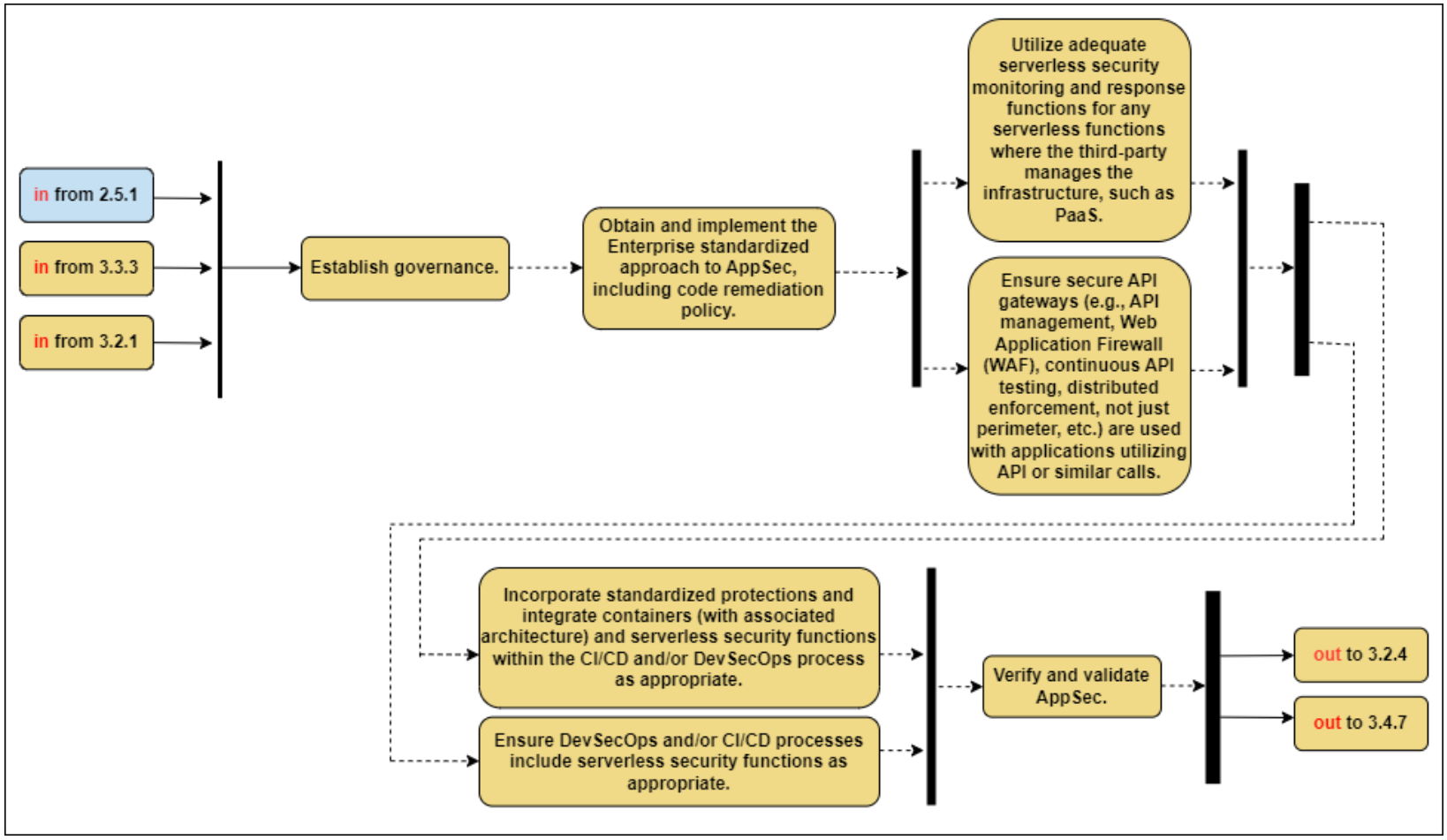

Figure D- 32: Implementation Tasks for Activity 3.2.3 — Automate Application Security and Code Remediation Part 1

Activity 3.3.1 Approved Binaries and Code

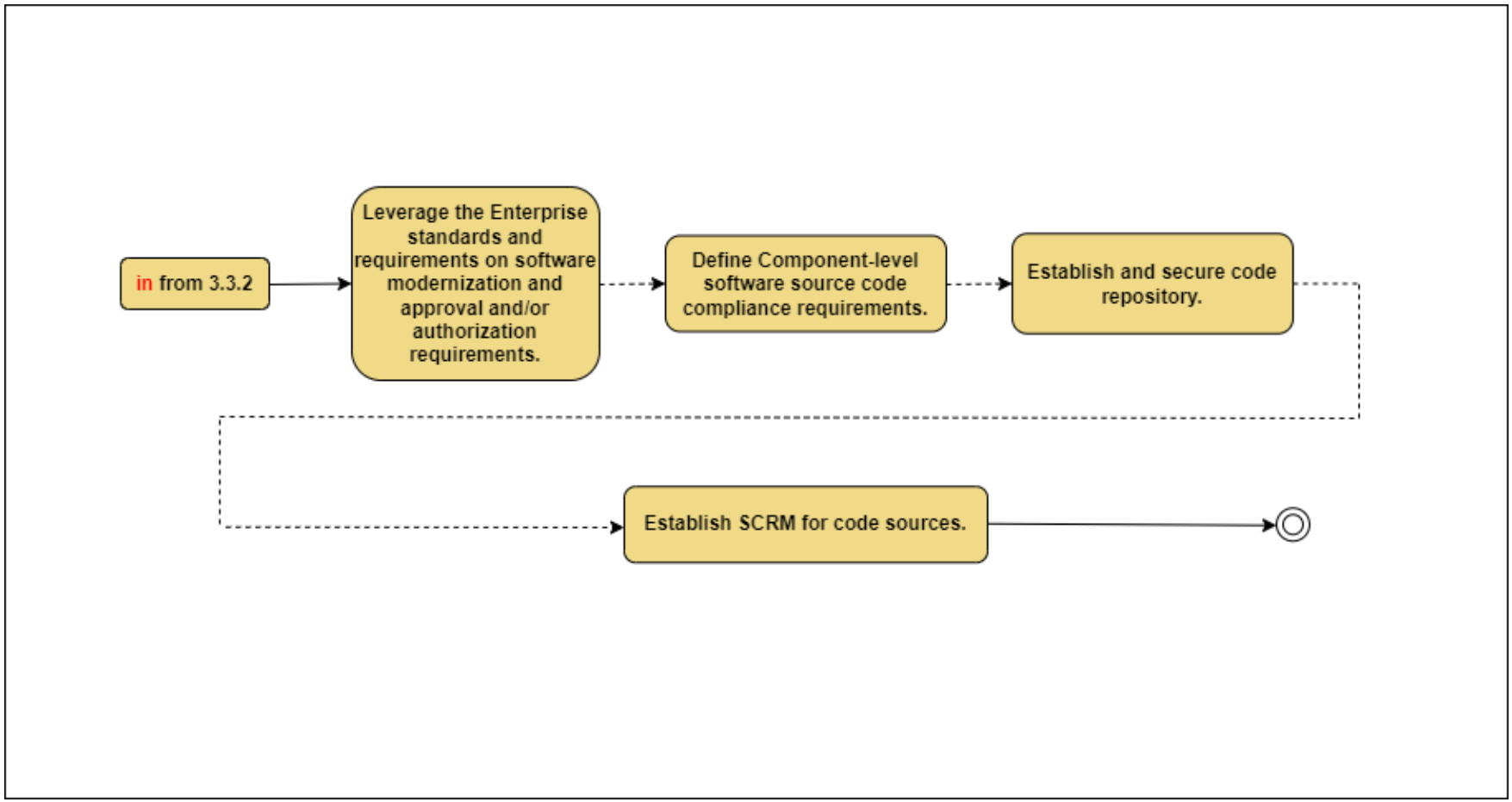

Figure D- 33: Implementation Tasks for Activity 3.3.1 — Approved Binaries and Code

Activity 3.3.2 Vulnerability Management Program Part 1

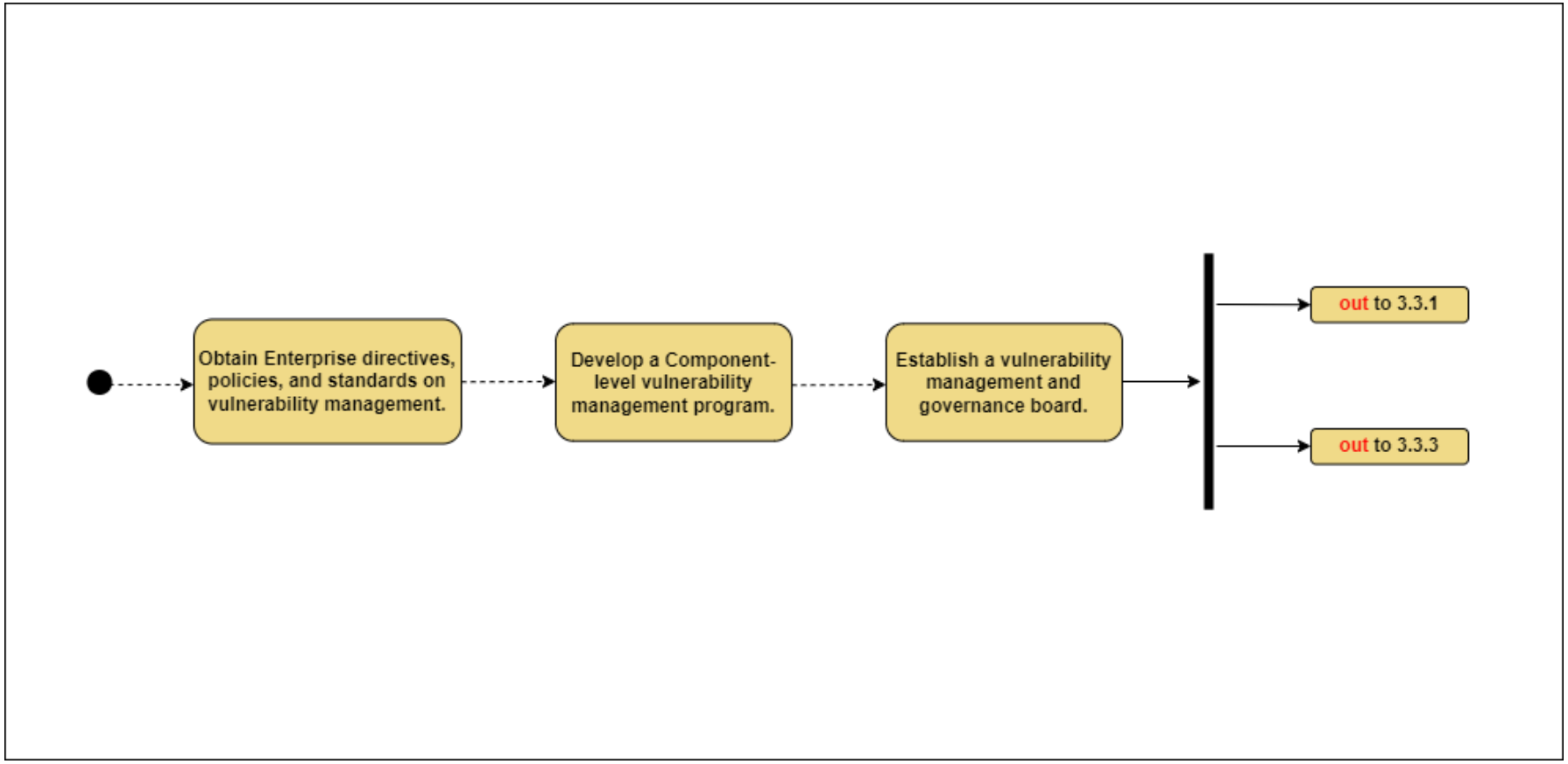

Figure D- 34: Implementation Tasks for Activity 3.3.2 — Vulnerability Management Program Part 1

Activity 3.3.3 Vulnerability Management Program Part 2

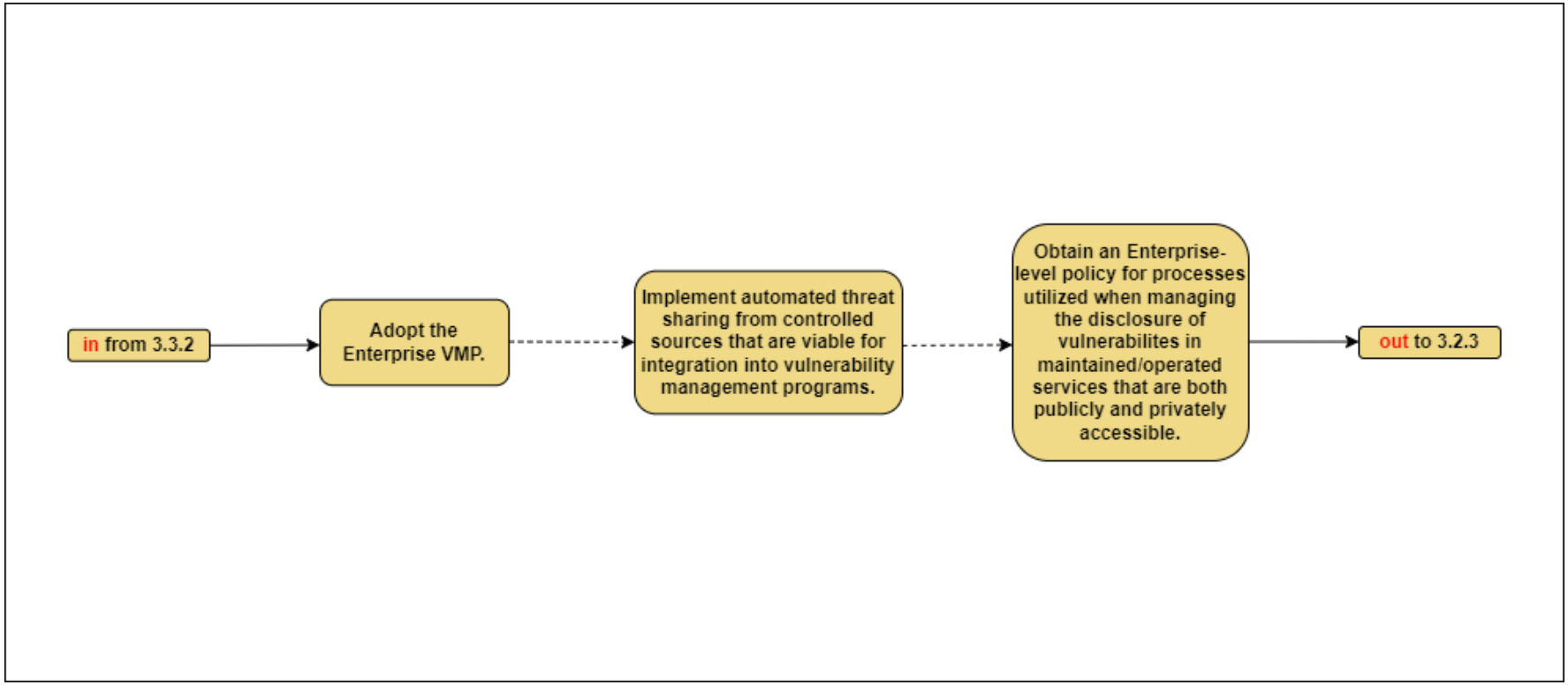

Figure D- 35: Implementation Tasks for Activity 3.3.3 — Vulnerability Management Program Part 2

Activity 3.3.4 Continual Validation

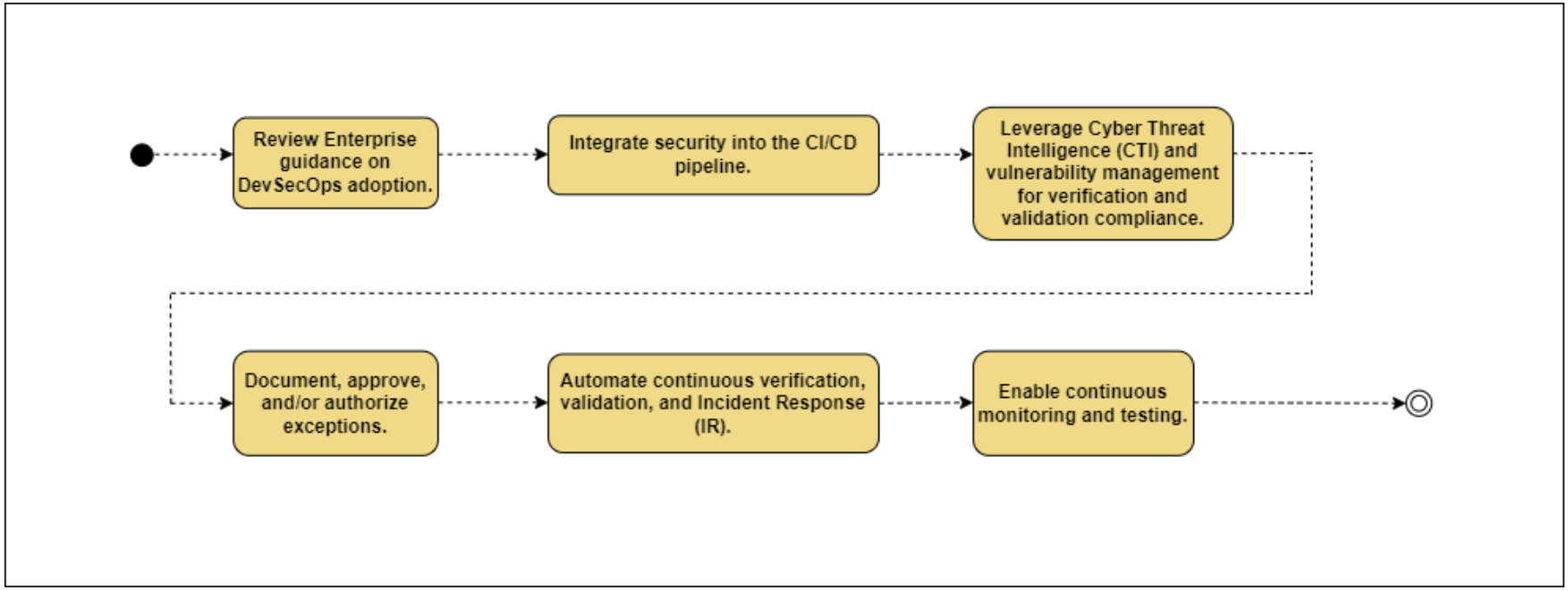

Figure D- 36: Implementation Tasks for Activity 3.3.4 — Continual Validation

Activity 3.4.1 Resource Authorization Part 1

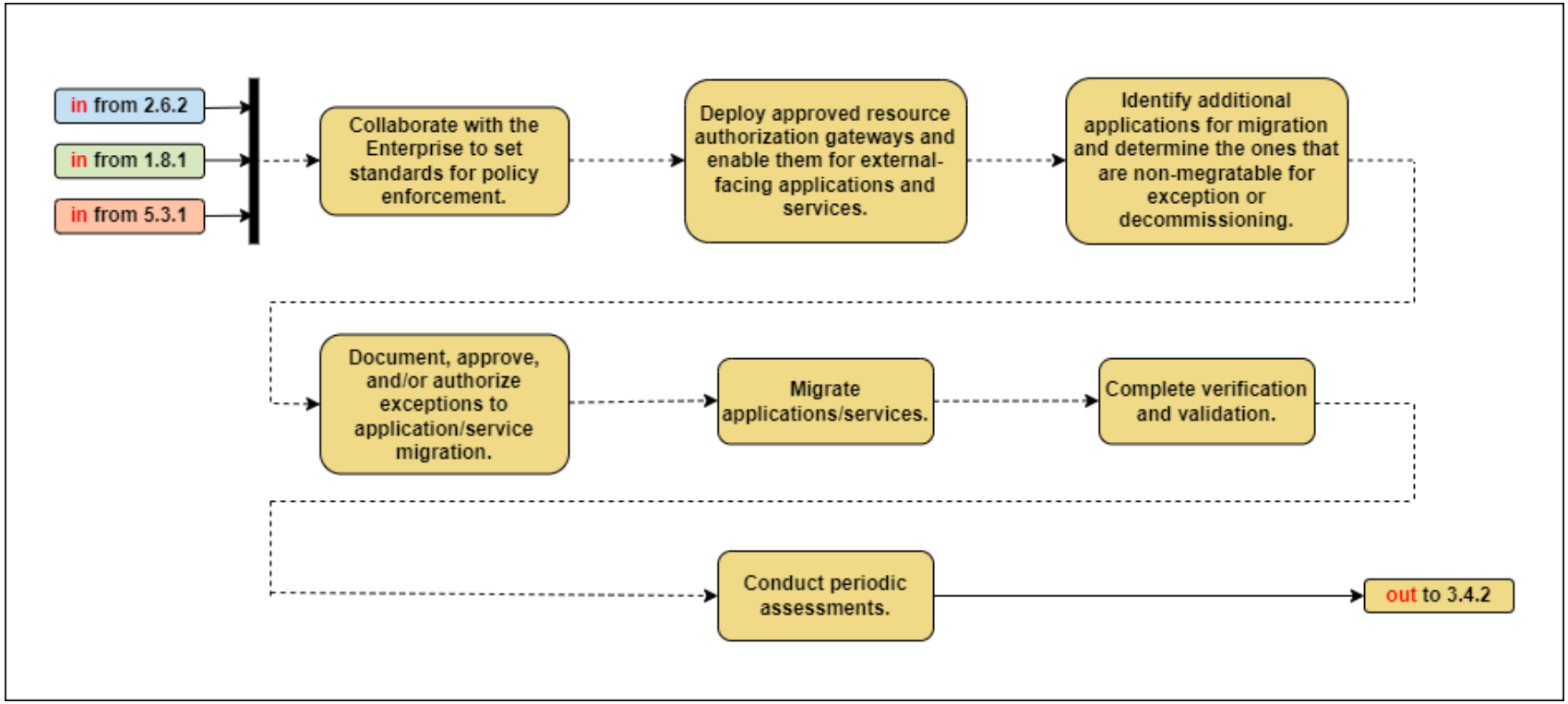

Figure D- 37: Implementation Tasks for Activity 3.4.1 — Resource Authorization Part 1

Activity 3.4.2 Resource Authorization Part 2

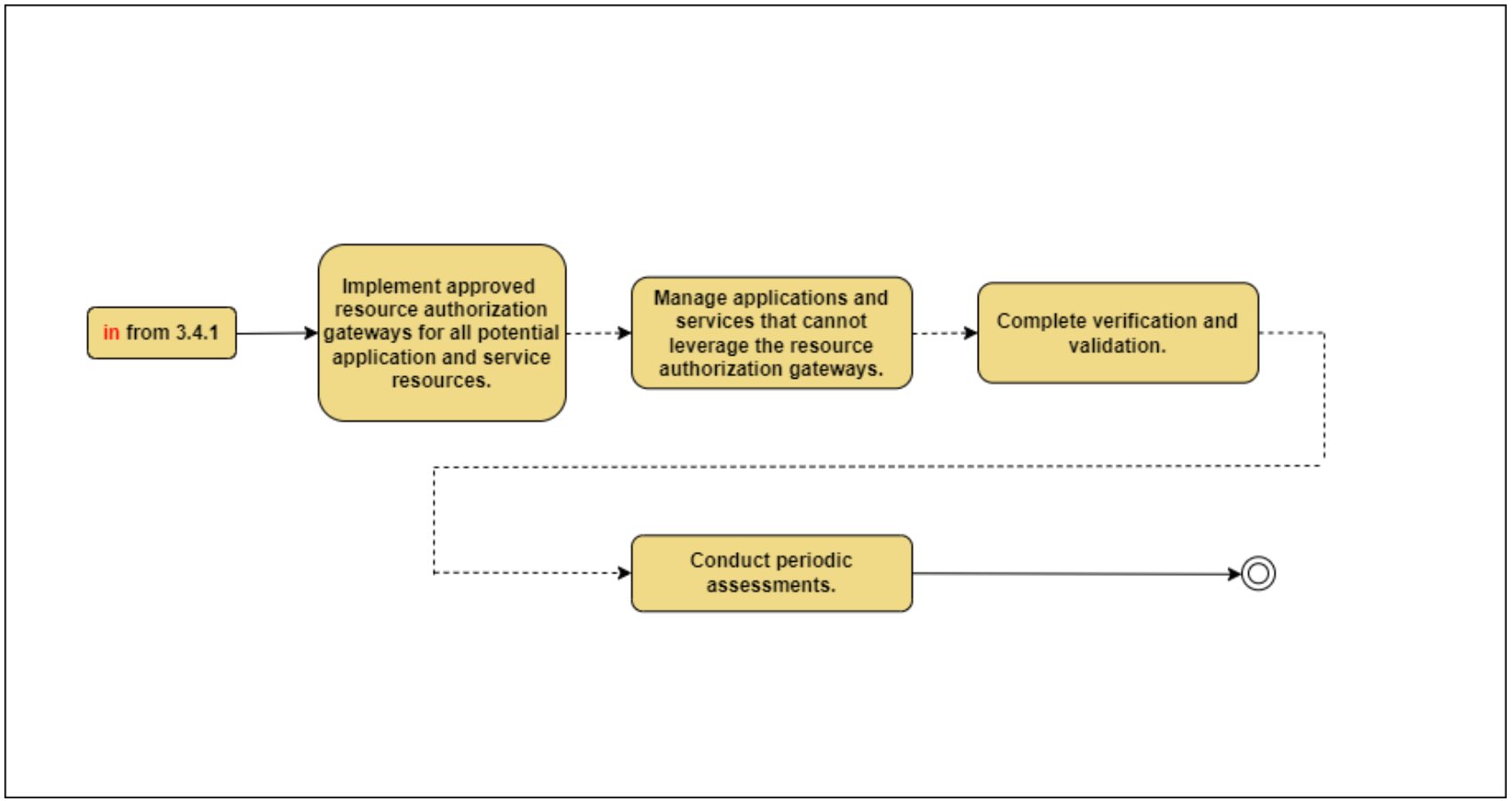

Figure D- 38: Implementation Tasks for Activity 3.4.2 — Resource Authorization Part 2

Activity 3.4.3 Software-Defined Compute (SDC) Resource Authorization Part 1

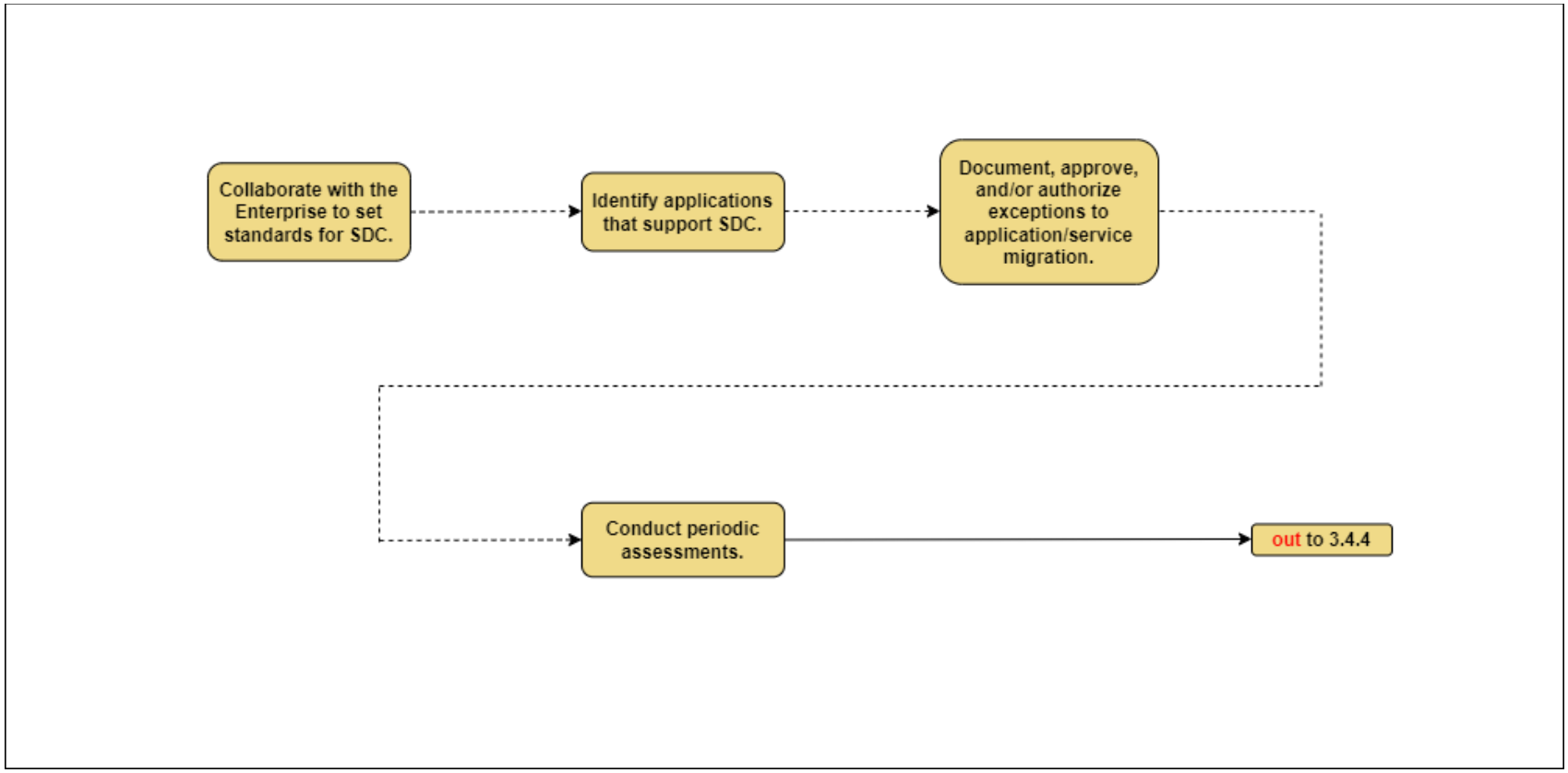

Figure D- 39: Implementation Tasks for Activity 3.4.3 — Software-Defined Compute (SDC) Resource Authorization Part 1

Activity 3.4.4 Software-Defined Compute (SDC) Resource Authorization Part 2

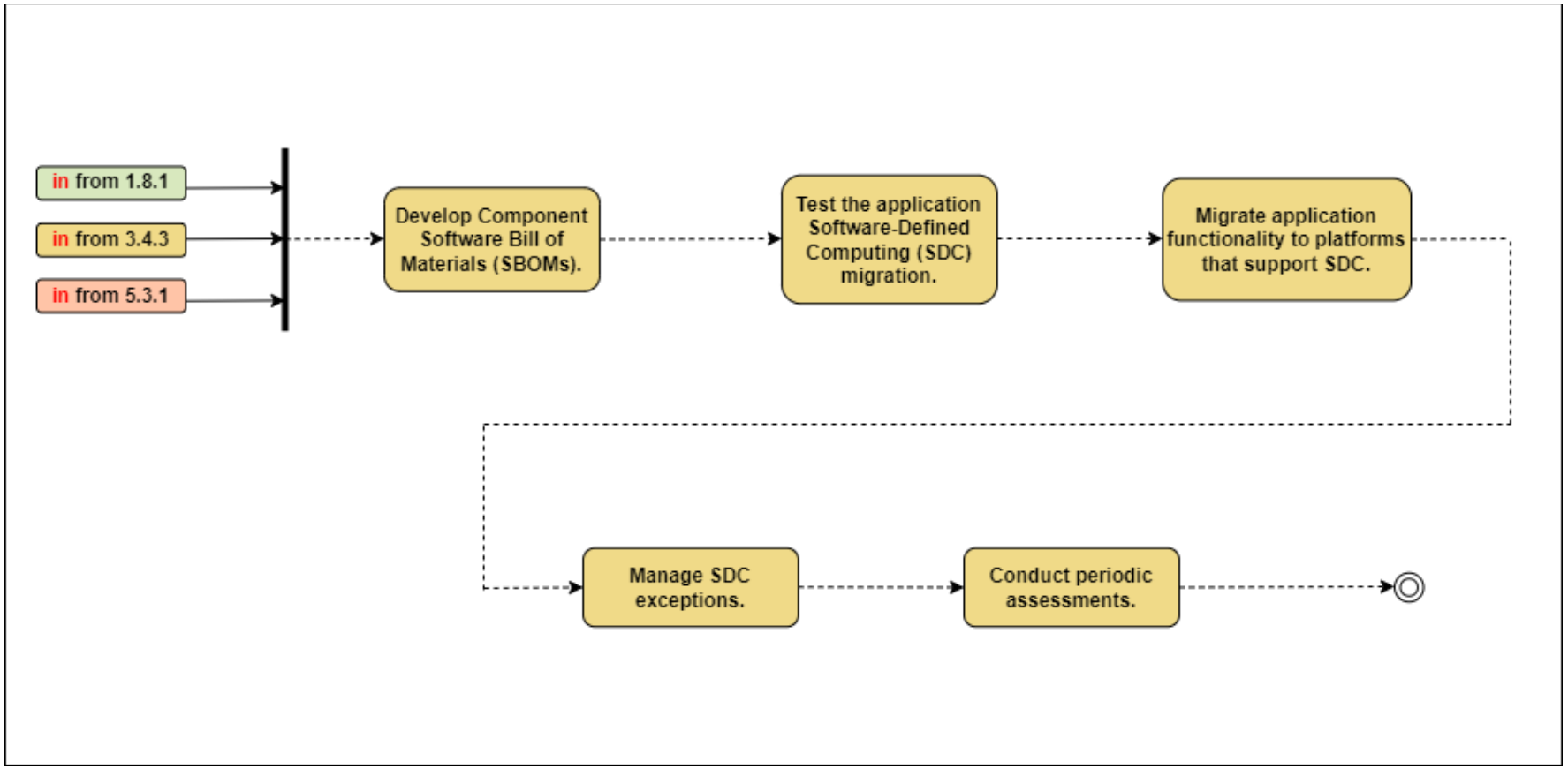

Figure D- 40: Implementation Tasks for Activity 3.4.4 — Software-Defined Compute (SDC) Resource Authorization Part 2

Activity 4.1.1 Data Analysis

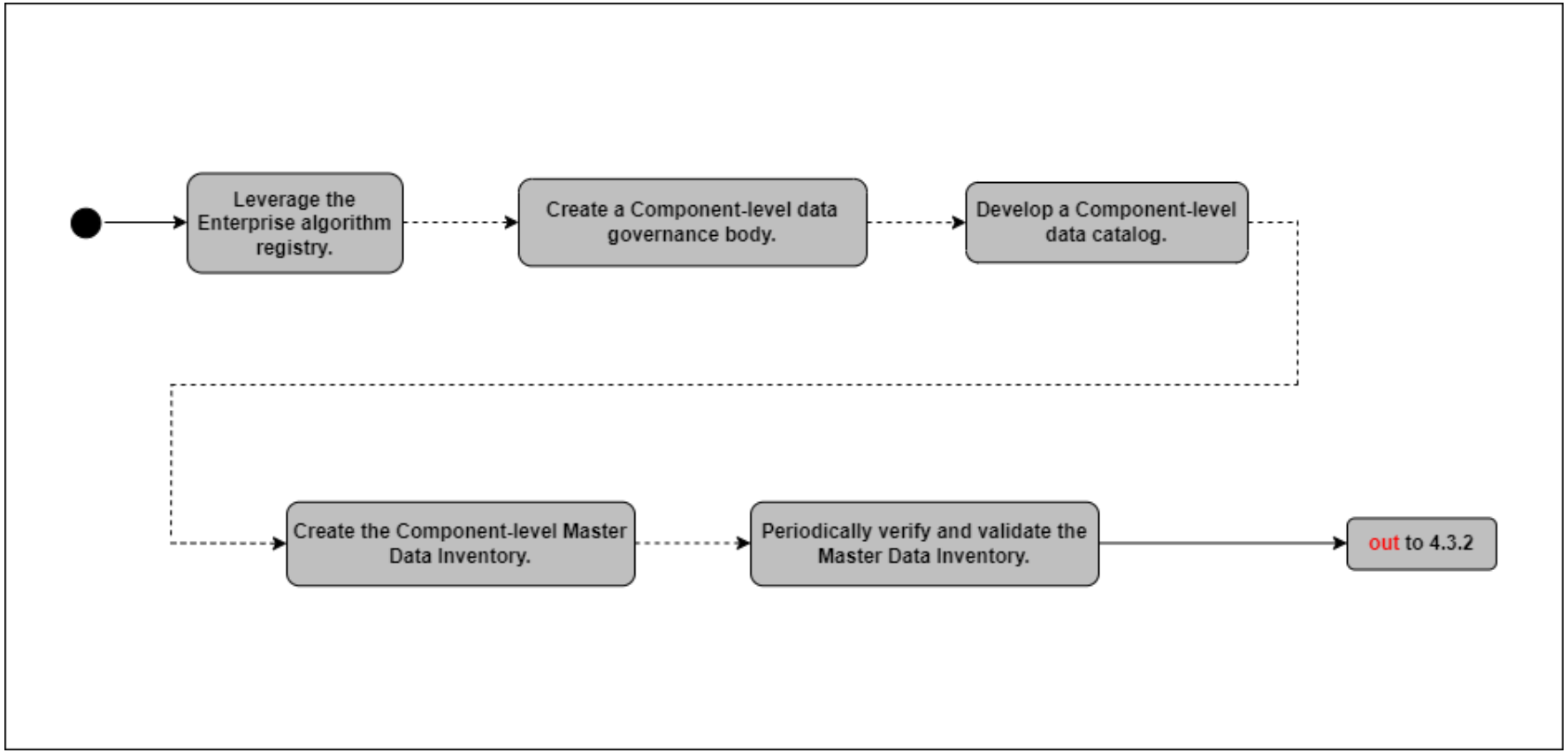

Figure D- 41: Implementation Tasks for Activity 4.1.1 — Data Analysis

Activity 4.2.1 Define Data Tagging Standards

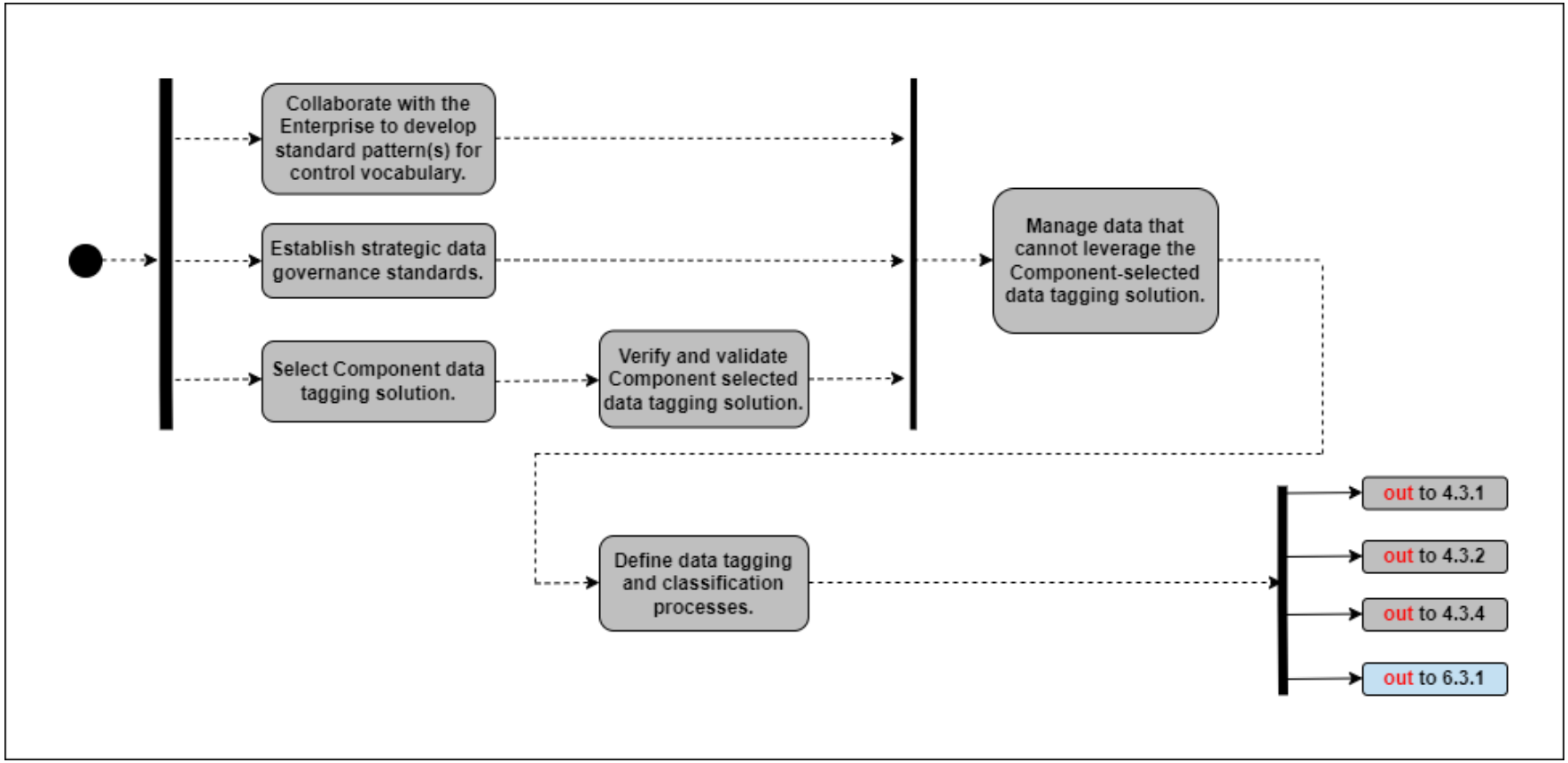

Figure D- 42: Implementation Tasks for Activity 4.2.1 — Define Data Tagging Standards

Activity 4.2.2 Interoperability Standards

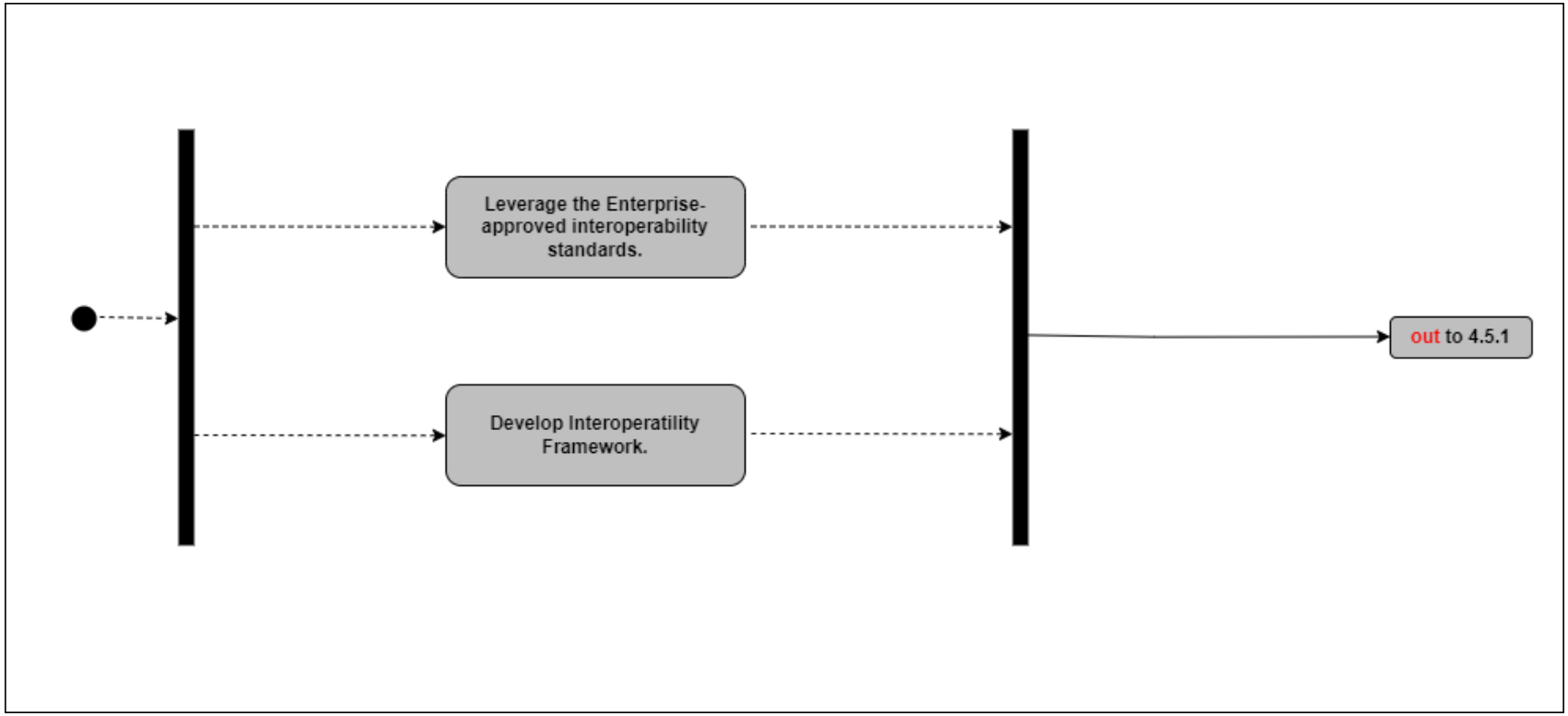

Figure D- 43: Implementation Tasks for Activity 4.2.2 — Interoperability Standards

Activity 4.2.3 Develop Software-Defined Storage (SDS) Policy

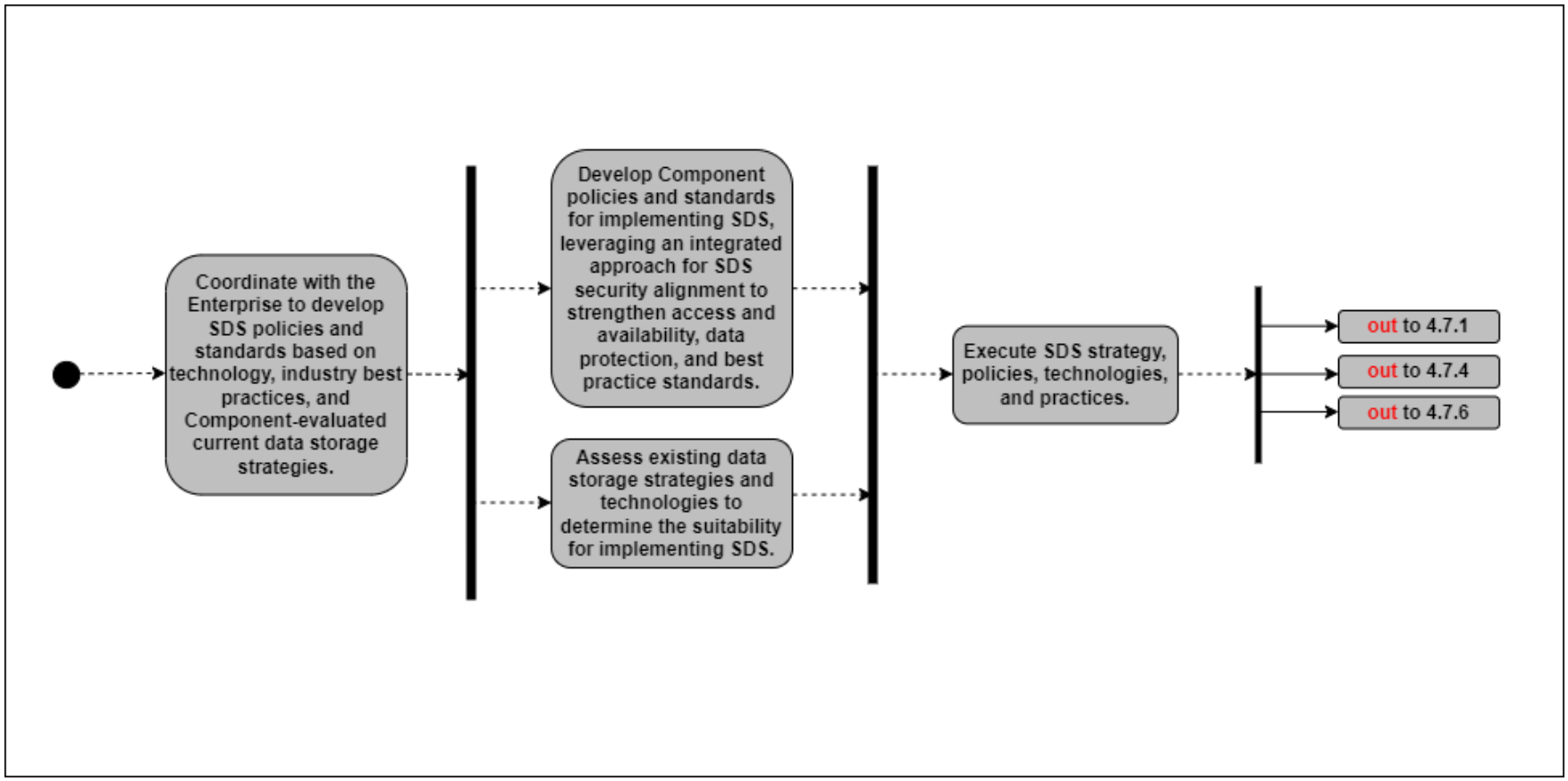

Figure D- 44: Implementation Tasks for Activity 4.2.3 — Develop Software-Defined Storage (SDS) Policy

Activity 4.3.1 Implement Data Tagging and Classification Tools

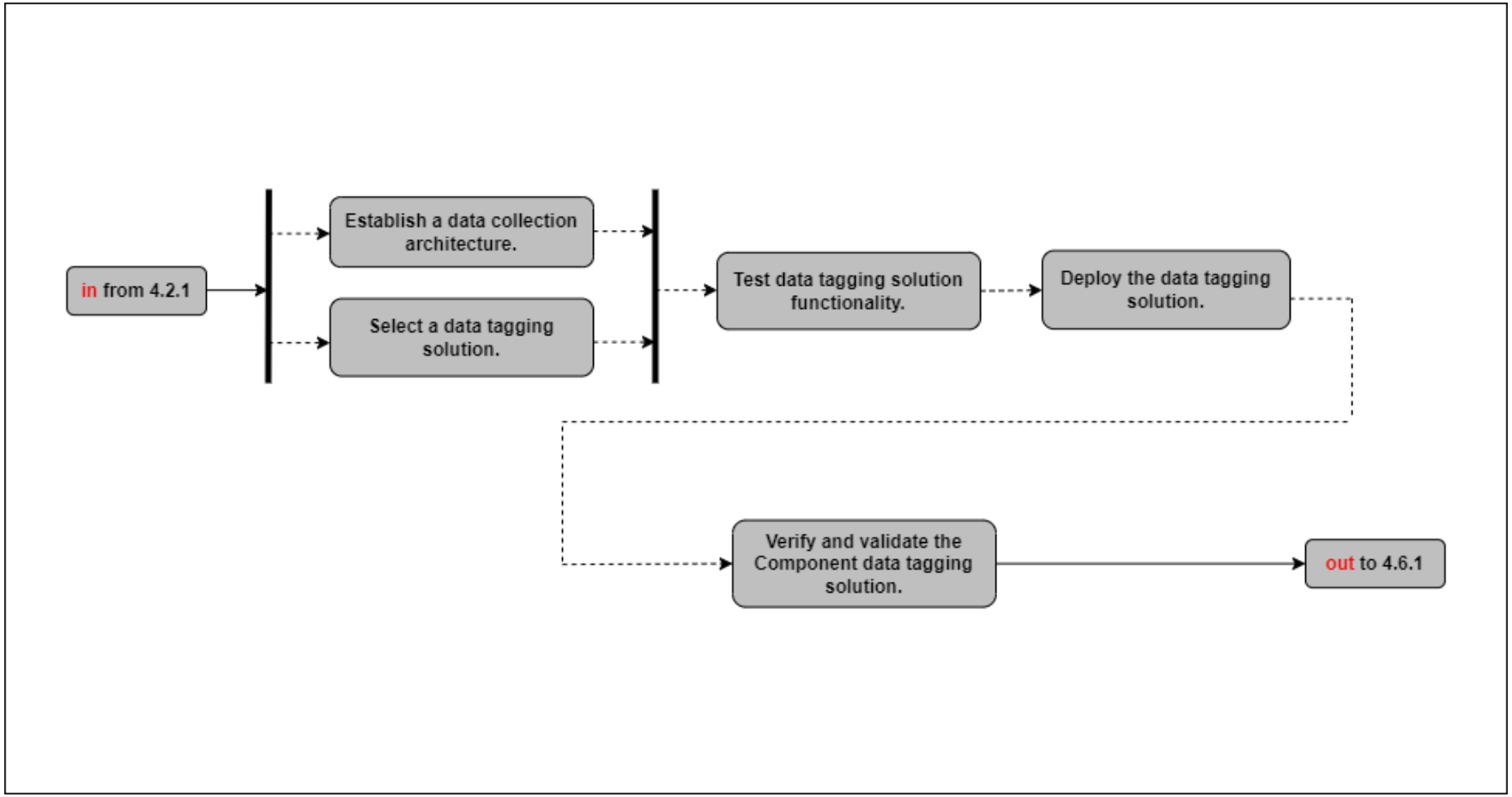

Figure D- 45: Implementation Tasks for Activity 4.3.1 — Implement Data Tagging and Classification Tools

Activity 4.3.2 Manual Data Tagging Part 1

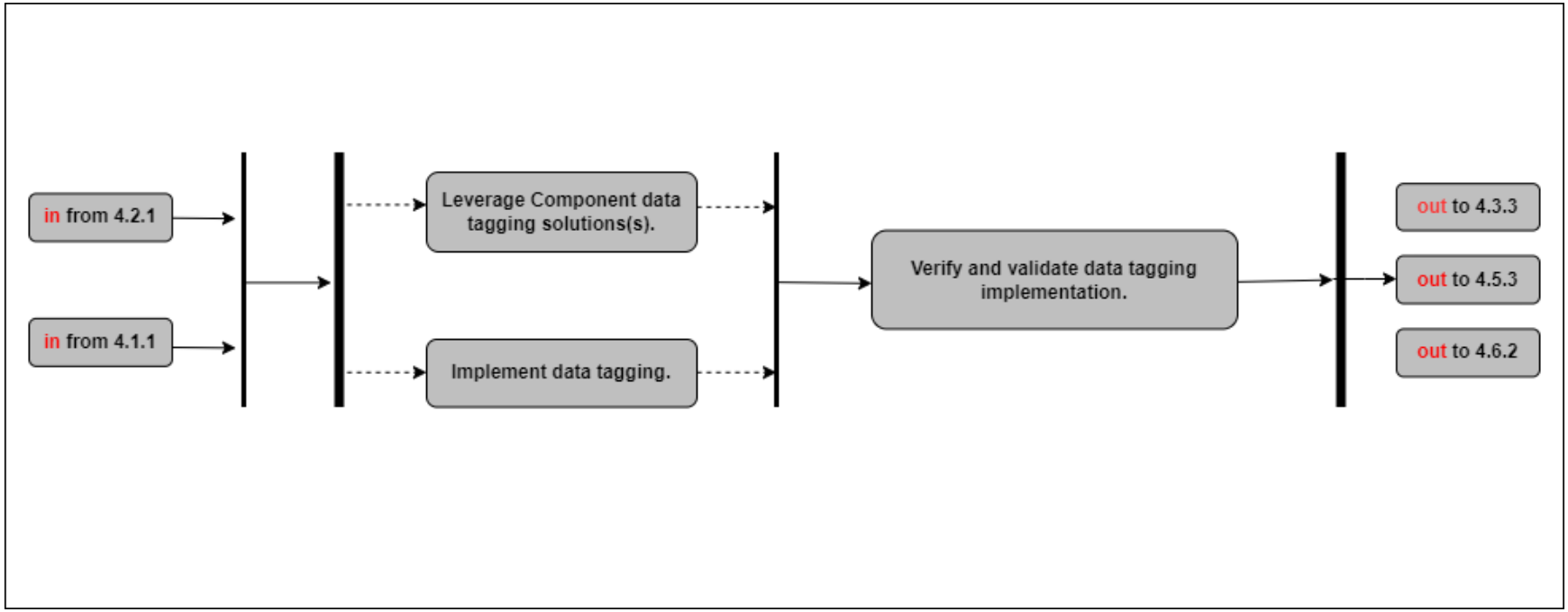

Figure D- 46: Implementation Tasks for Activity 4.3.2 — Manual Data Tagging Part 1

Activity 4.4.1 Data Loss Prevention (DLP) Enforcement Point Logging and Analysis

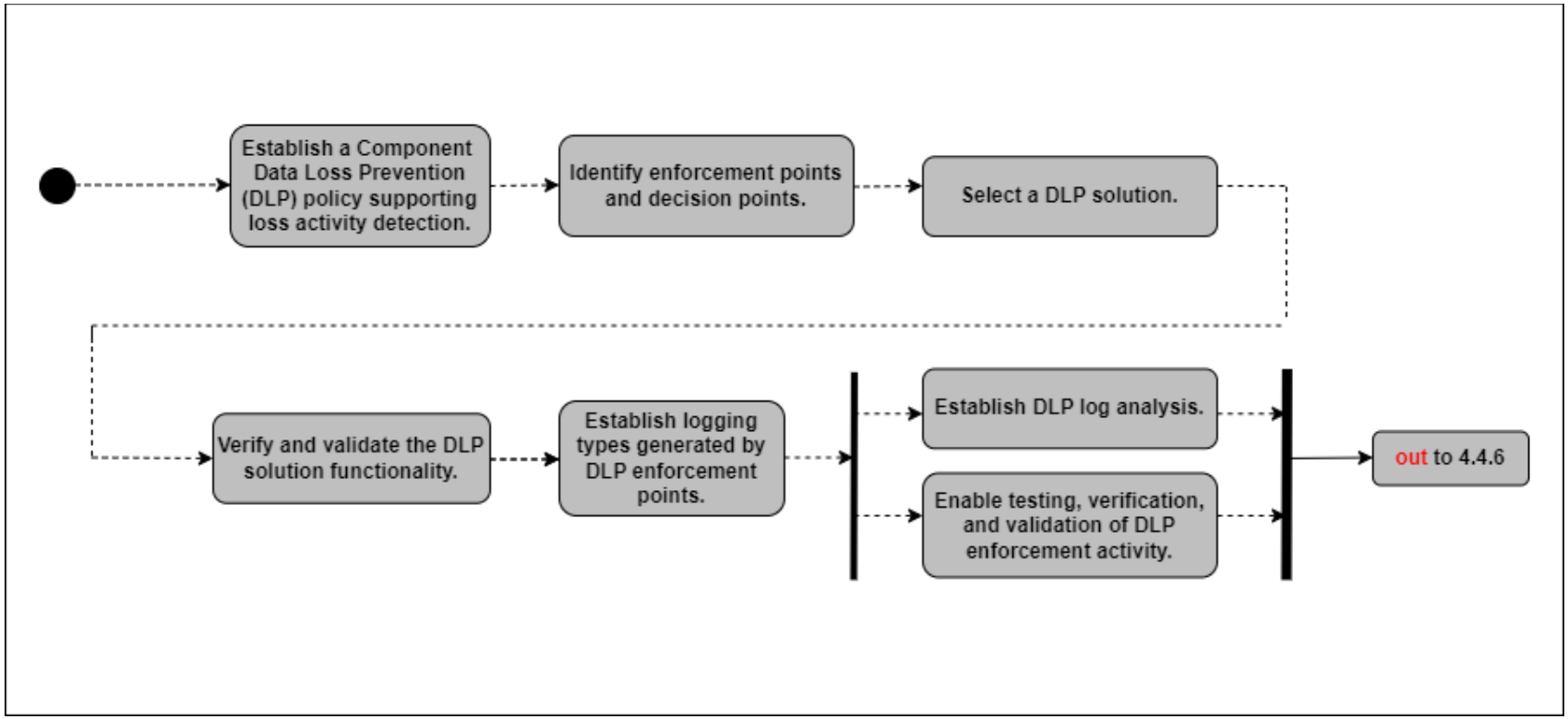

Figure D- 47: Implementation Tasks for Activity 4.4.1 — Data Loss Prevention (DLP) Enforcement Point Logging and Analysis

Activity 4.4.2 Data Rights Management (DRM) Enforcement Point Logging and Analysis

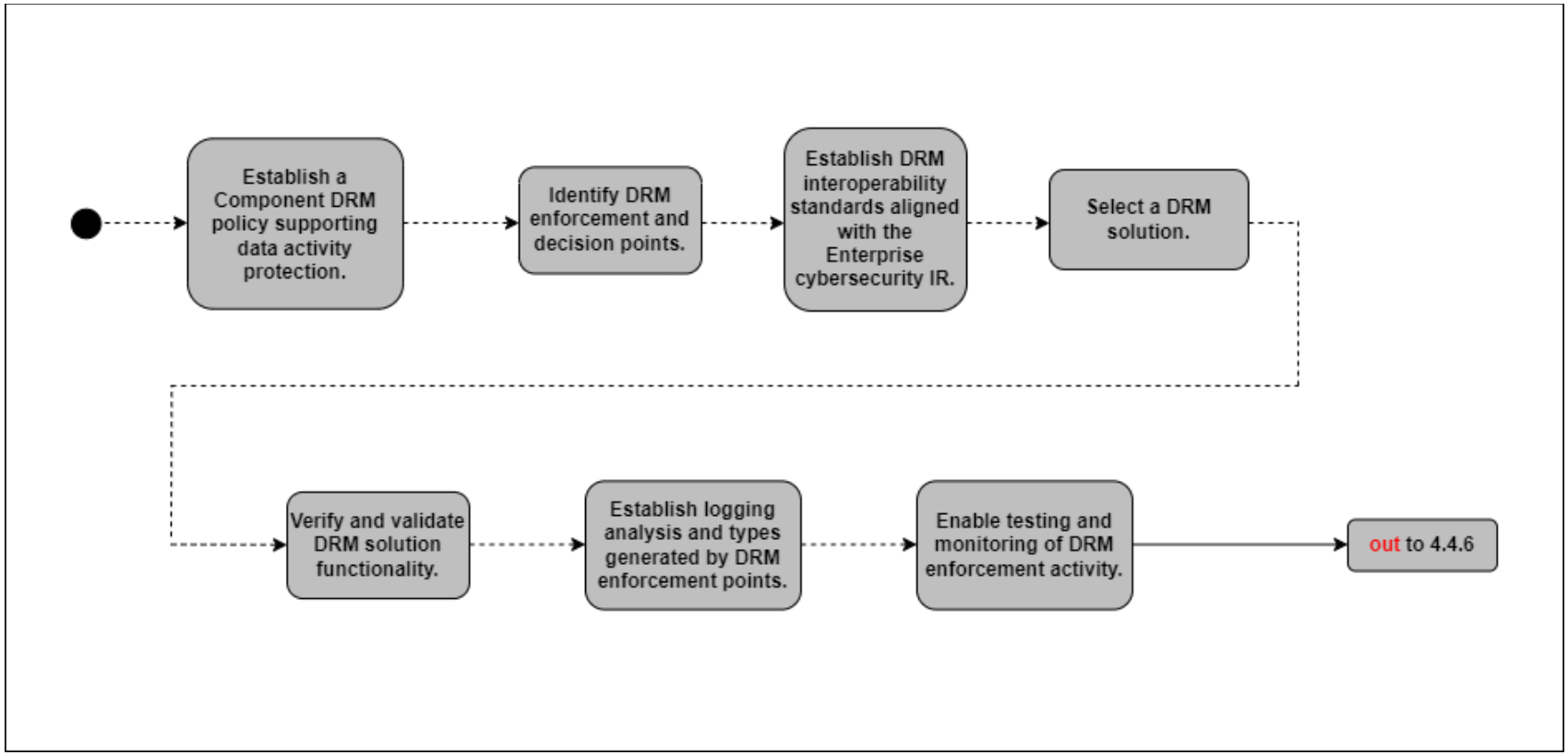

Figure D- 48: Implementation Tasks for Activity 4.4.2 — Data Rights Management (DRM) Enforcement Point Logging and Analysis

Activity 4.4.3 File Activity Monitoring Part 1

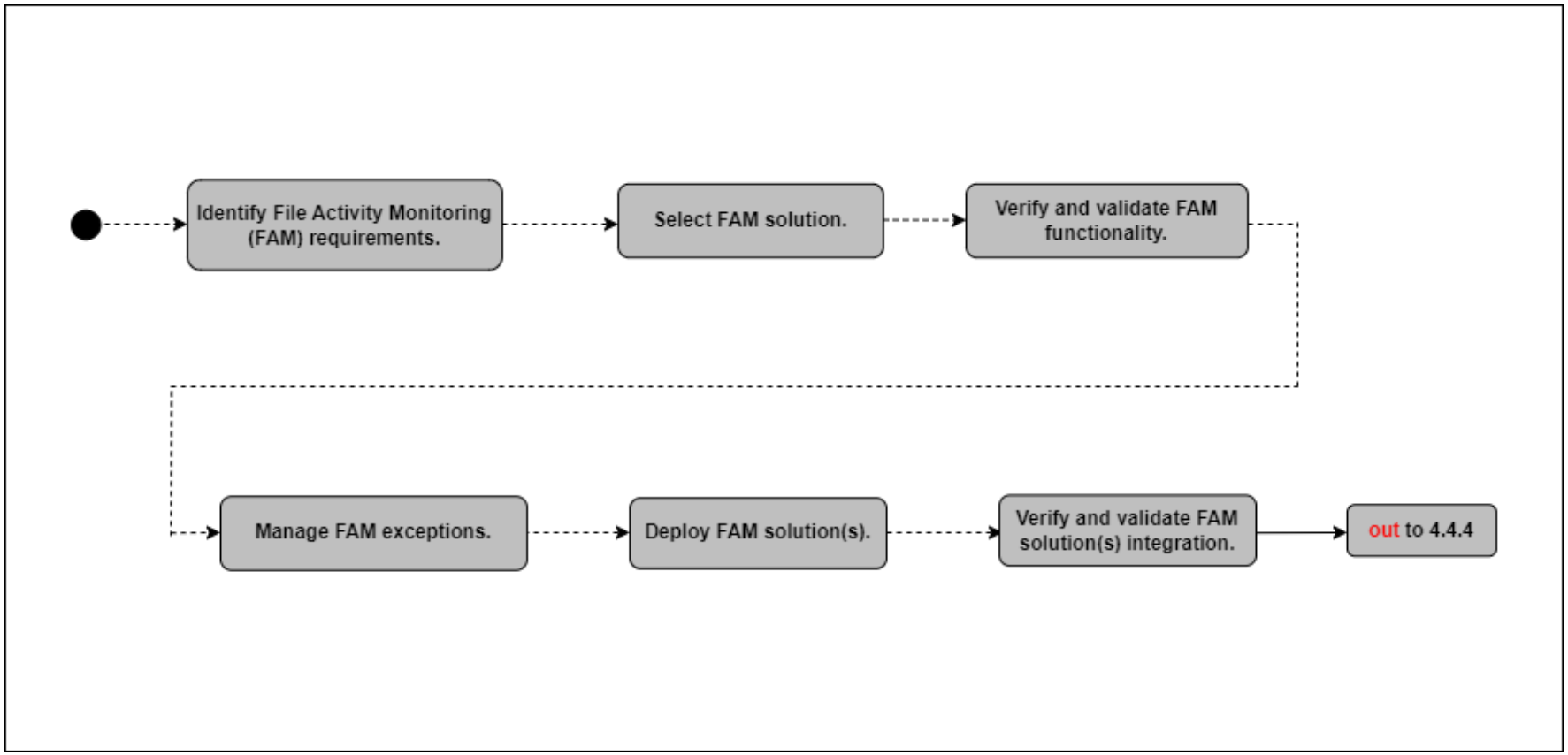

Figure D- 49: Implementation Tasks for Activity 4.4.3 — File Activity Monitoring Part 1

Activity 4.4.4 File Activity Monitoring Part 2

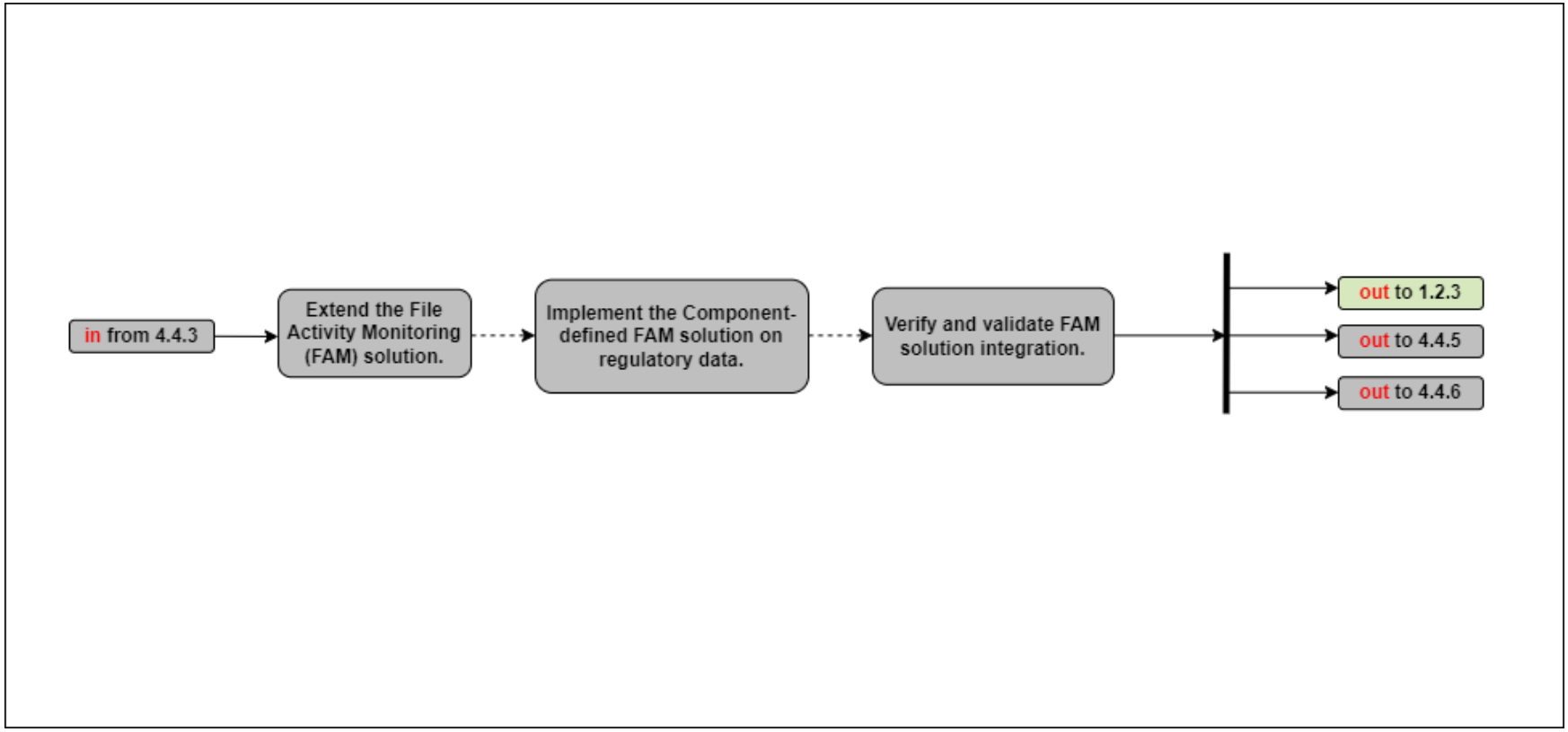

Figure D- 50: Implementation Tasks for Activity 4.4.4 — File Activity Monitoring Part 2

Activity 4.5.1 Implement Data Rights Management (DRM) and Protection Tools Part 1

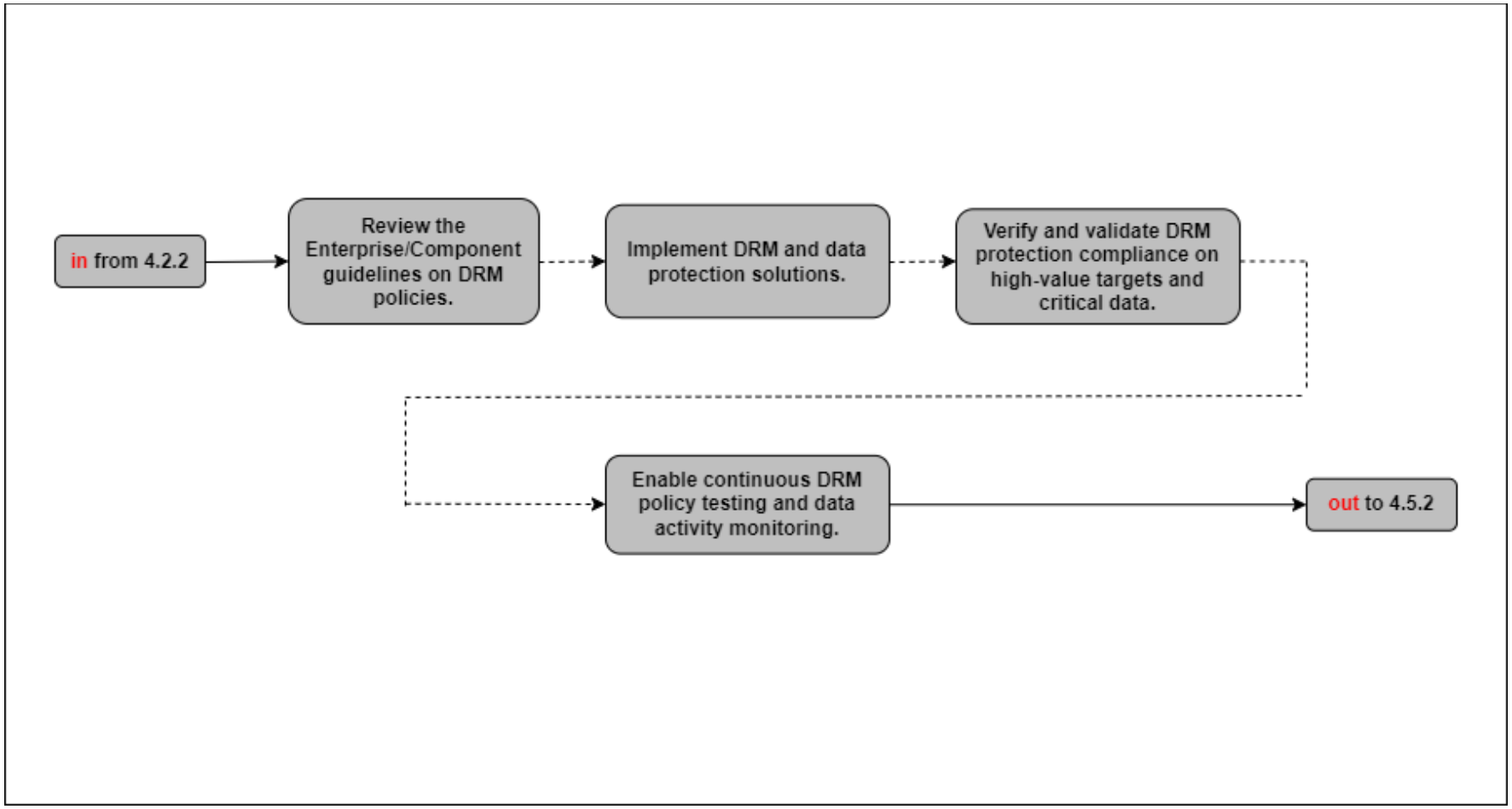

Figure D- 51: Implementation Tasks for Activity 4.5.1 — Implement Data Rights Management (DRM) and Protection Tools Part 1

Activity 4.5.2 Implement Data Rights Management (DRM) and Protection Tools Part 2

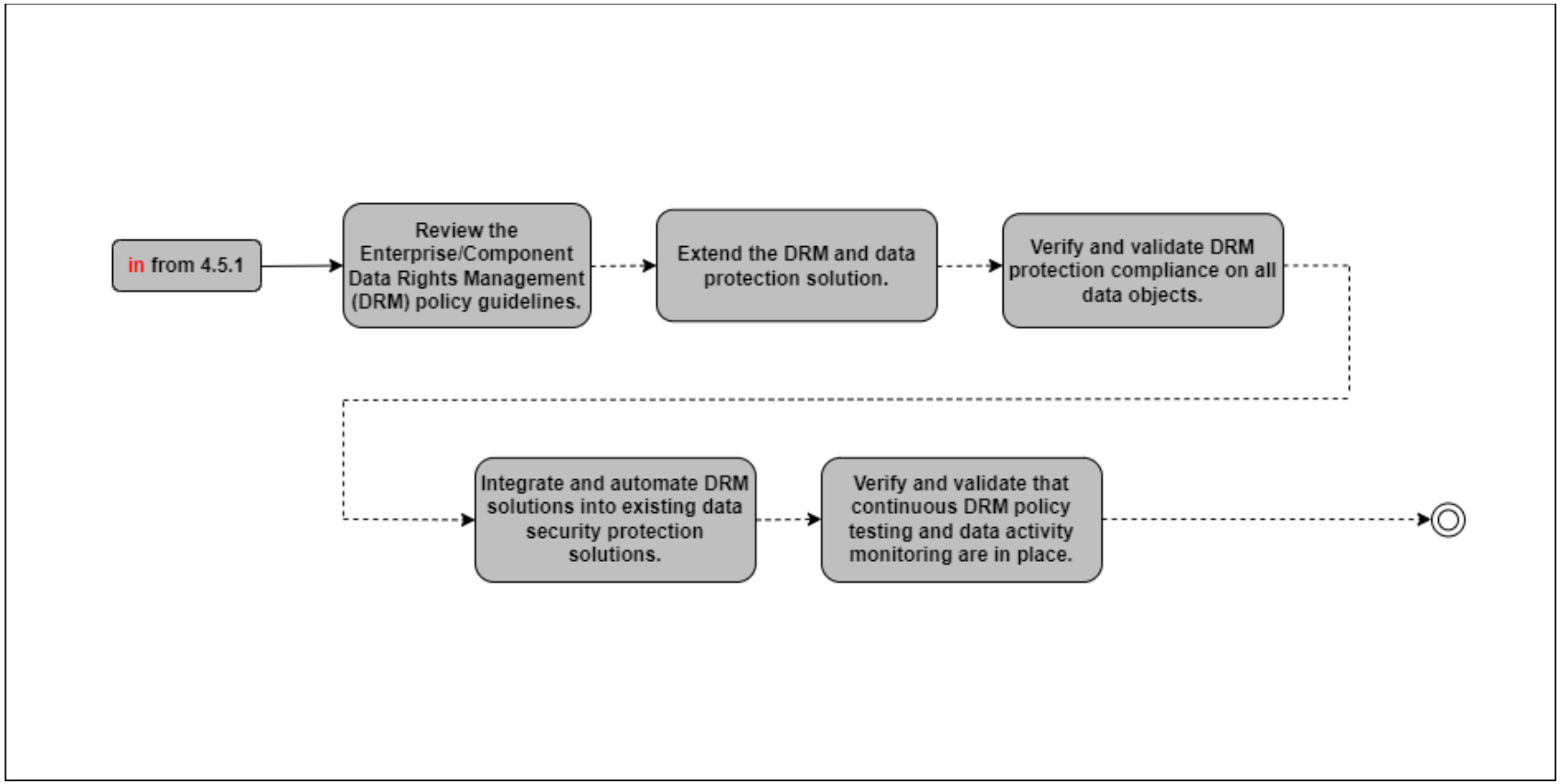

Figure D- 52: Implementation Tasks for Activity 4.5.2 — Implement Data Rights Management (DRM) and Protection Tools Part 2

Activity 4.5.3 Data Rights Management (DRM) Enforcement via Data Tags and Analytics Part 1

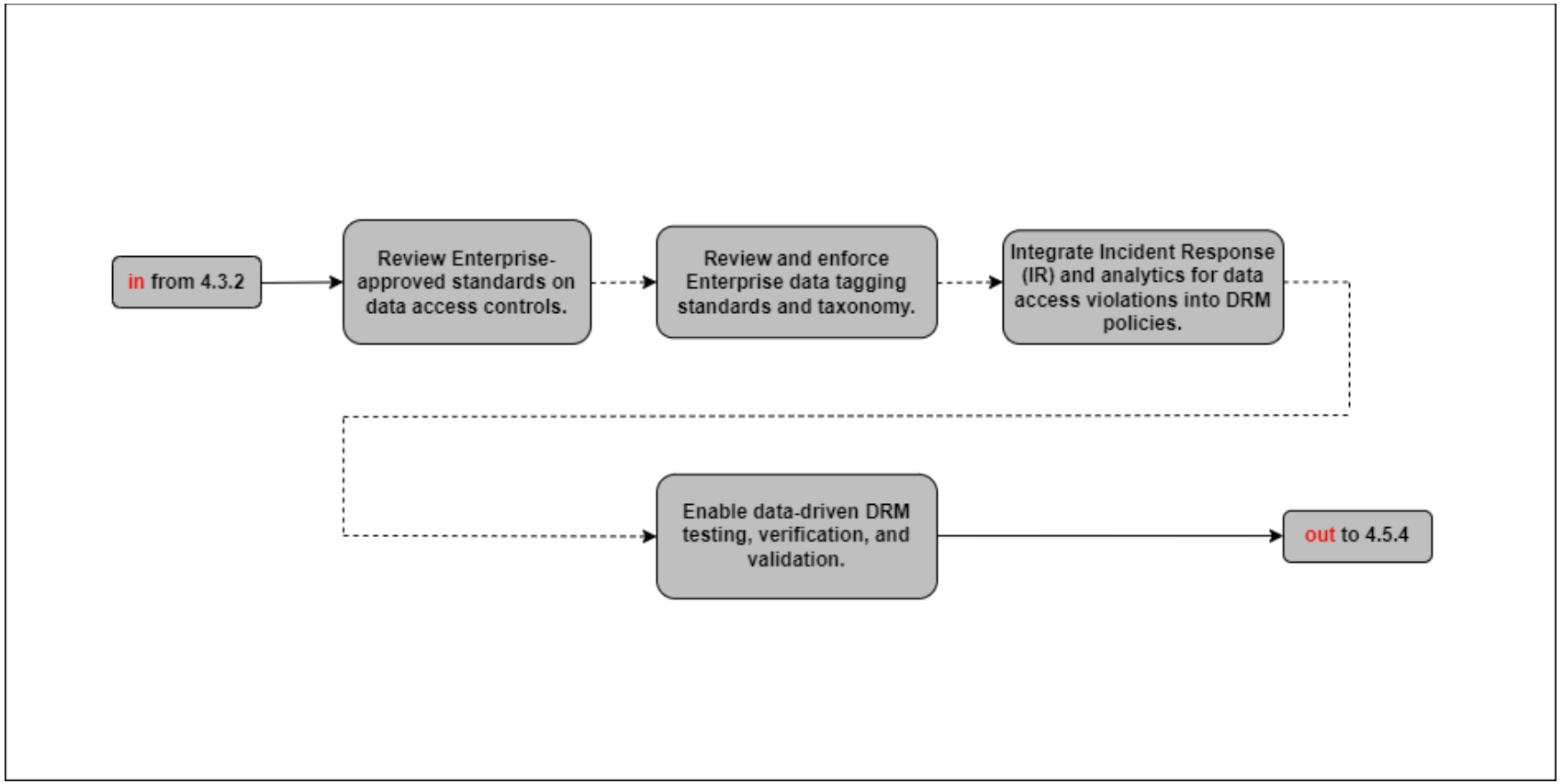

Figure D- 53: Implementation Tasks for Activity 4.5.3 — Data Rights Management (DRM) Enforcement via Data Tags and Analytics Part 1

Activity 4.6.1 Implement Enforcement Points

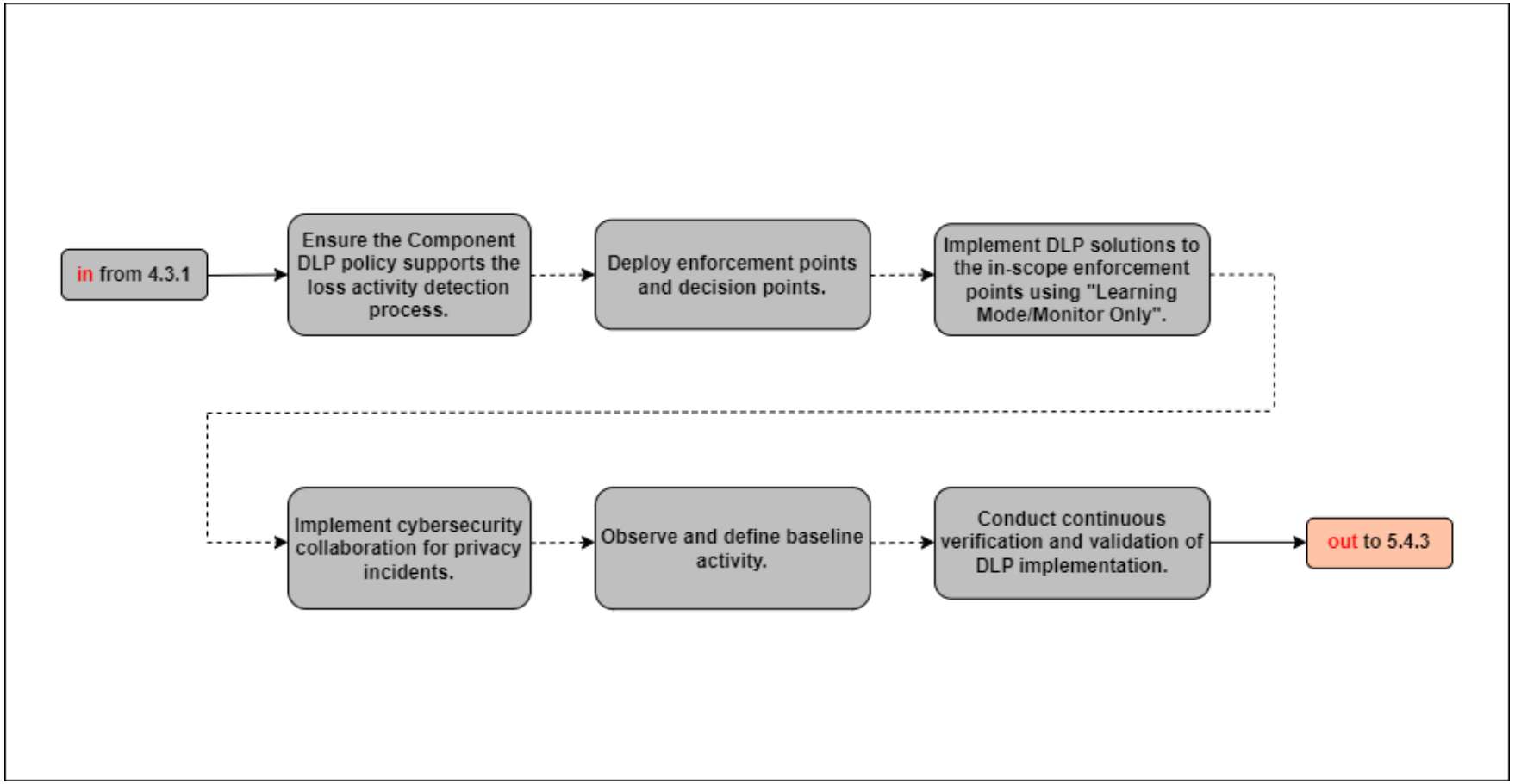

Figure D- 54: Implementation Tasks for Activity 4.6.1 — Implement Enforcement Points

Activity 4.6.2 Data Loss Prevention (DLP) Enforcement via Data Tags and Analytics Part 1

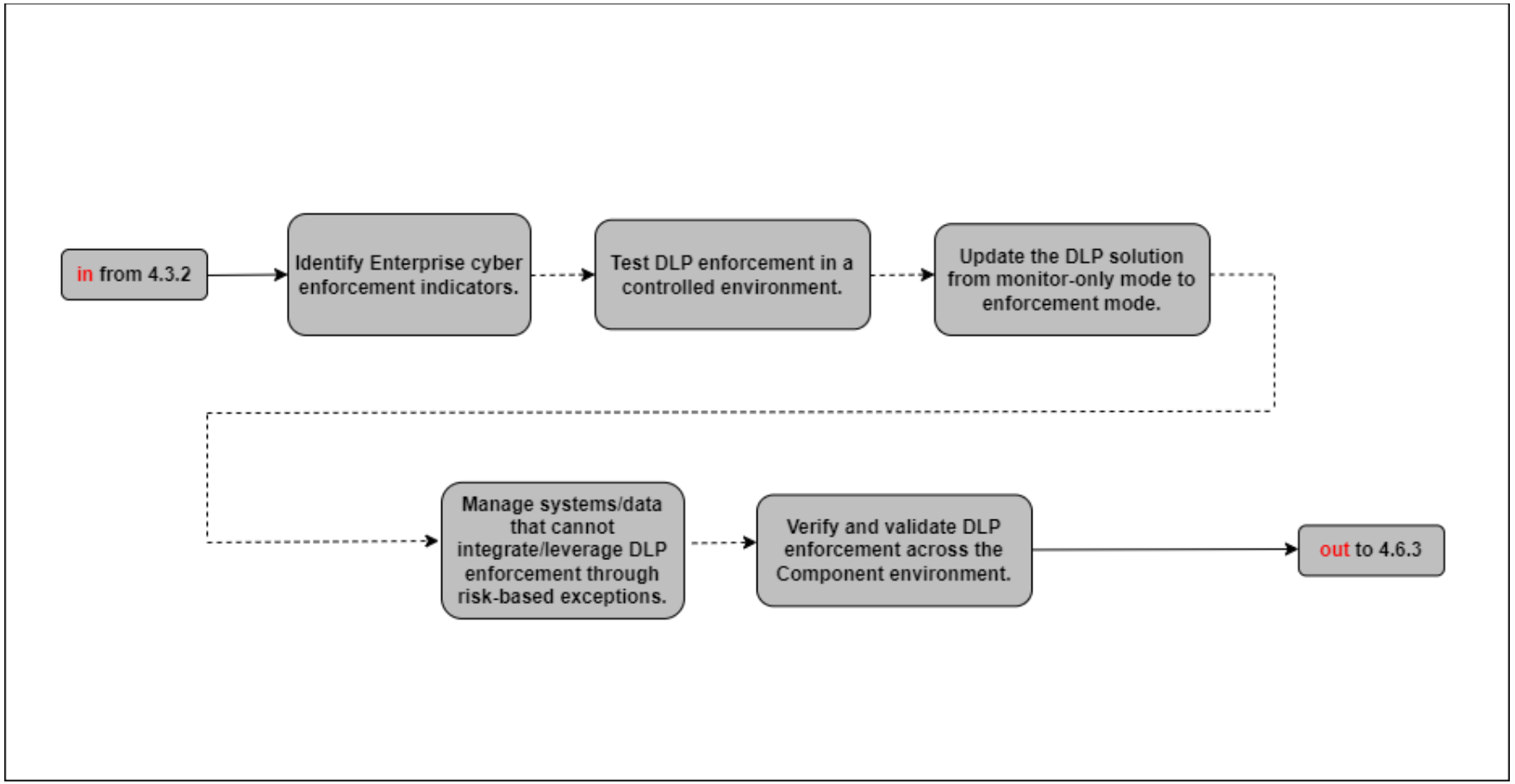

Figure D- 55: Implementation Tasks for Activity 4.6.2 — Data Loss Prevention (DLP) Enforcement via Data Tags and Analytics Part 1

Activity 4.7.1 Integrate Data, Applications, Assets, Services (DAAS) Access with Software-Defined Storage (SDS) Policy Part 1

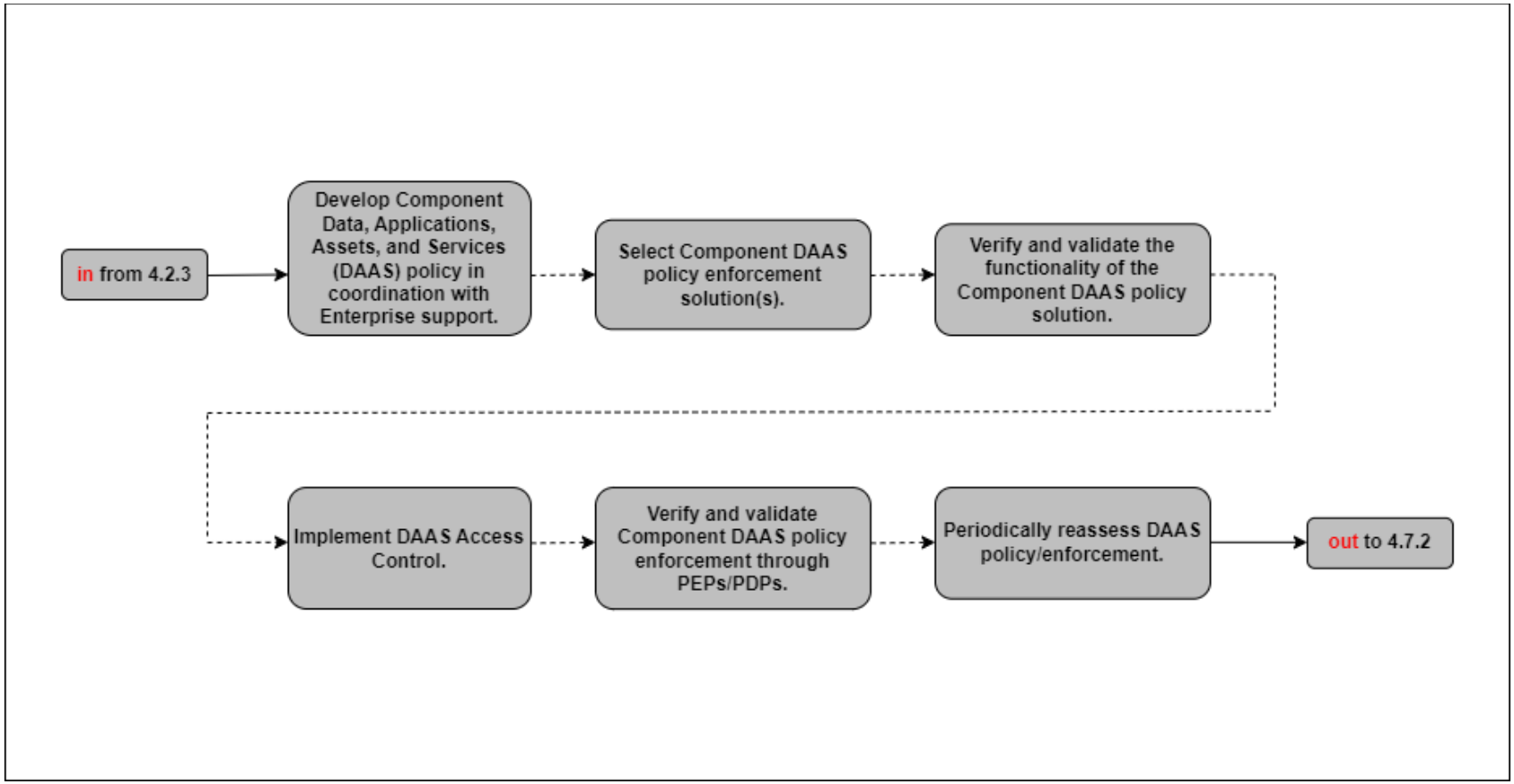

Figure D- 56: Implementation Tasks for Activity 4.7.1 — Integrate Data, Applications, Assets, Services (DAAS) Access with Software-Defined Storage (SDS) Policy Part 1

Activity 4.7.4 Integrate Solution(s) and Policy with Enterprise Identity Provider (IdP) Part 1

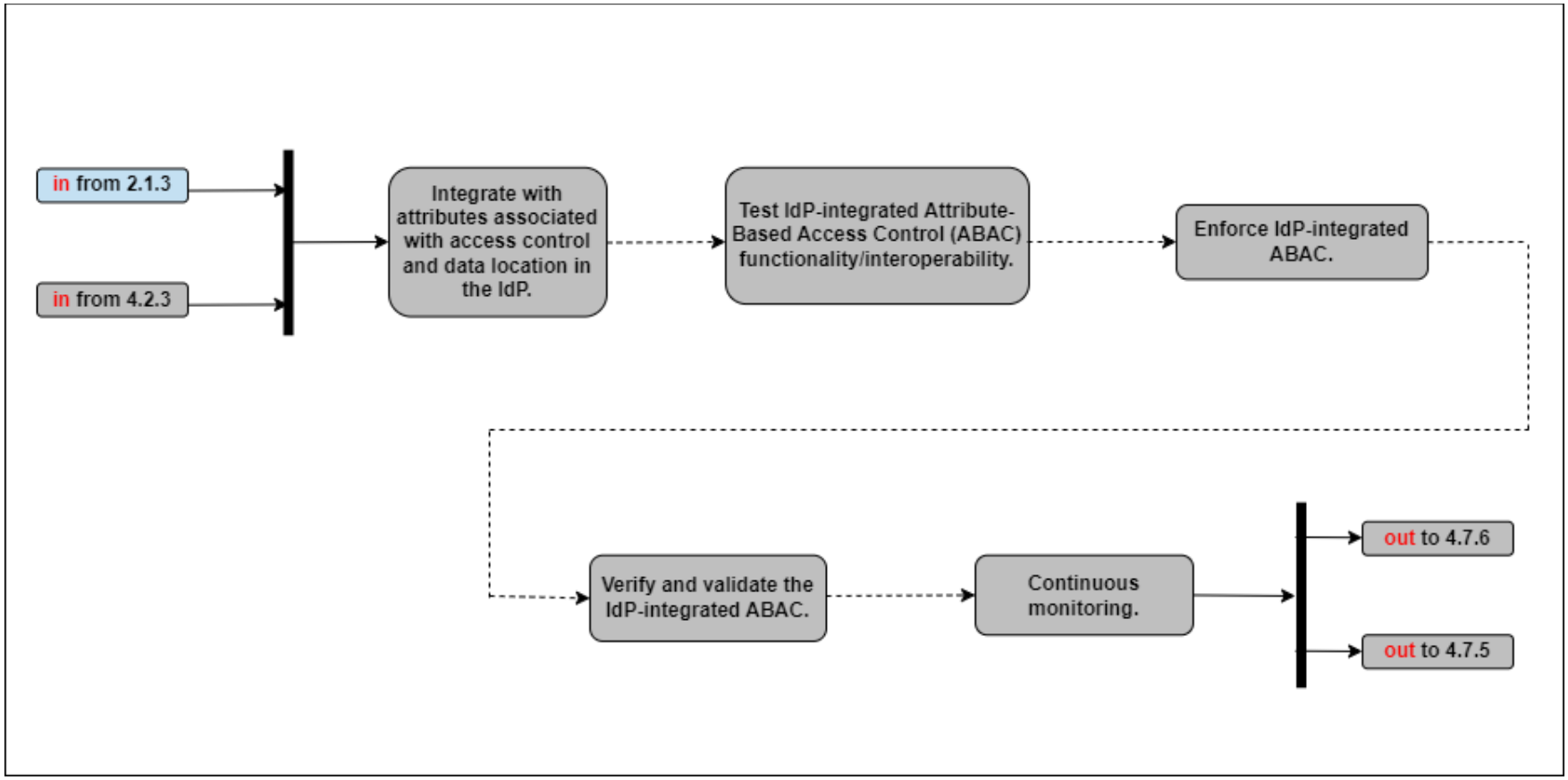

Figure D- 57: Implementation Tasks for Activity 4.7.4 — Integrate Solution(s) and Policy with Enterprise Identity Provider (IdP) Part 1

Activity 5.1.1 Define Granular Control Access Rules and Policies Part 1

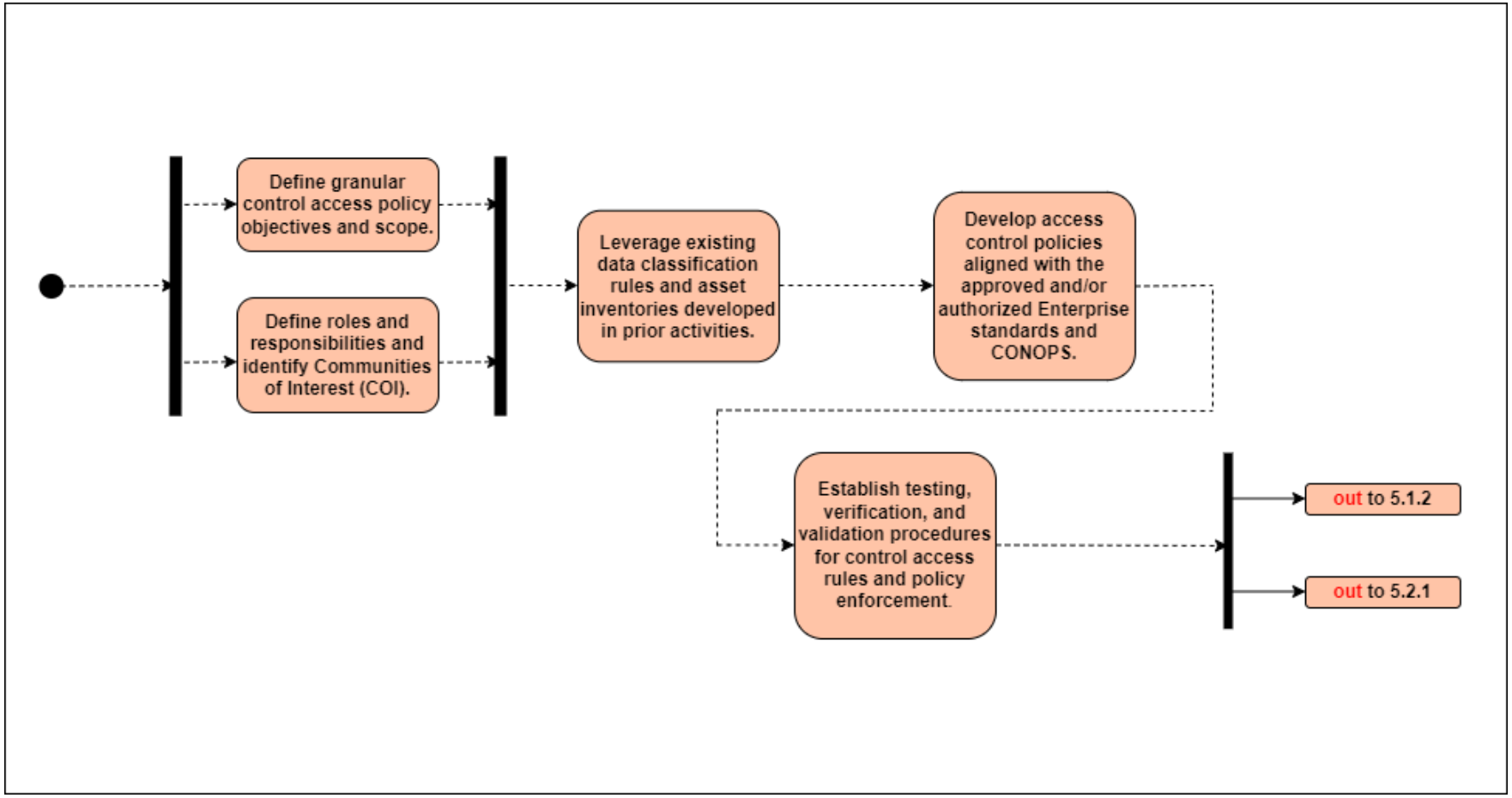

Figure D- 58: Implementation Tasks for Activity 5.1.1 — Define Granular Control Access Rules and Policies Part 1

Activity 5.1.2 Define Granular Control Access Rules and Policies Part 2

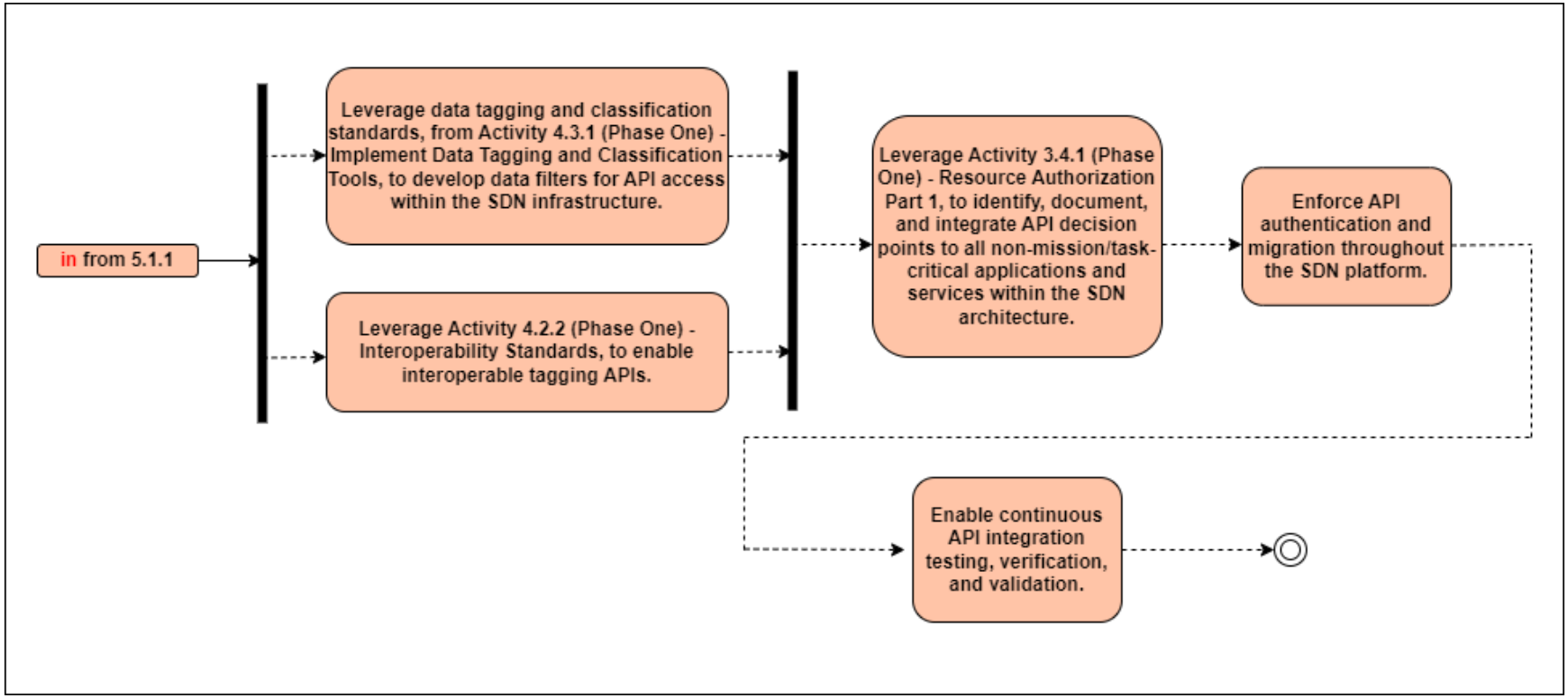

Figure D- 59: Implementation Tasks for Activity 5.1.2 — Define Granular Control Access Rules and Policies Part 2

Activity 5.2.1 Define Software-Defined Networking (SDN) Application Programming Interfaces (APIs)

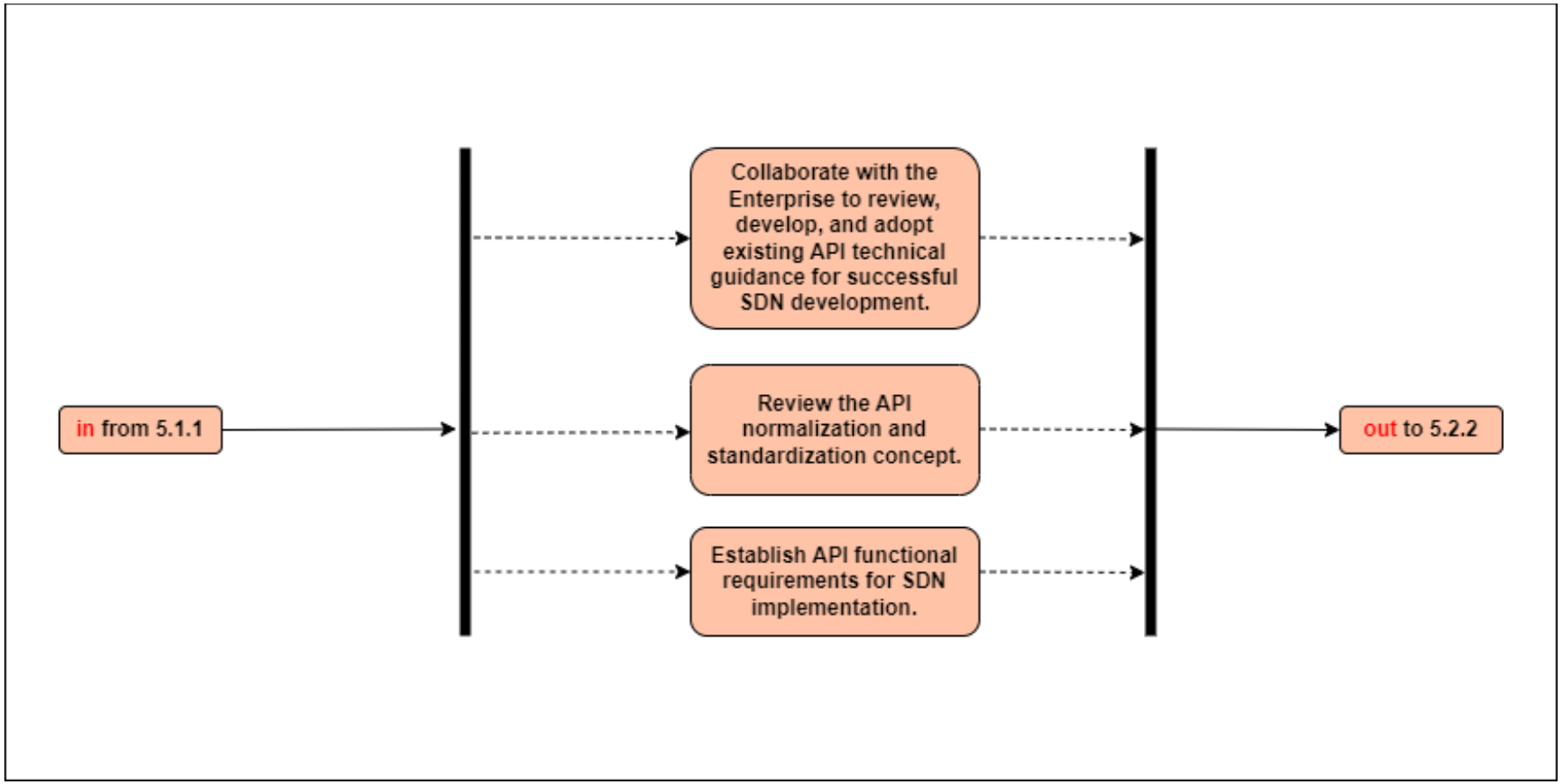

Figure D- 60: Implementation Tasks for Activity 5.2.1 — Define Software-Defined Networking (SDN) Application Programming Interfaces (APIs)

Activity 5.2.2 Implement Software-Defined Networking (SDN) Programmable Infrastructure

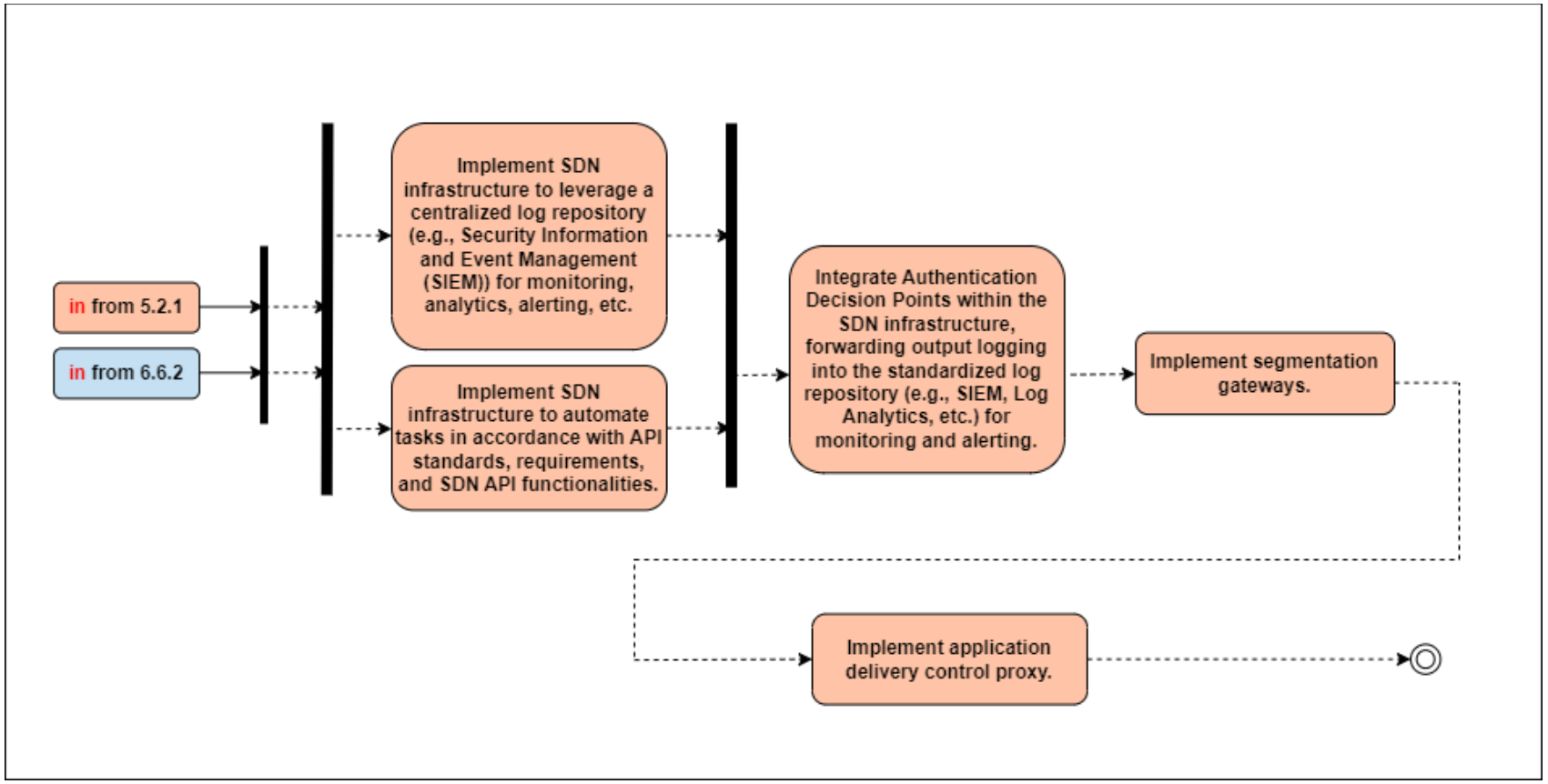

Figure D- 61: Implementation Tasks for Activity 5.2.2 — Implement Software-Defined Networking (SDN) Programmable Infrastructure

Activity 5.2.3 Segment Flows into Control, Management, and Data Planes

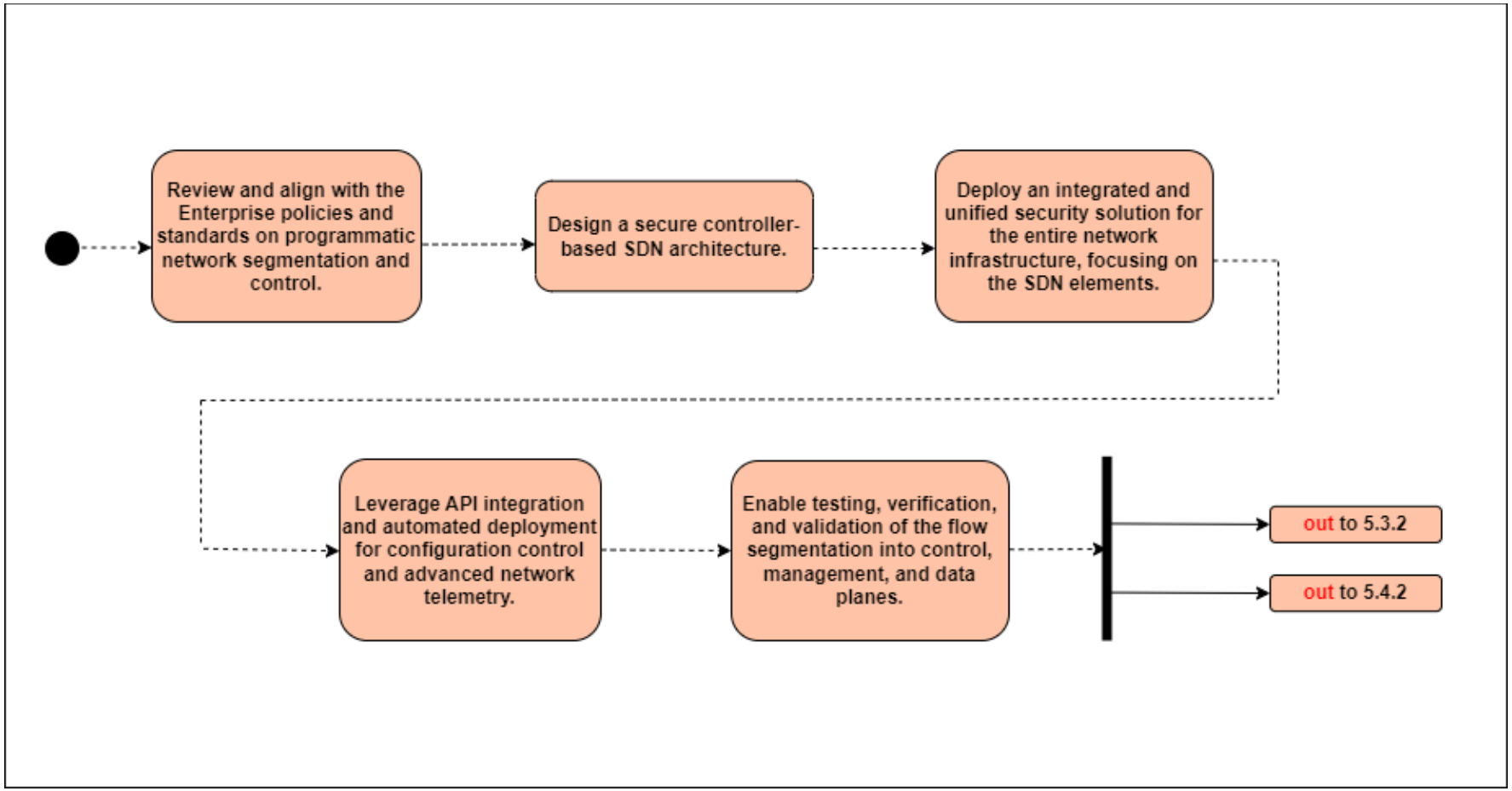

Figure D- 62: Implementation Tasks for Activity 5.2.3 — Segment Flows into Control, Management, and Data Planes

Activity 5.3.1 Datacenter Macro-Segmentation

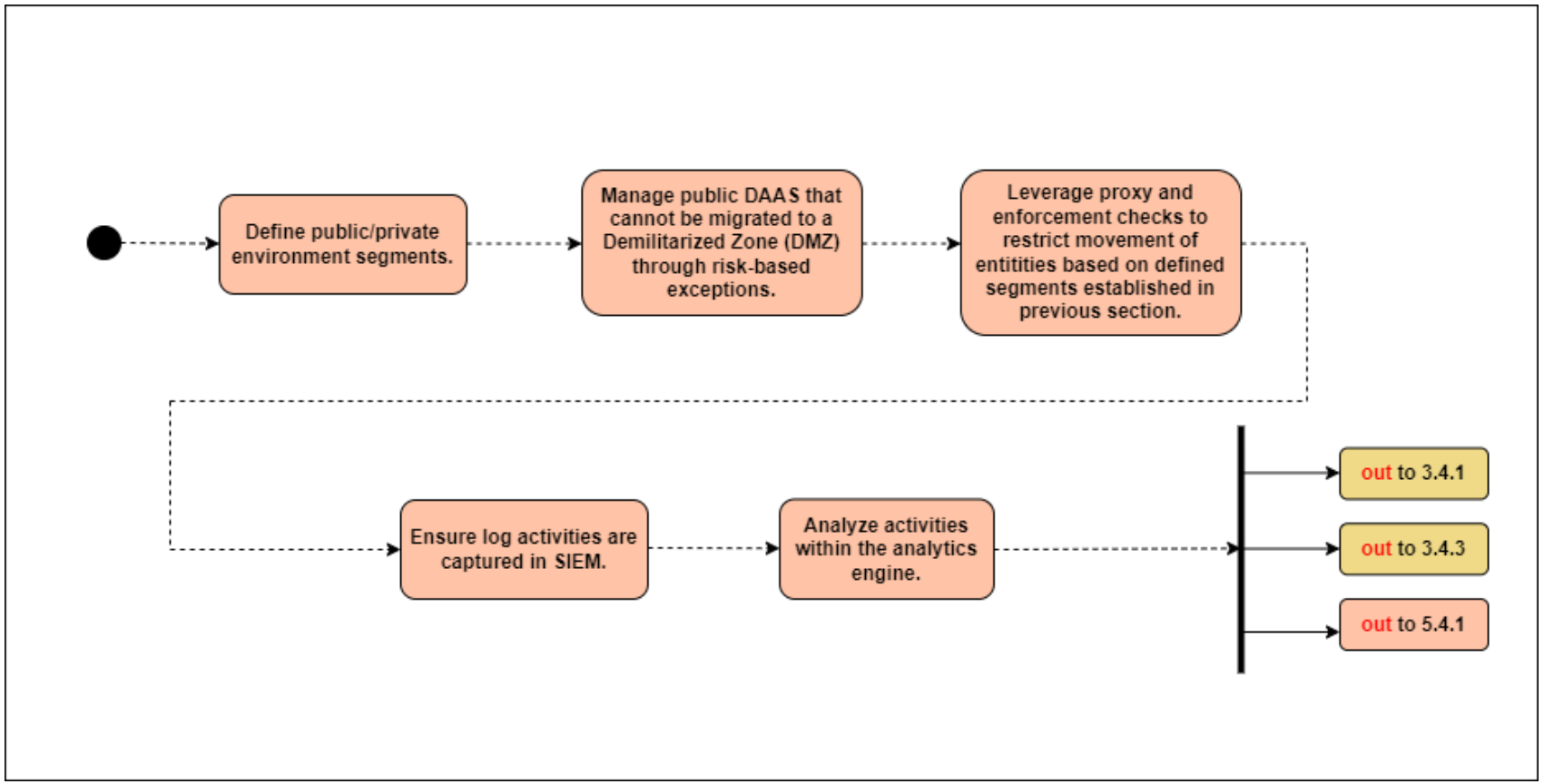

Figure D- 63: Implementation Tasks for Activity 5.3.1 — Datacenter Macro-Segmentation

Activity 5.3.2 Base/Camp/Post/Station (B/C/P/S) Macro-Segmentation

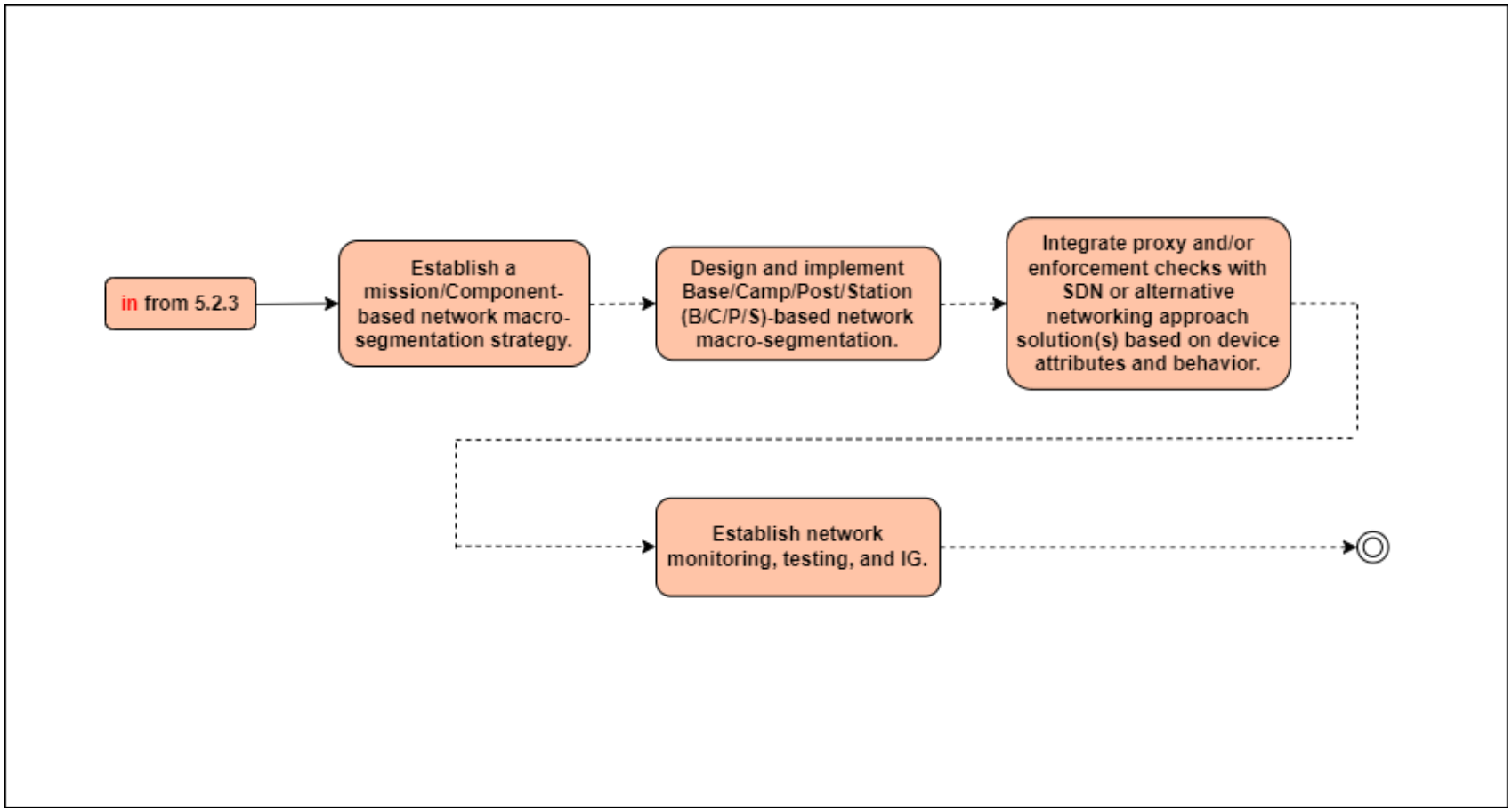

Figure D- 64: Implementation Tasks for Activity 5.3.2 — Base/Camp/Post/Station (B/C/P/S) Macro-Segmentation

Activity 5.4.1 Implement Micro-Segmentation

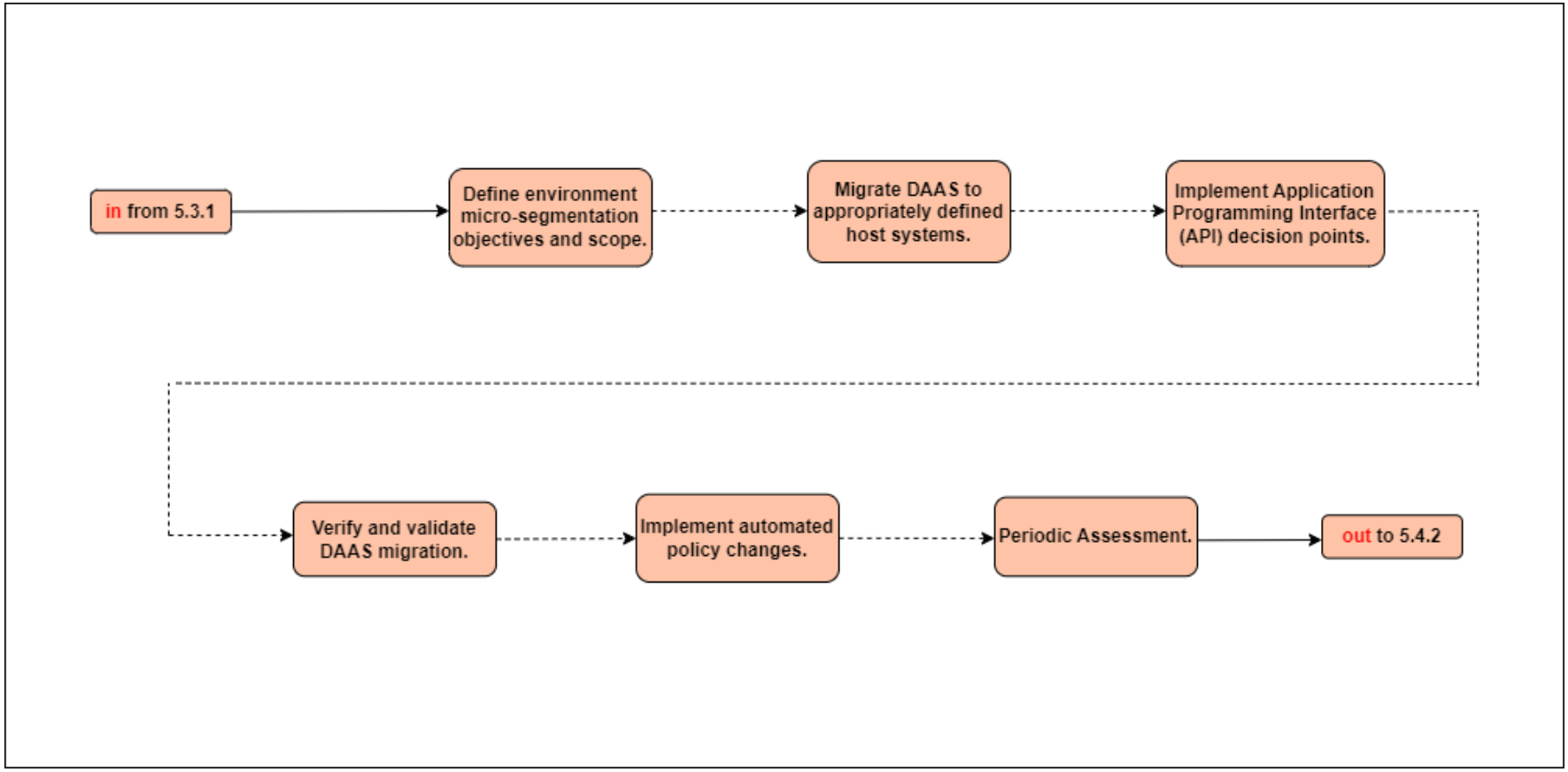

Figure D- 65: Implementation Tasks for Activity 5.4.1 — Implement Micro-Segmentation

Activity 5.4.2 Application and Device Micro-Segmentation

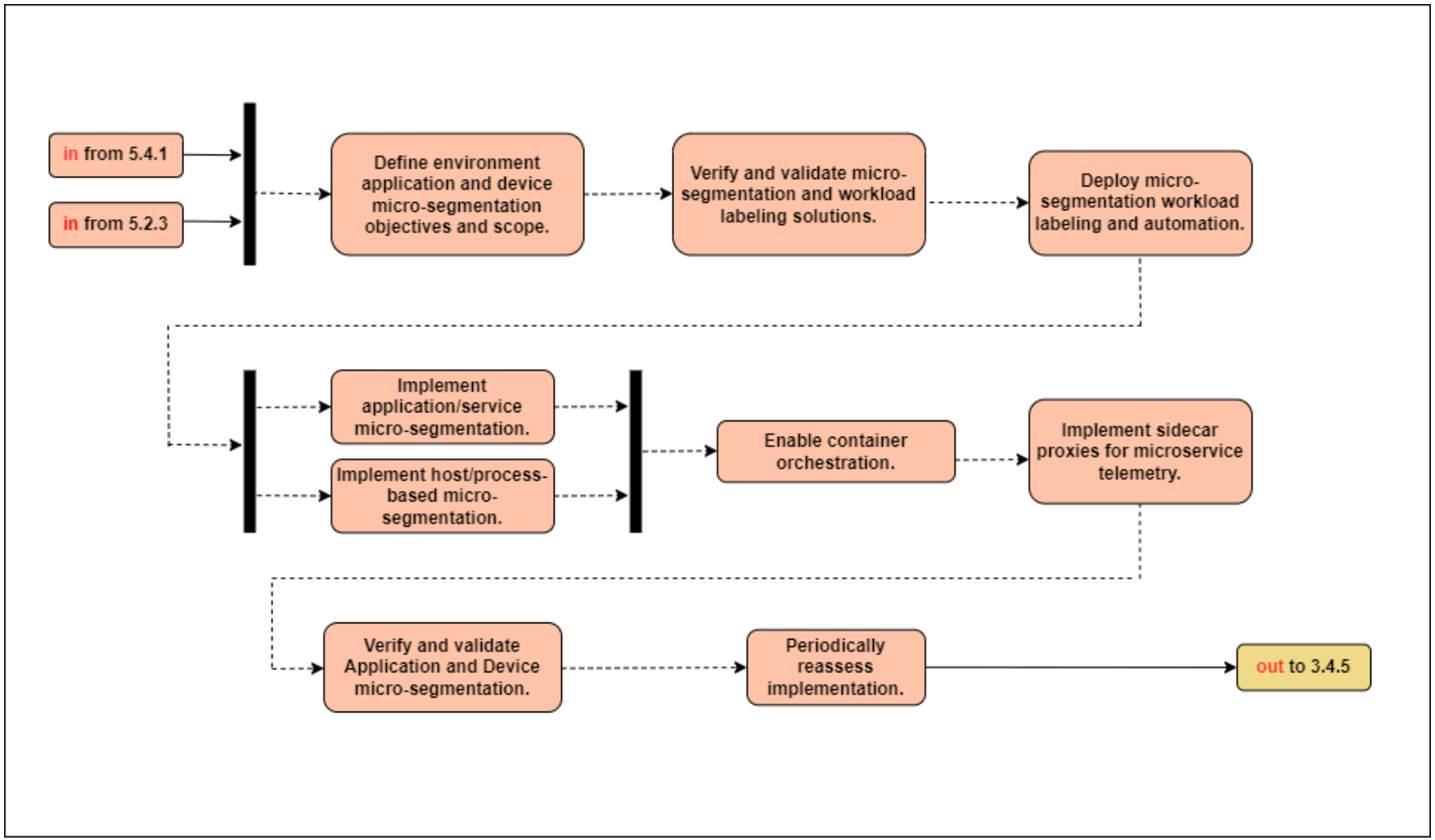

Figure D- 66: Implementation Tasks for Activity 5.4.2 — Application and Device Micro-Segmentation

Activity 5.4.4 Protect Data in Transit

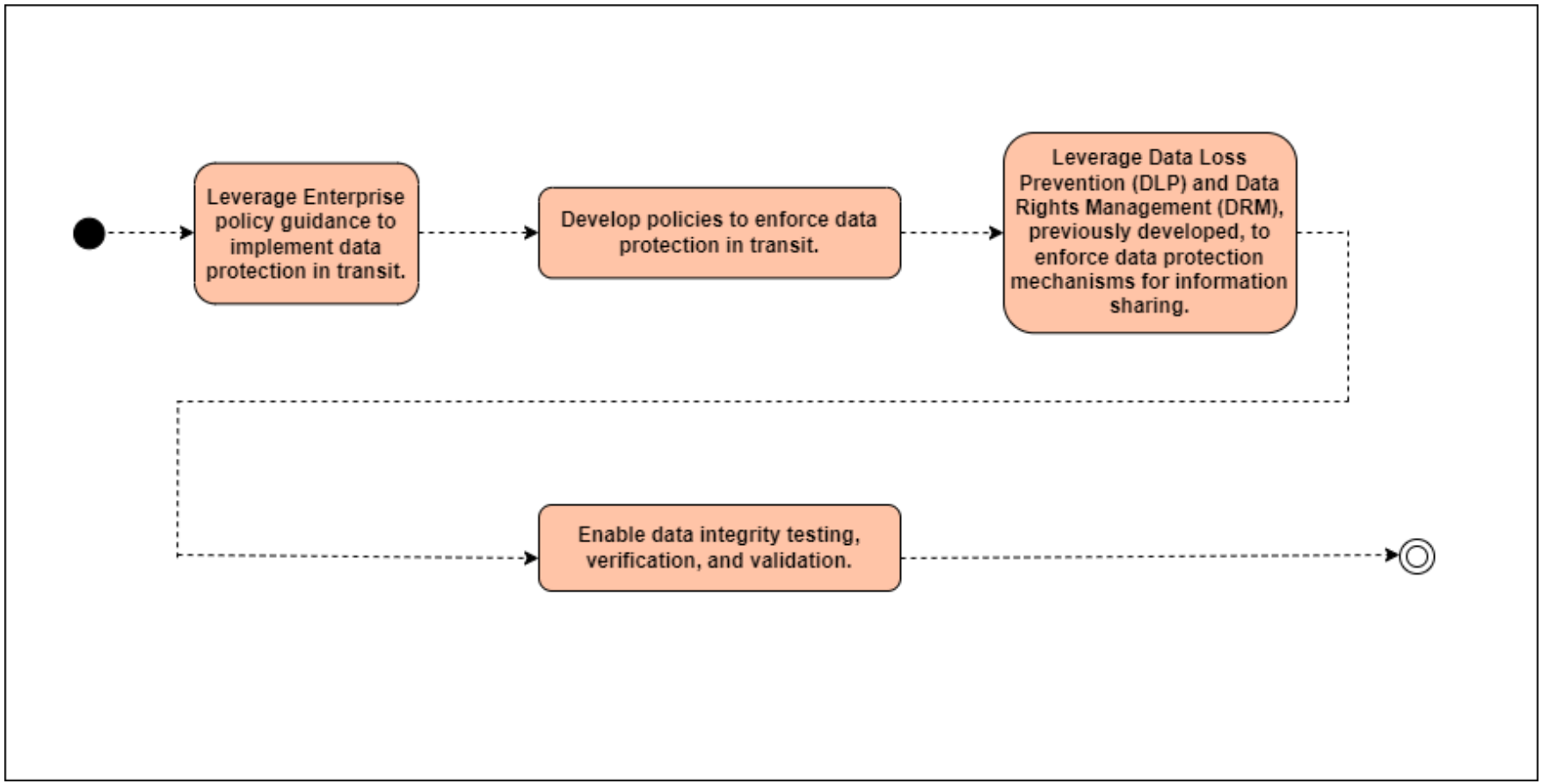

Figure D- 67: Implementation Tasks for Activity 5.4.4 — Protect Data in Transit

Activity 6.1.1 Policy Inventory and Development

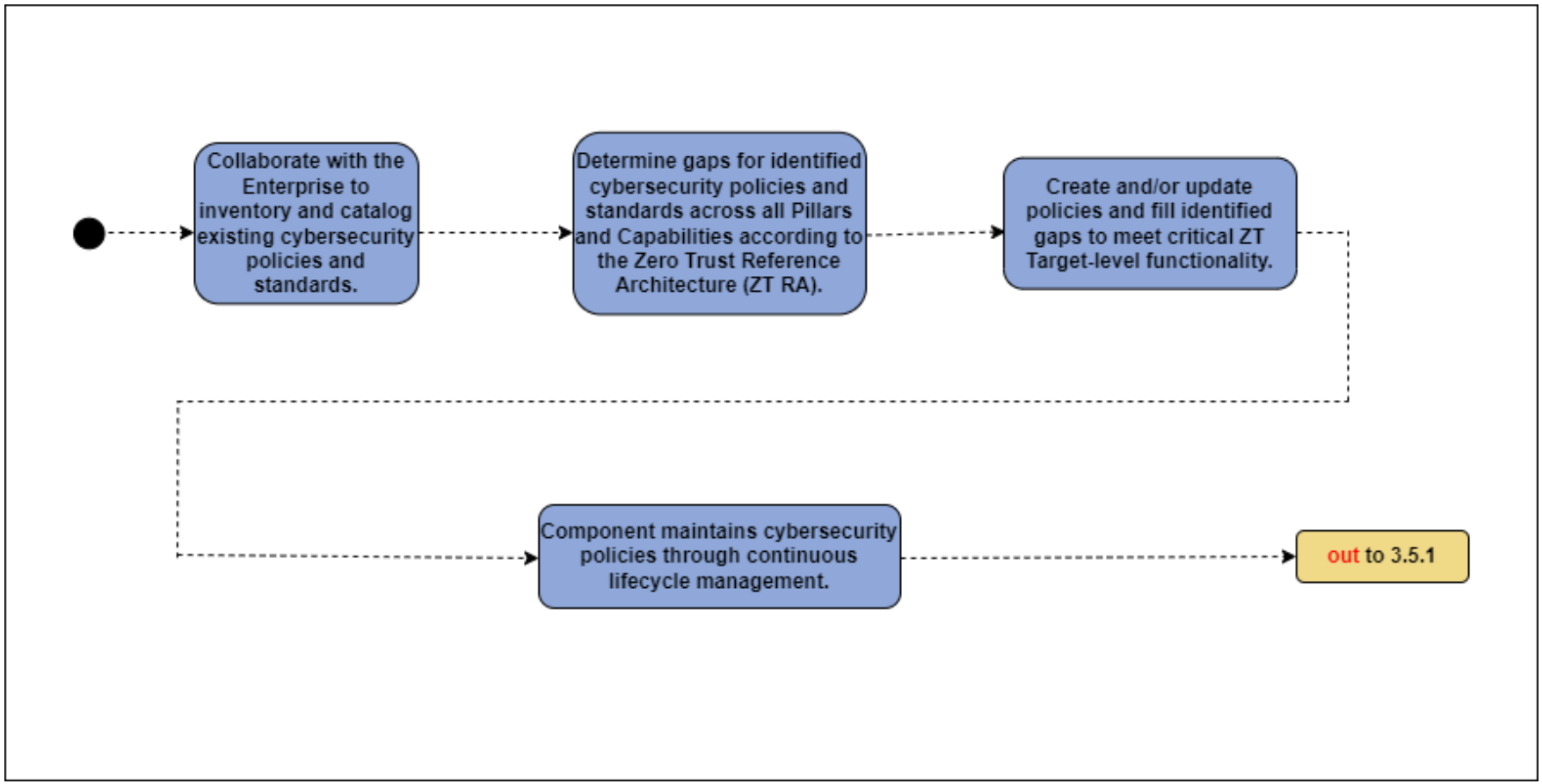

Figure D- 68: Implementation Tasks for Activity 6.1.1 — Policy Inventory and Development

Activity 6.1.2 Organization Access Profile

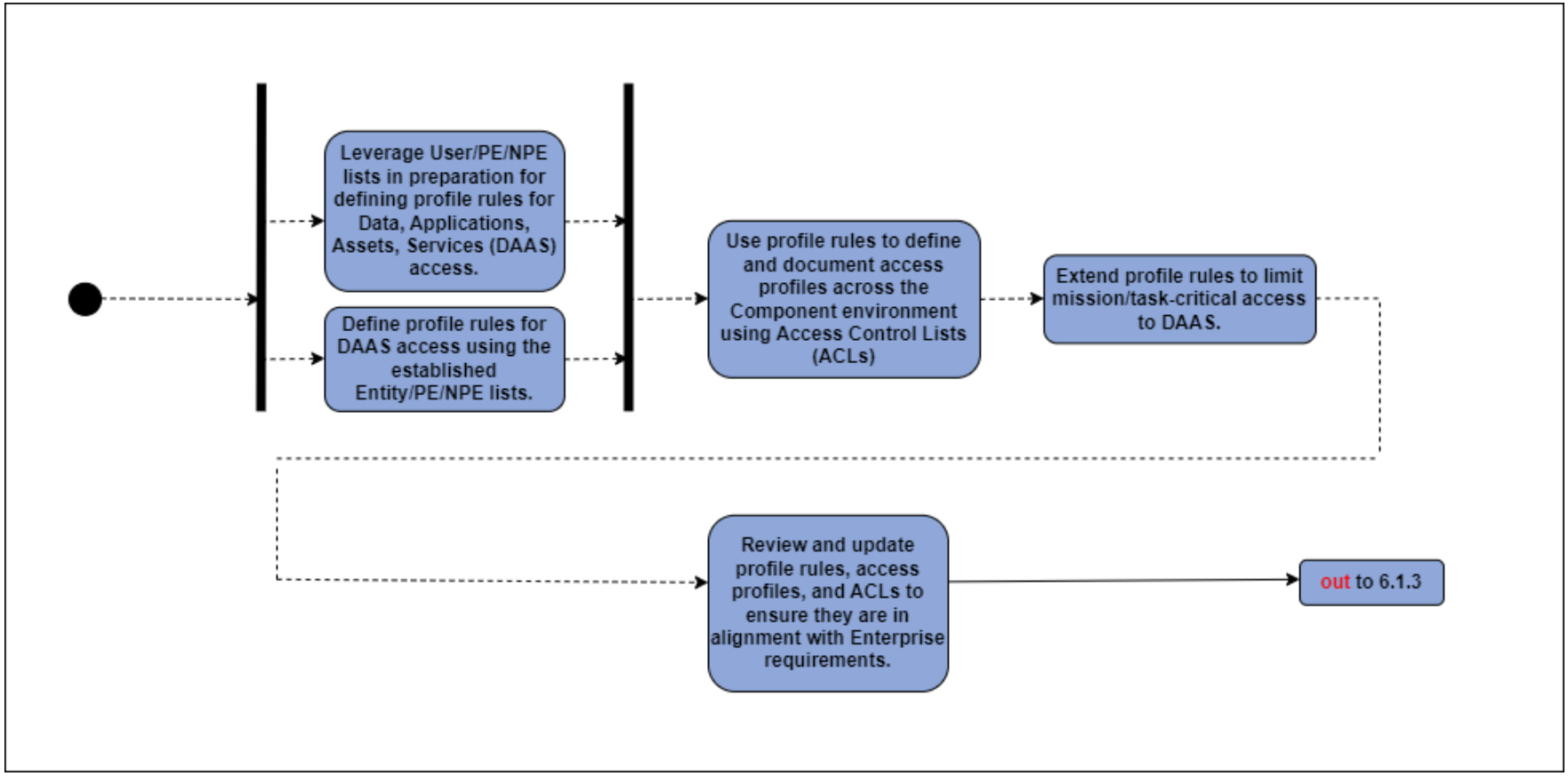

Figure D- 69: Implementation Tasks for Activity 6.1.2 — Organization Access Profile

Activity 6.1.3 Enterprise Security Profile Part 1

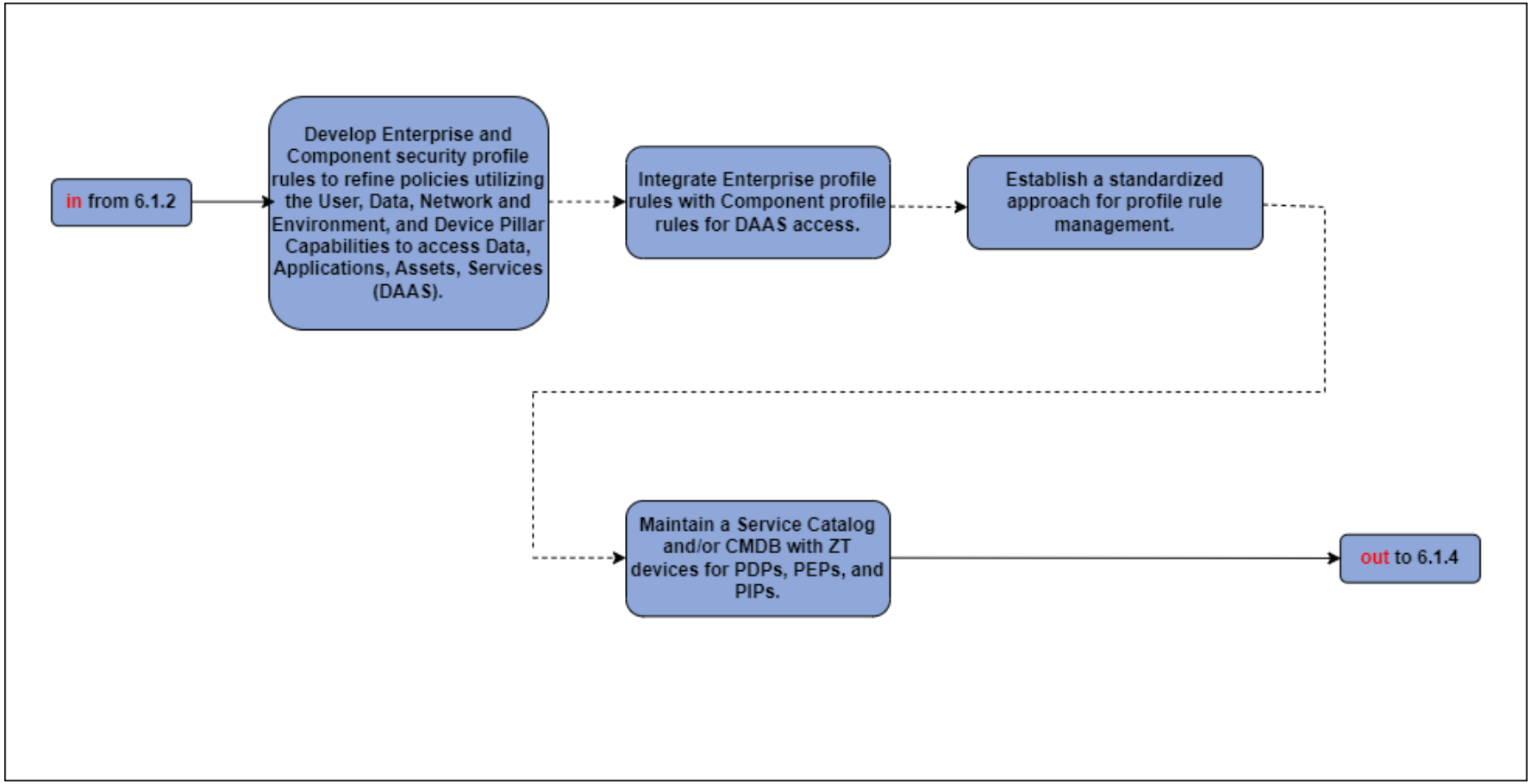

Figure D- 70: Implementation Tasks for Activity 6.1.3 — Enterprise Security Profile Part 1

Activity 6.2.1 Task Automation Analysis

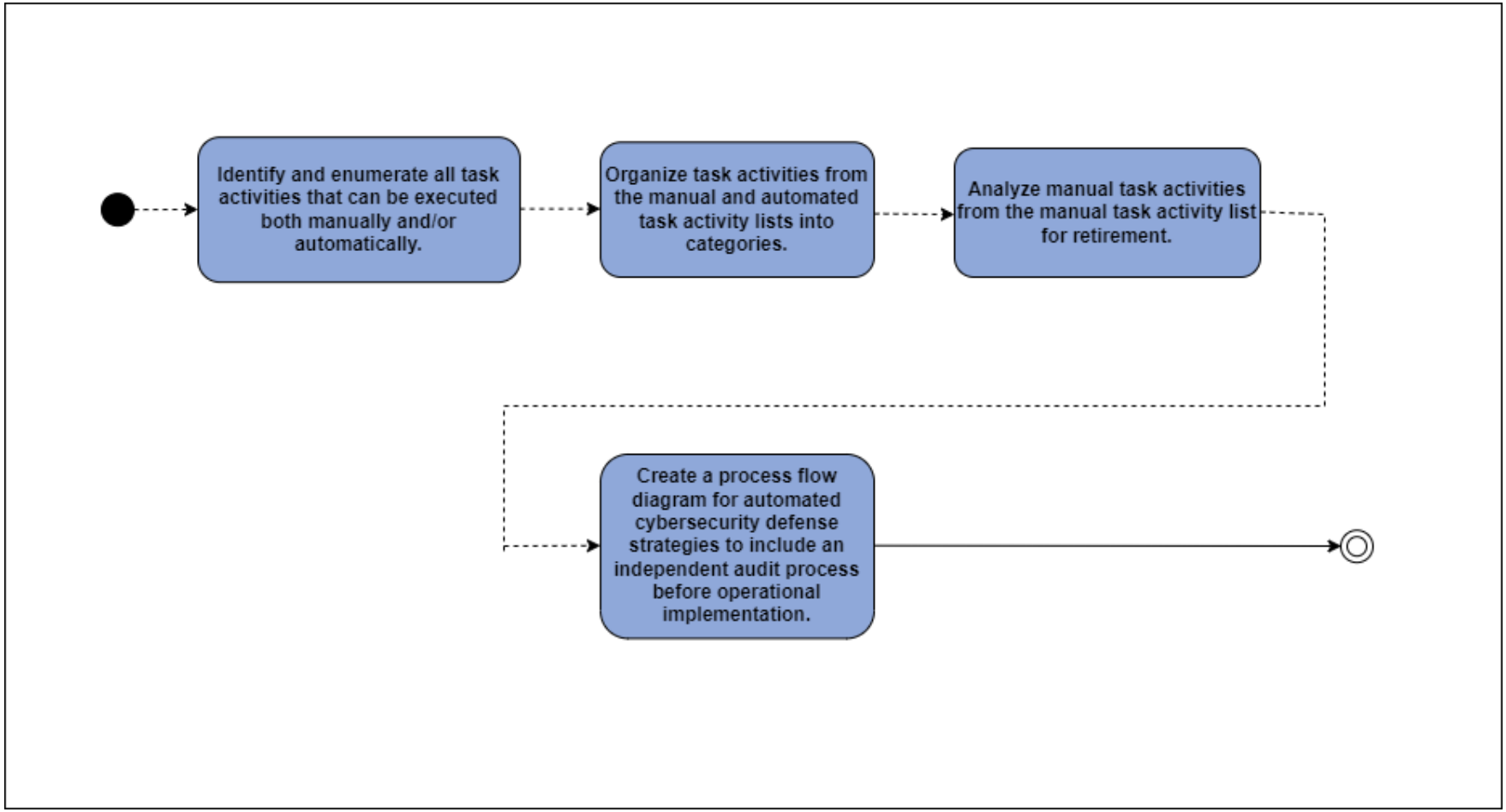

Figure D- 71: Implementation Tasks for Activity 6.2.1 — Task Automation Analysis

Activity 6.2.2 Enterprise Integration and Workflow Provisioning Part 1

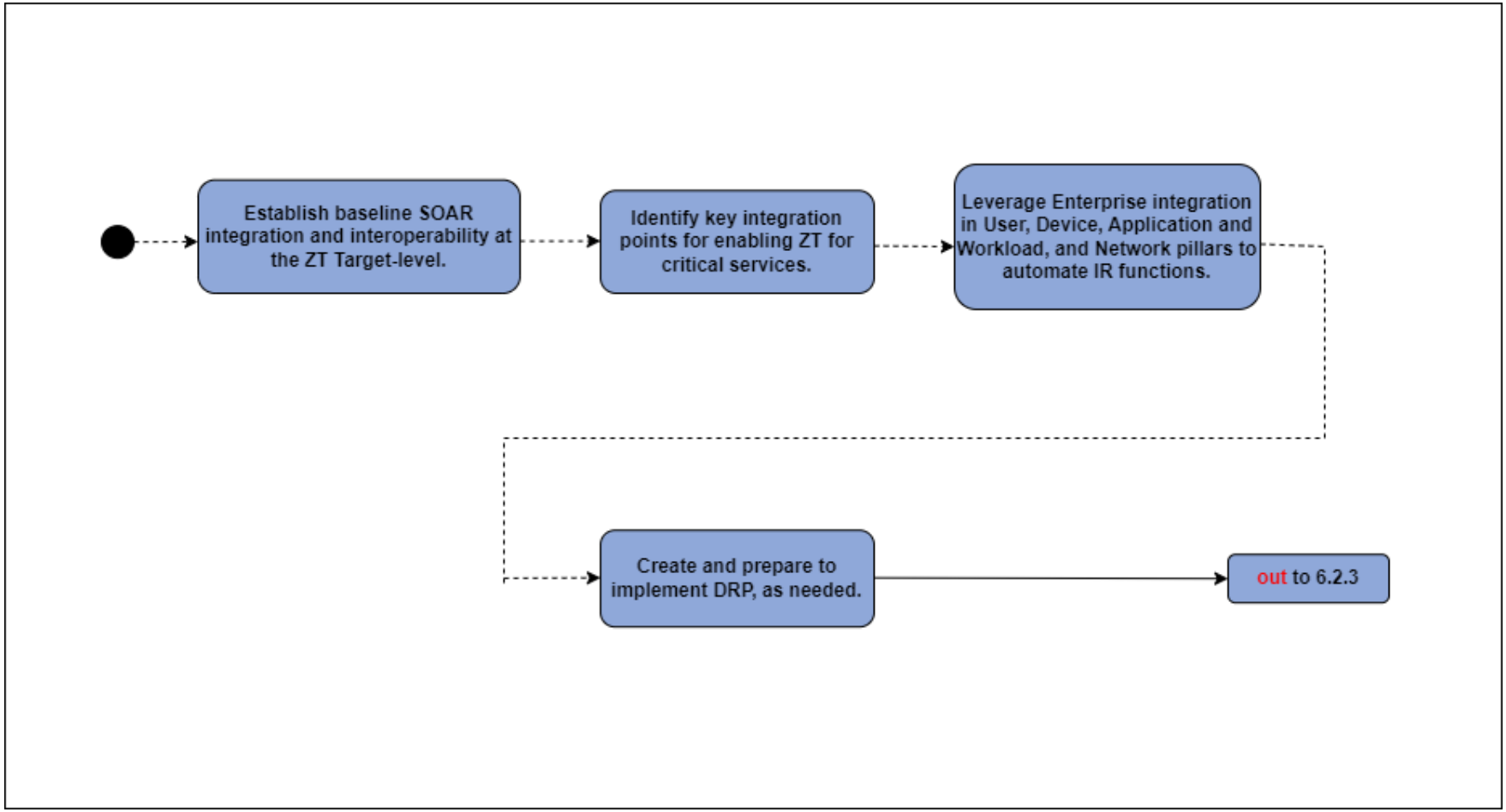

Figure D- 72: Implementation Tasks for Activity 6.2.2 — Enterprise Integration and Workflow Provisioning Part 1

Activity 6.3.1 Implement Data Tagging and Classification Machine Learning (ML) Tools

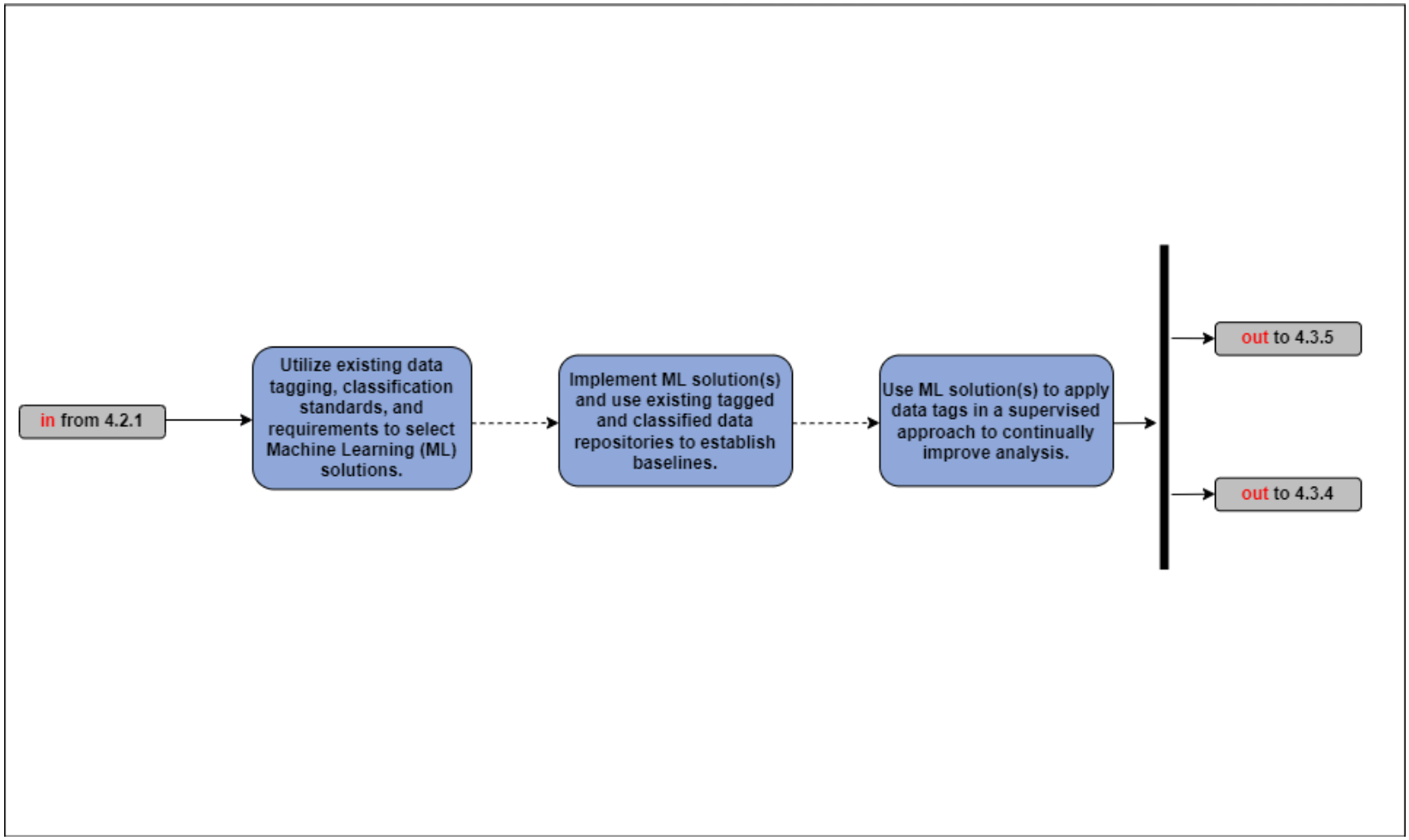

Figure D- 73: Implementation Tasks for Activity 6.3.1 — Implement Data Tagging and Classification Machine Learning (ML) Tools

Activity 6.5.1 Response Automation Analysis

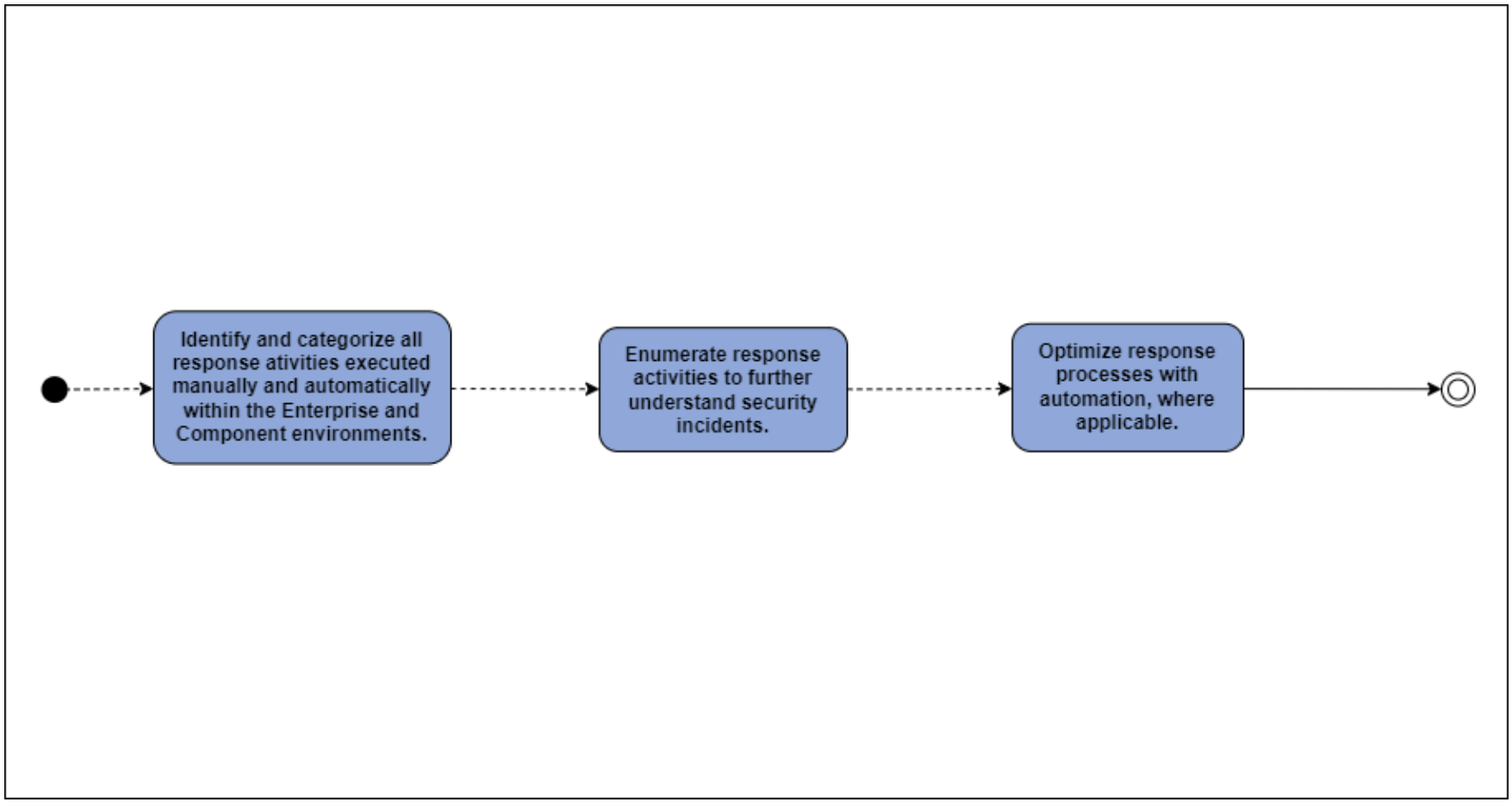

Figure D- 74: Implementation Tasks for Activity 6.5.1 — Response Automation Analysis

Activity 6.5.2 Implement Security Orchestration, Automation, and Response (SOAR) Tools

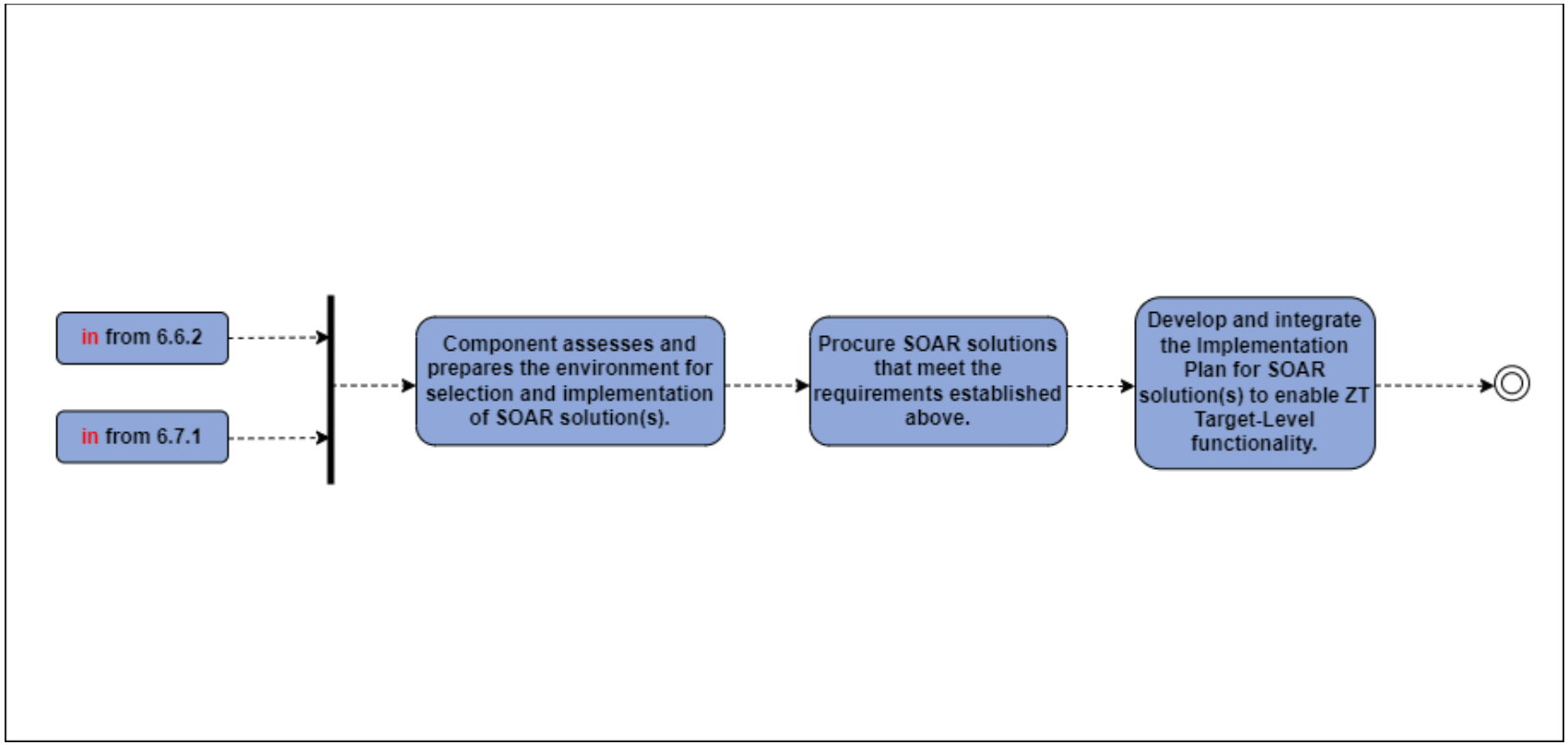

Figure D- 75: Implementation Tasks for Activity 6.5.2 — Implement Security Orchestration, Automation, and Response (SOAR) Tools

Activity 6.6.1 Tool Compliance Analysis

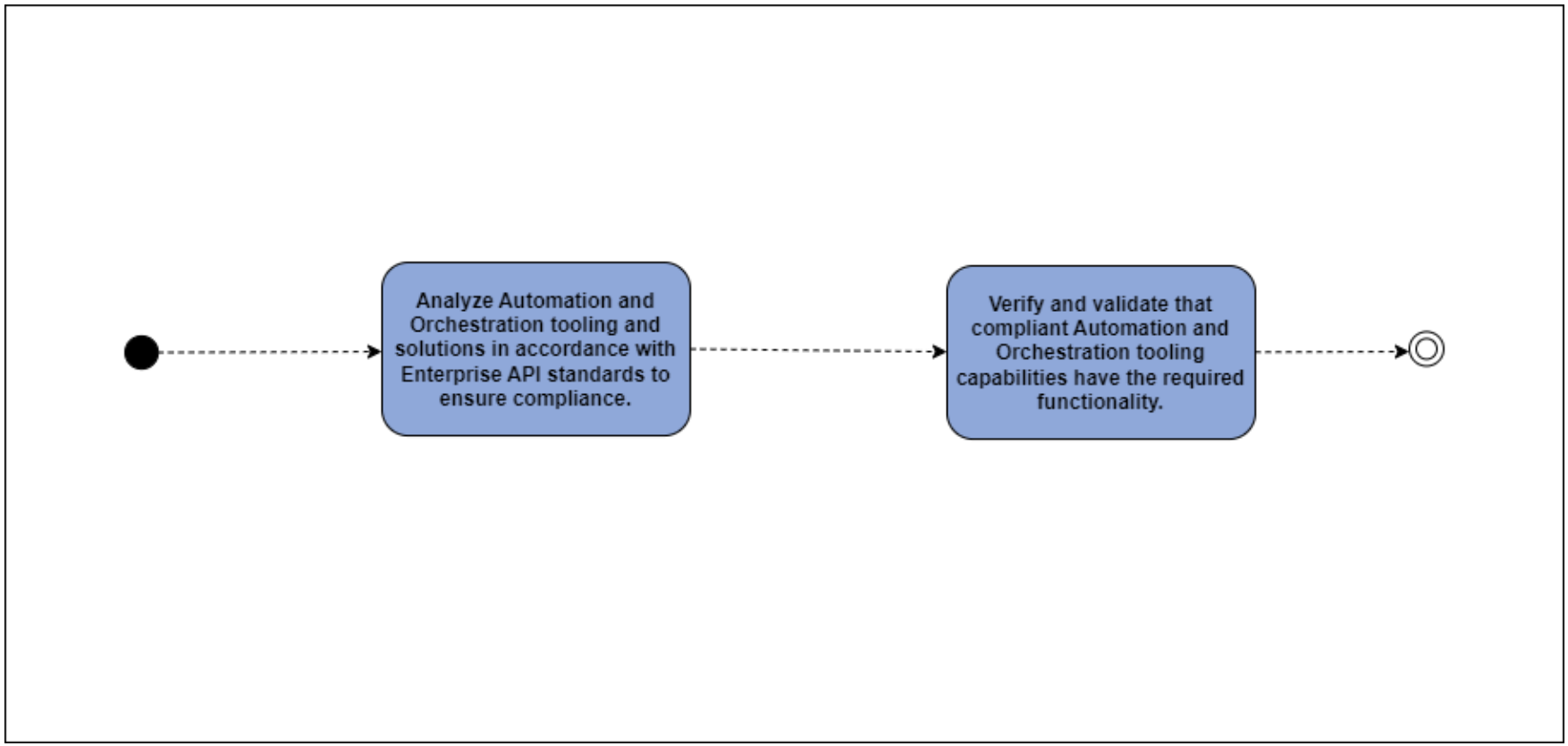

Figure D- 76: Implementation Tasks for Activity 6.6.1 — Tool Compliance Analysis

Activity 6.6.2 Standardized Application Programming Interface (API) Calls and Schemas Part 1

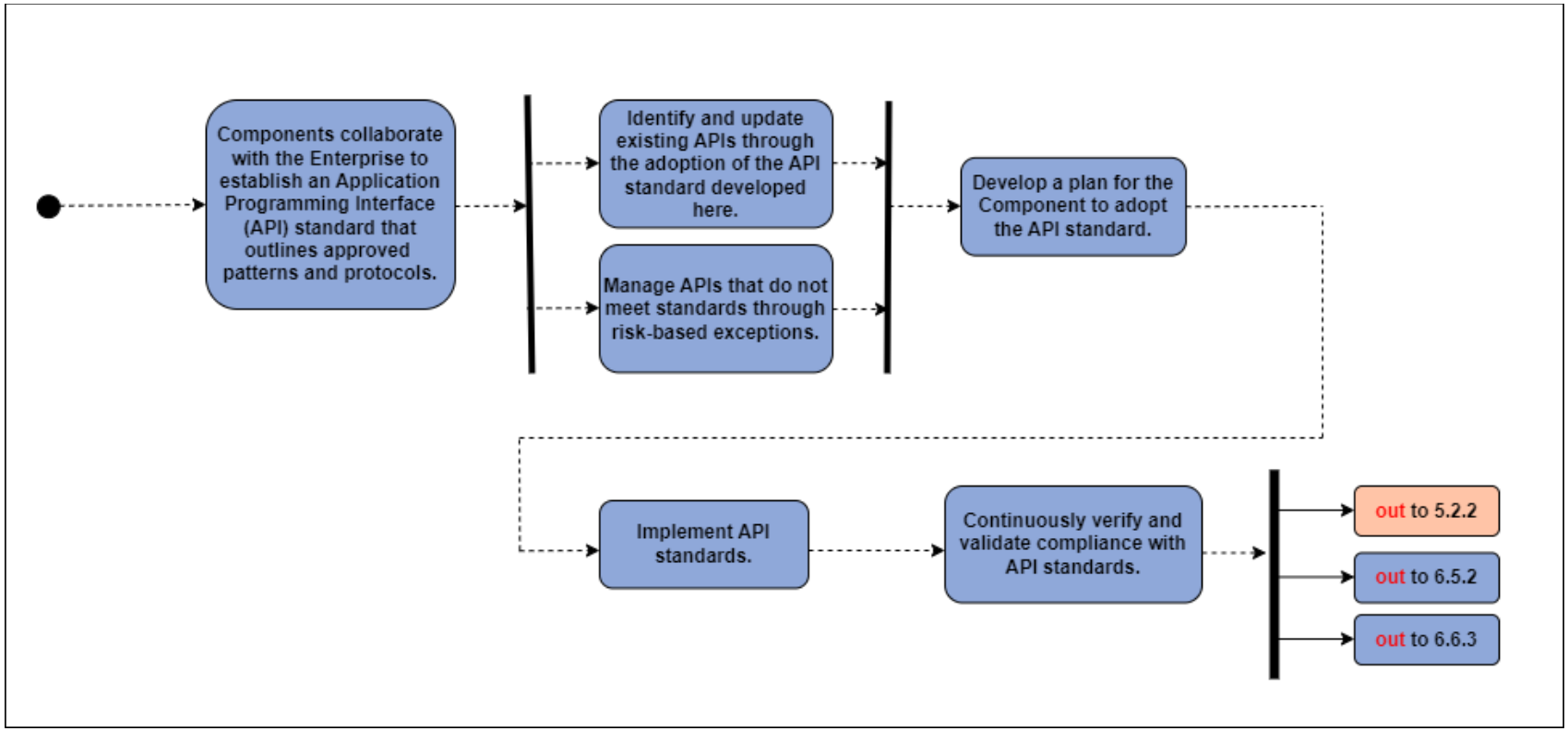

Figure D- 77: Implementation Tasks for Activity 6.6.2 — Standardized Application Programming Interface (API) Calls and Schemas Part 1

Activity 6.6.3 Standardized Application Programming Interface (API) Calls and Schemas Part 2

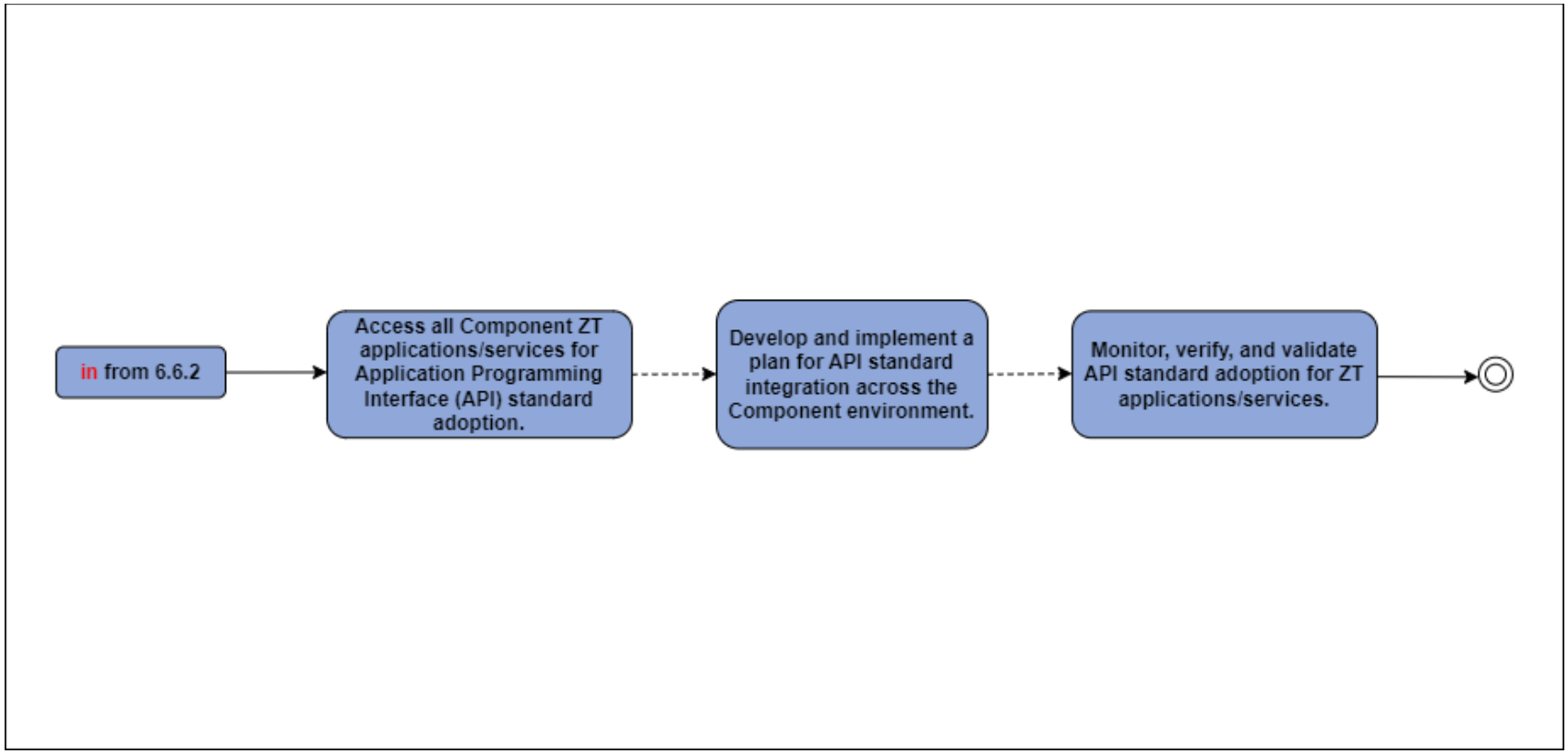

Figure D- 78: Implementation Tasks for Activity 6.6.3 — Standardized Application Programming Interface (API) Calls and Schemas Part 2

Activity 6.7.1 Workflow Enrichment Part 1

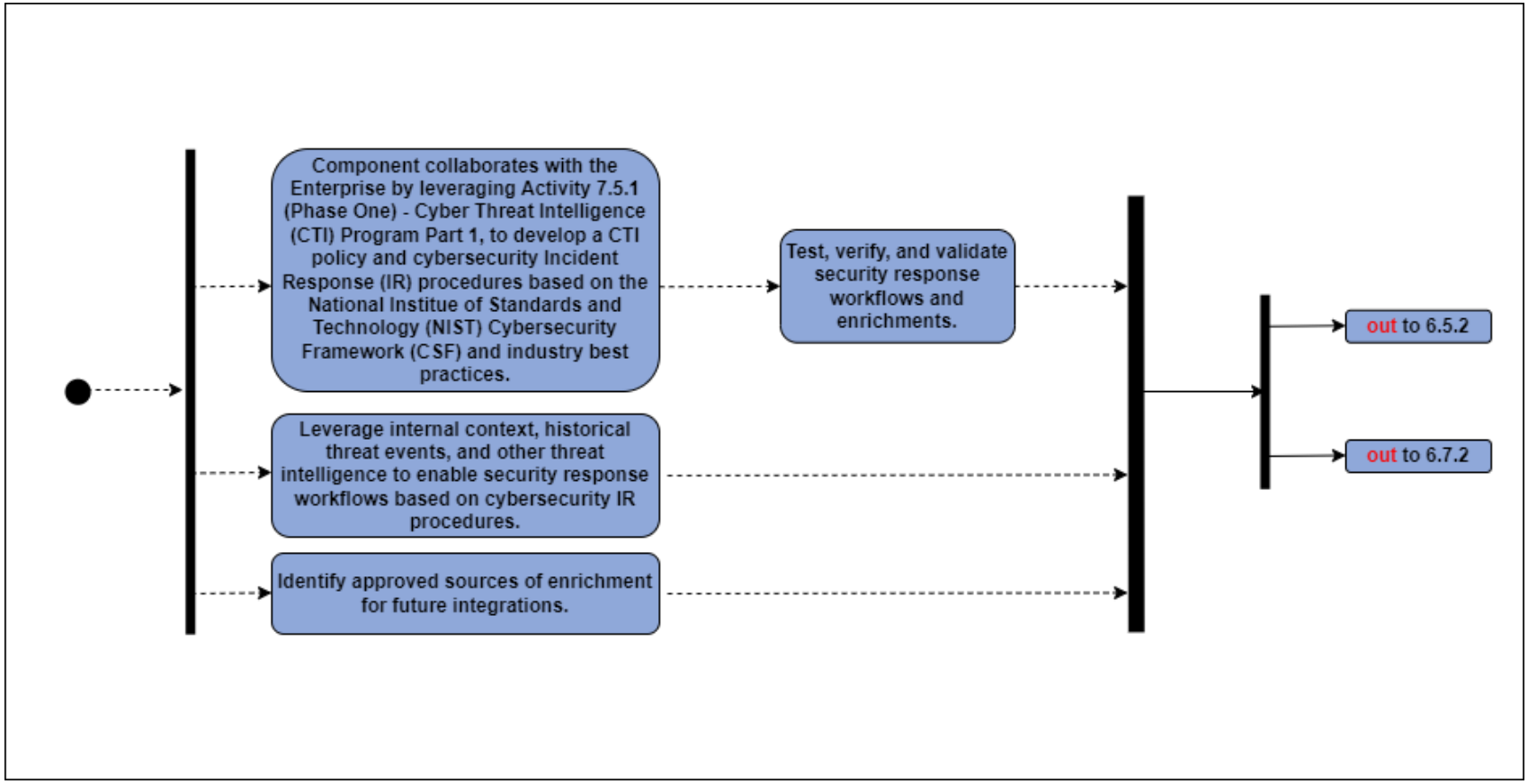

Figure D- 79: Implementation Tasks for Activity 6.7.1 — Workflow Enrichment Part 1

Activity 6.7.2 Workflow Enrichment Part 2

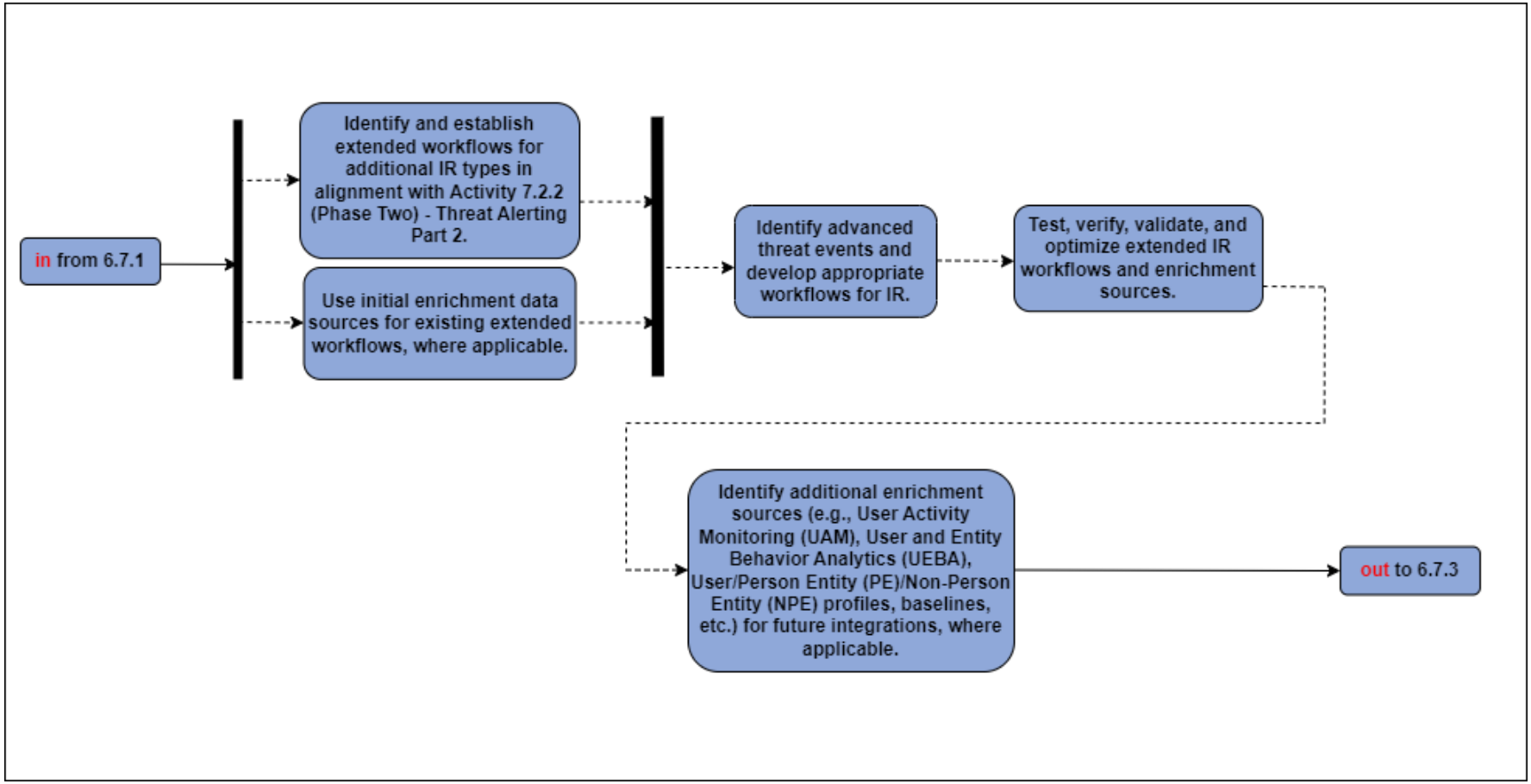

Figure D- 80: Implementation Tasks for Activity 6.7.2 — Workflow Enrichment Part 2

Activity 7.1.1 Scale Considerations

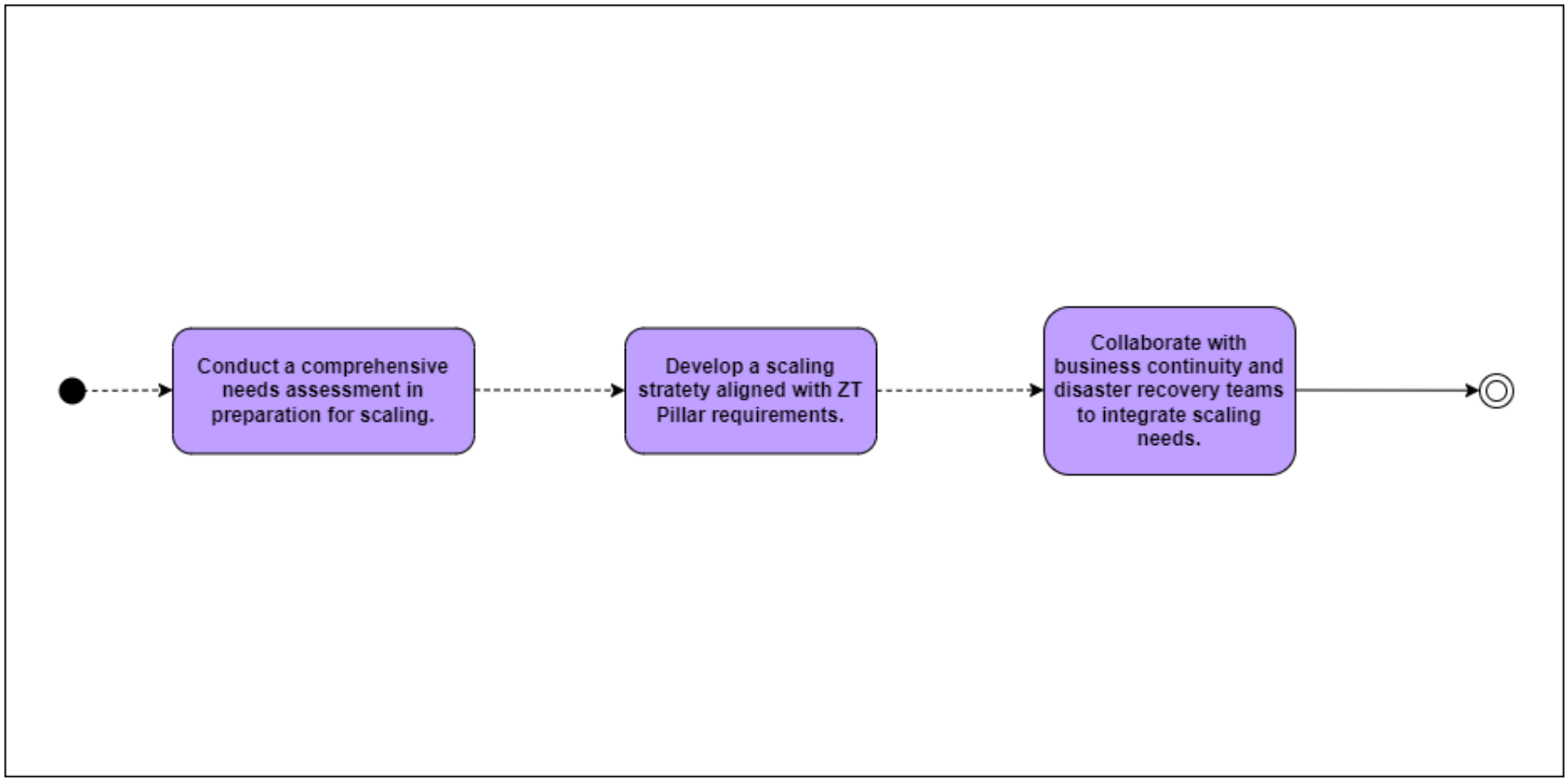

Figure D- 81: Implementation Tasks for Activity 7.1.1 — Scale Considerations

Activity 7.1.2 Log Parsing

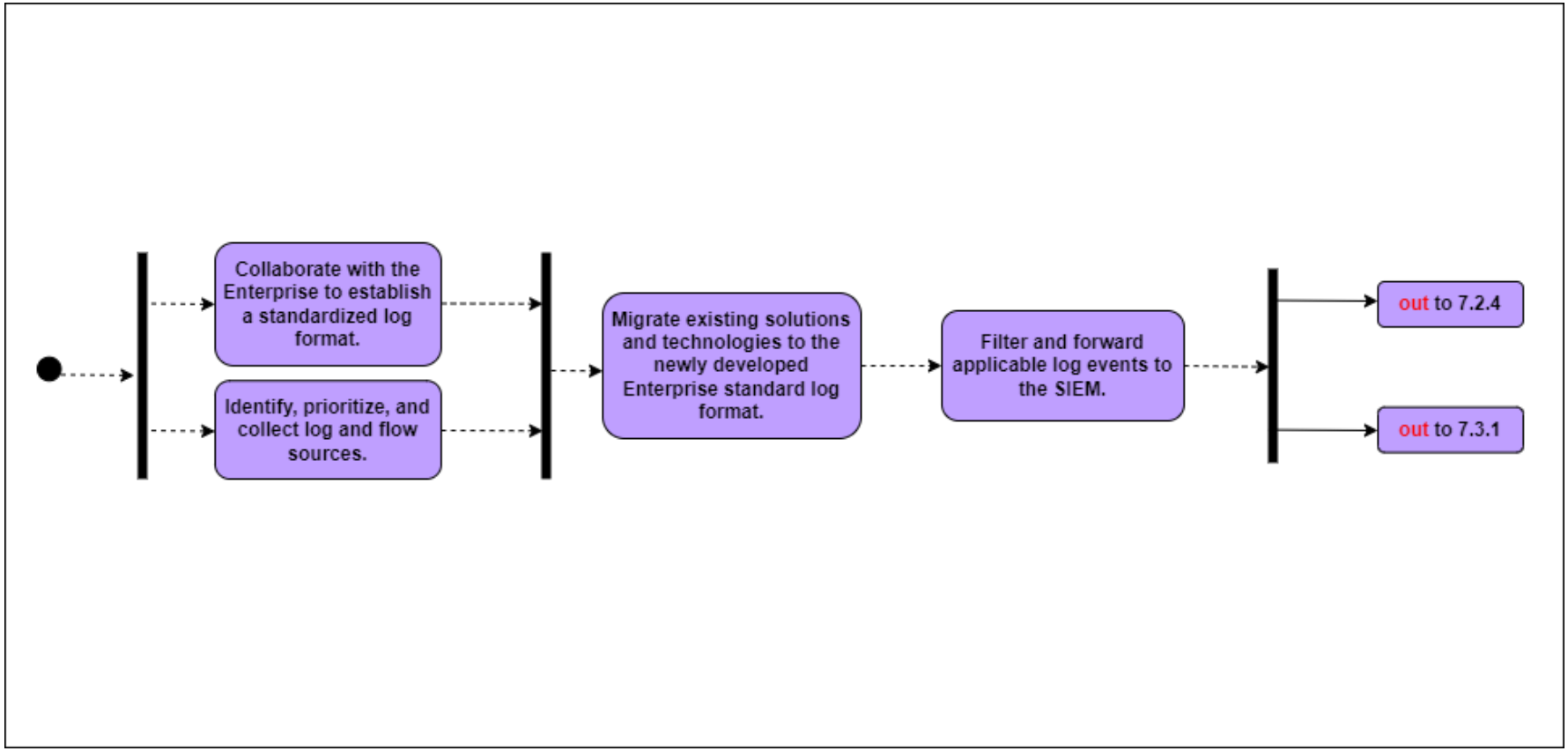

Figure D- 82: Implementation Tasks for Activity 7.1.2 — Log Parsing

Activity 7.1.3 Log Analysis

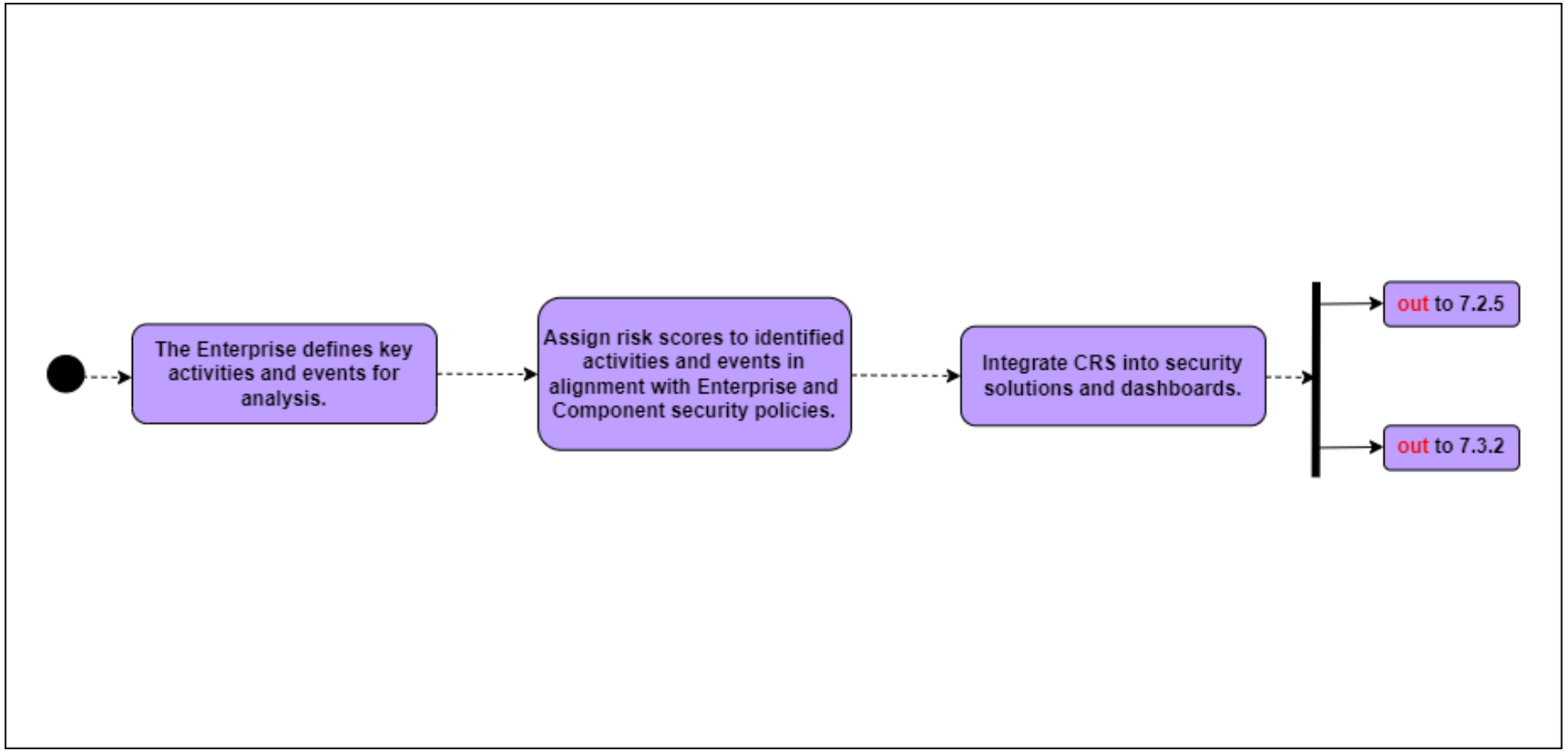

Figure D- 83: Implementation Tasks for Activity 7.1.3 — Log Analysis

Activity 7.2.1 Threat Alerting Part 1

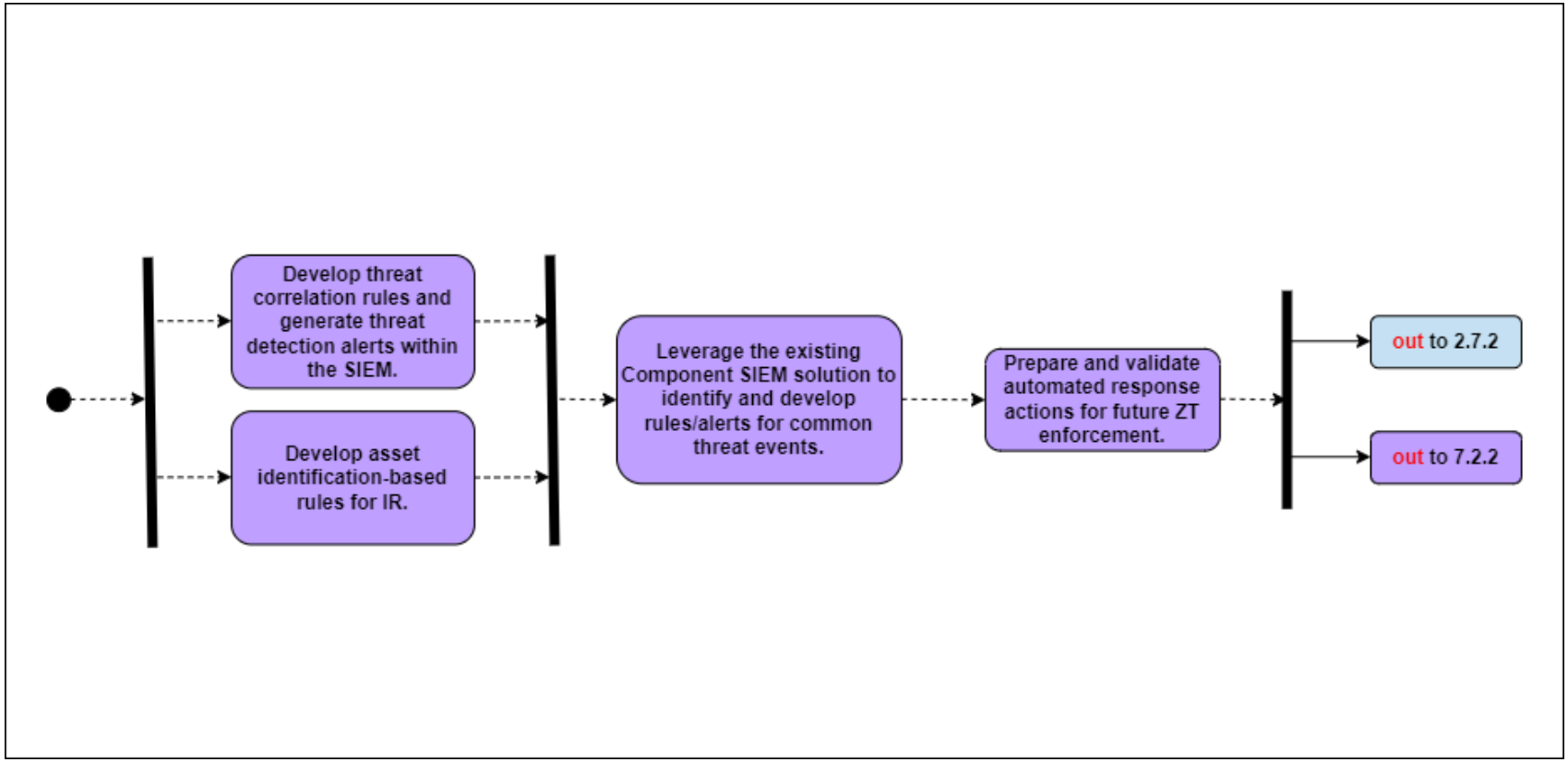

Figure D- 84: Implementation Tasks for Activity 7.2.1 — Threat Alerting Part 1

Activity 7.2.2 Threat Alerting Part 2

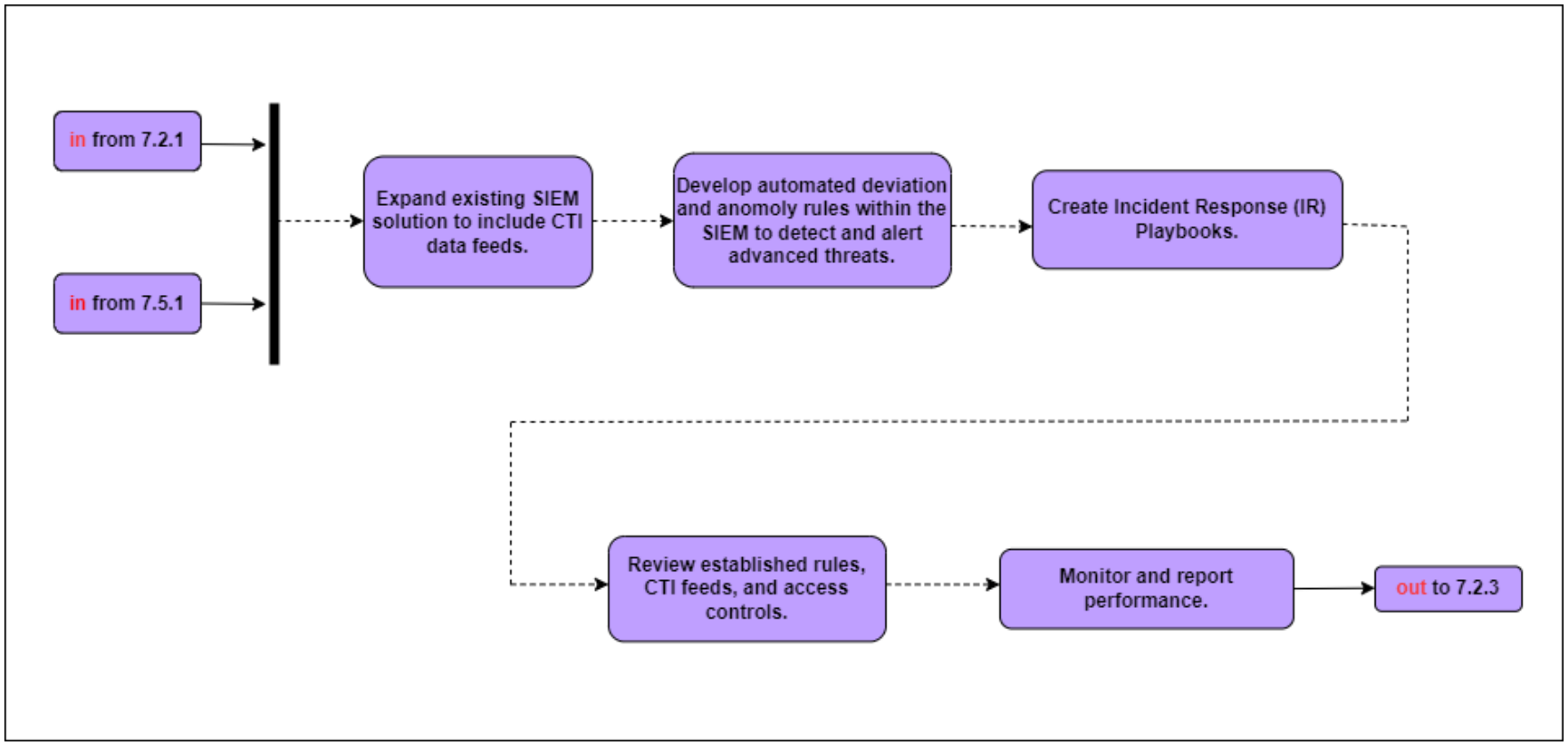

Figure D- 85: Implementation Tasks for Activity 7.2.2 — Threat Alerting Part 2

Activity 7.2.4 Asset ID and Alert Correlation

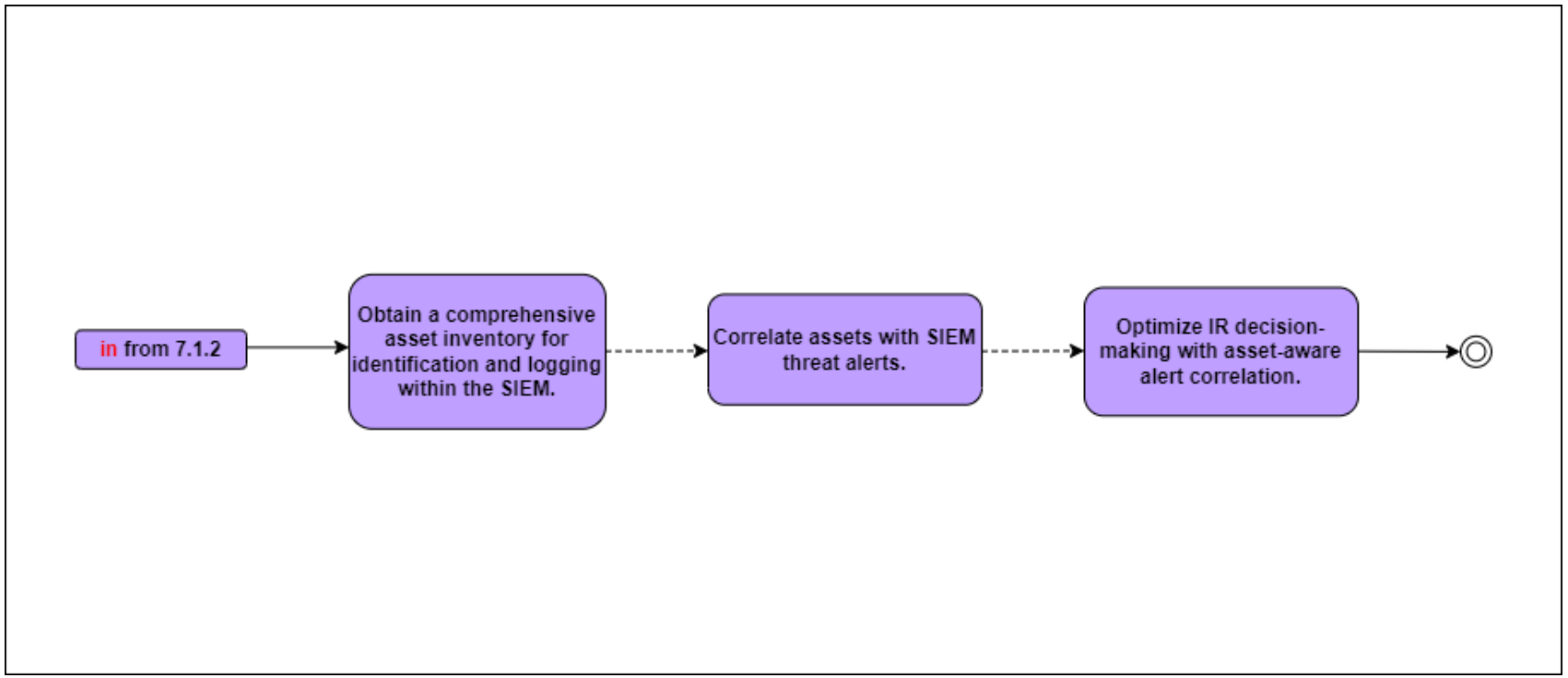

Figure D- 86: Implementation Tasks for Activity 7.2.4 — Asset ID and Alert Correlation

Activity 7.2.5 User and Device Baselines

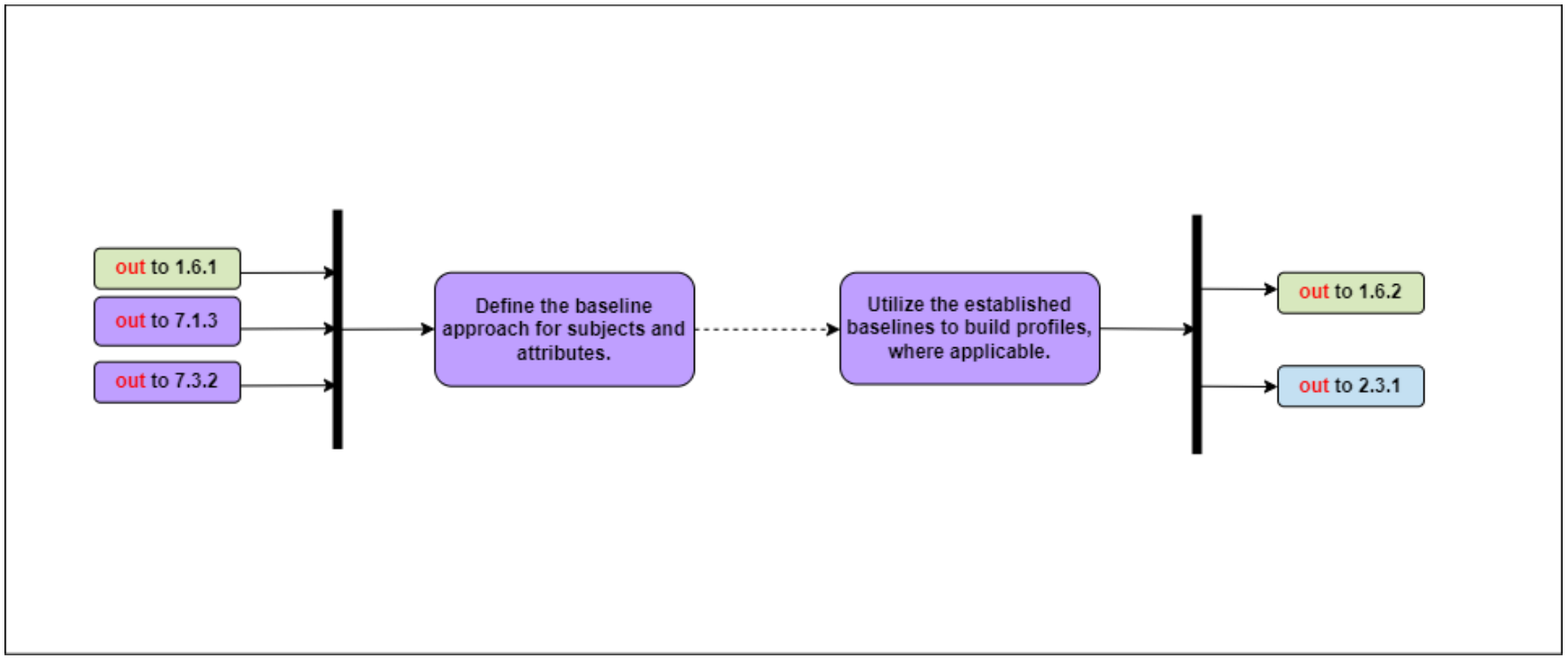

Figure D- 87: Implementation Tasks for Activity 7.2.5 — User and Device Baselines

Activity 7.3.1 Implement Analytics Tools

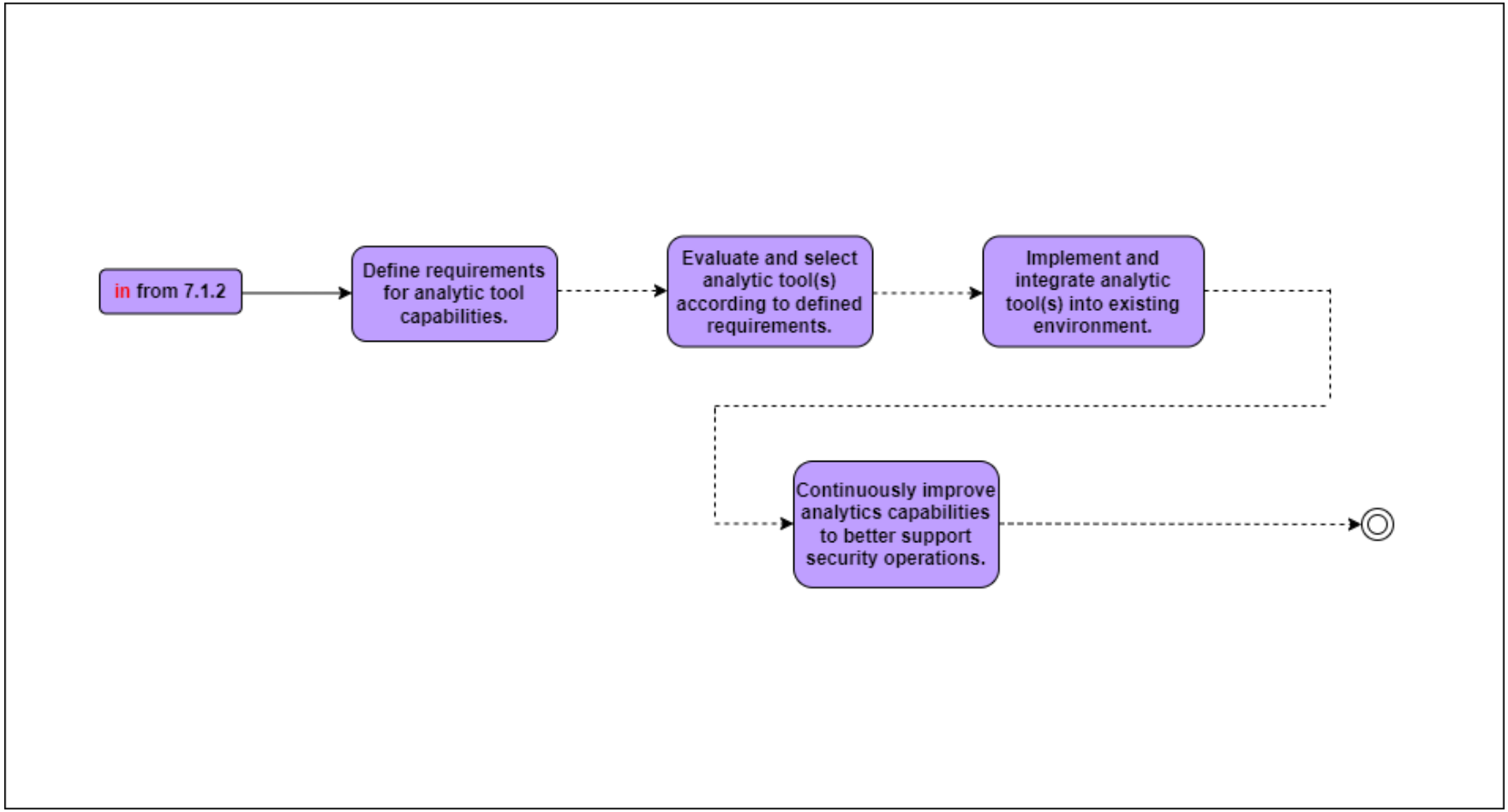

Figure D- 88: Implementation Tasks for Activity 7.3.1 — Implement Analytics Tools

Activity 7.3.2 Establish User Baseline Behavior

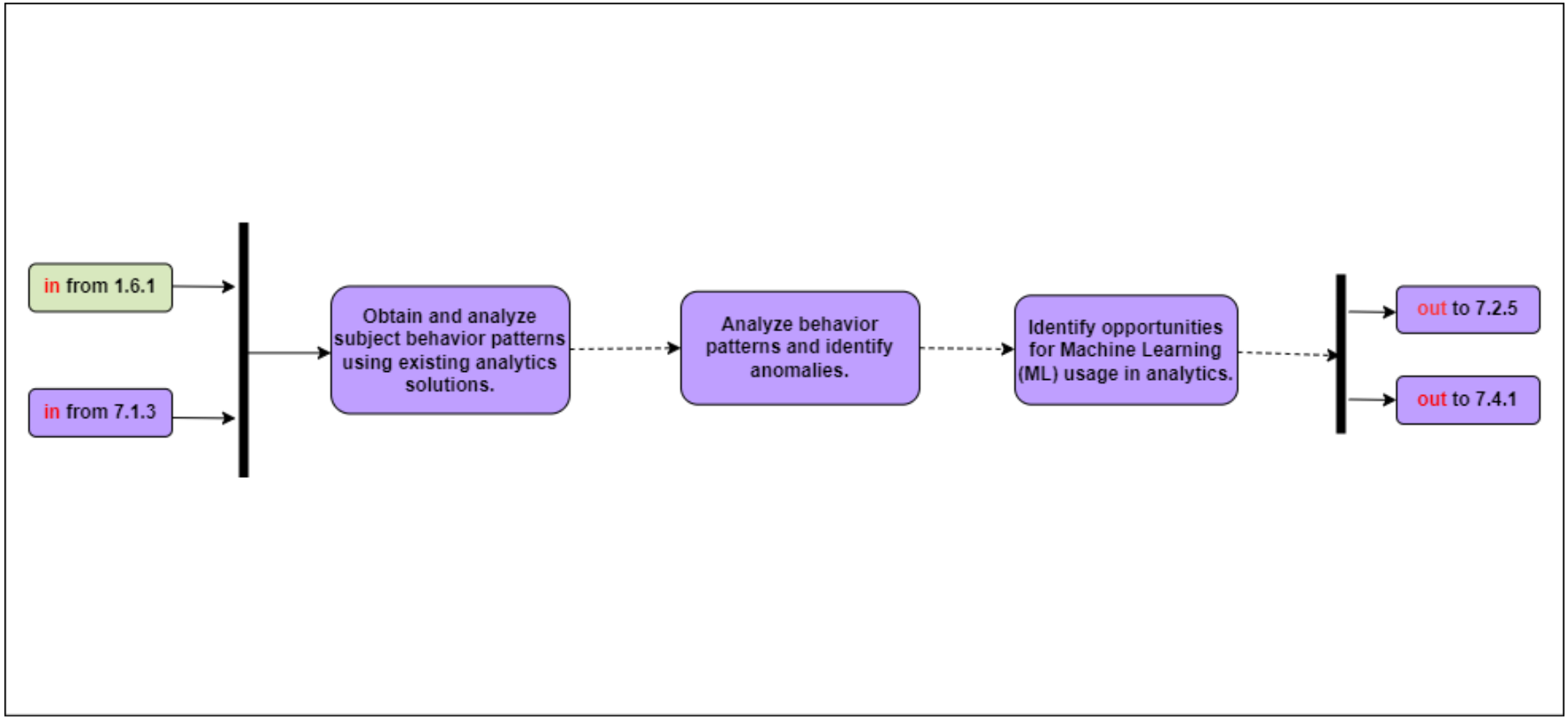

Figure D- 89: Implementation Tasks for Activity 7.3.2 — Establish User Baseline Behavior

Activity 7.4.1 Baseline and Profiling Part 1

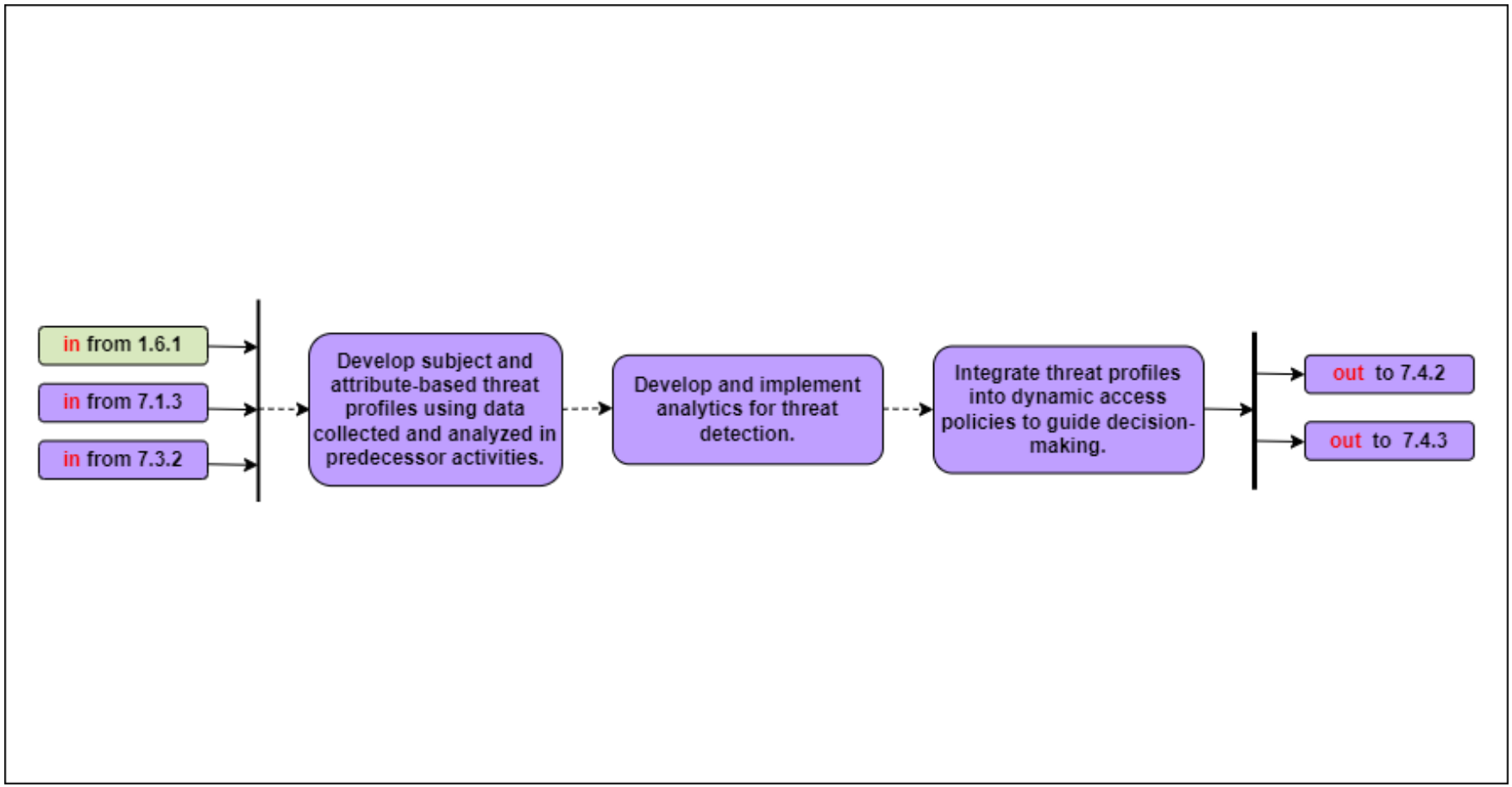

Figure D- 90: Implementation Tasks for Activity 7.4.1 — Baseline and Profiling Part 1

Activity 7.5.1 Cyber Threat Intelligence Program Part 1

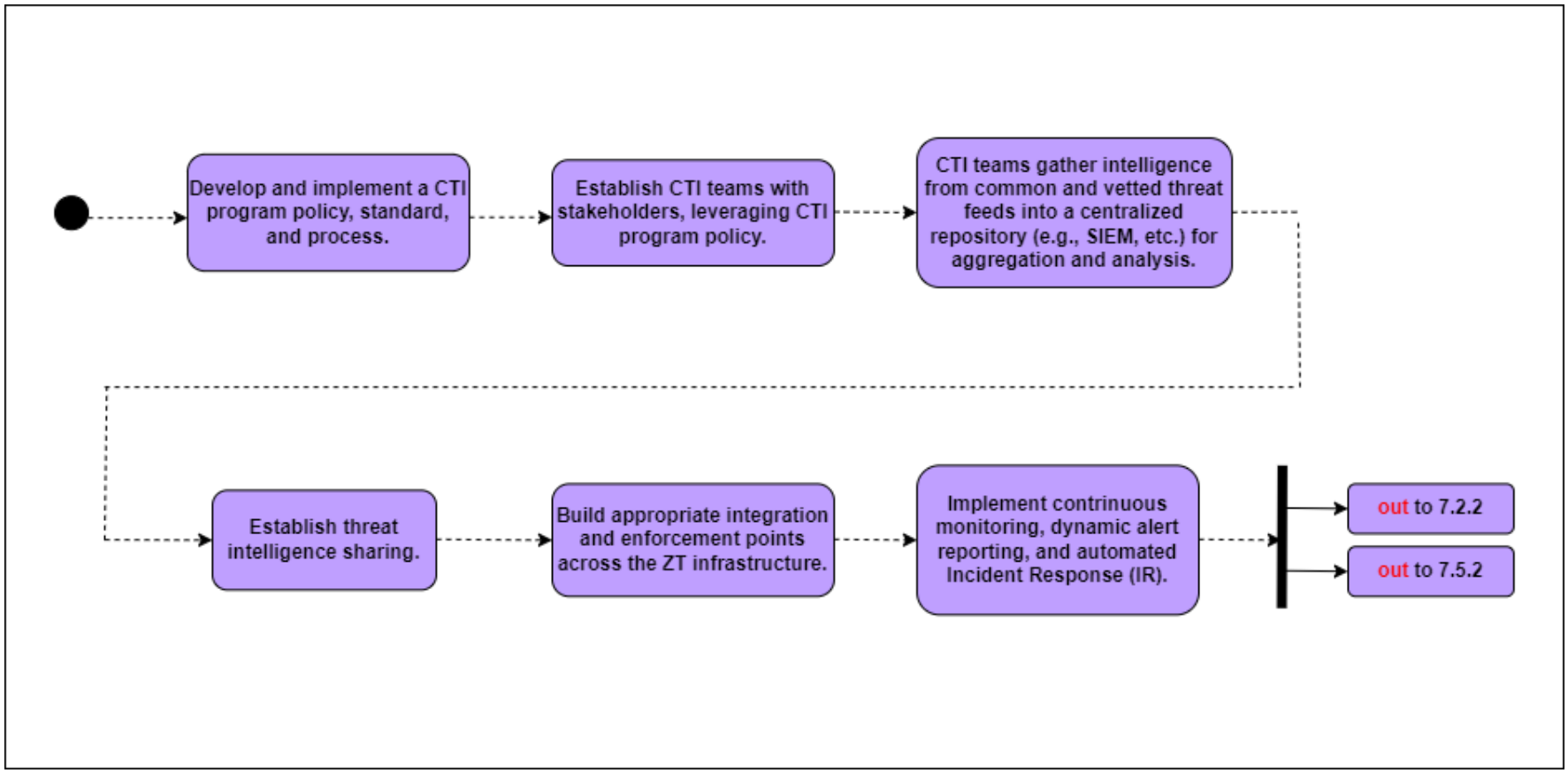

Figure D- 91: Implementation Tasks for Activity 7.5.1 — Cyber Threat Intelligence Program Part 1

Activity 7.5.2 Cyber Threat Intelligence Program Part 2

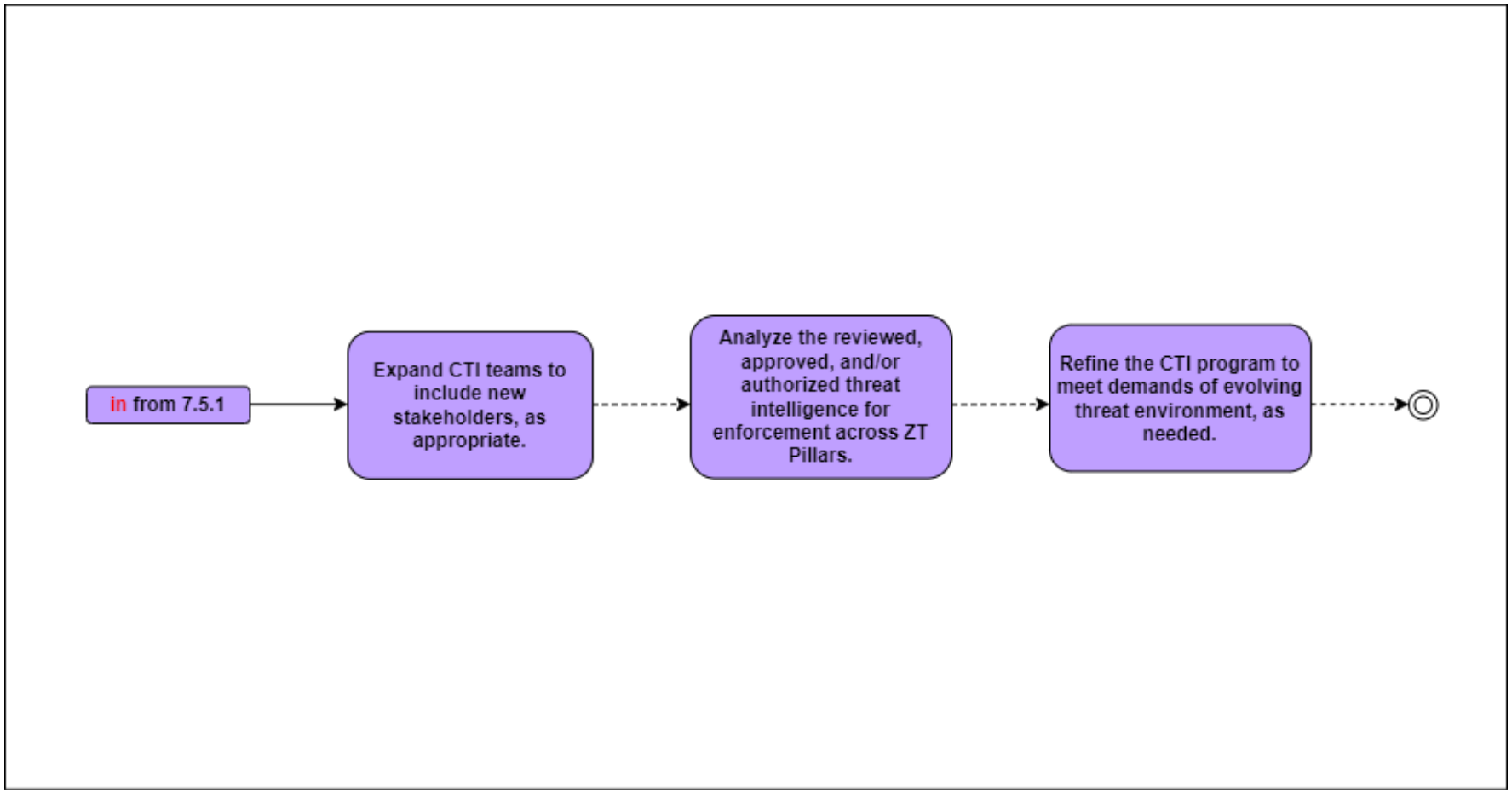

Figure D- 92: Implementation Tasks for Activity 7.5.2 — Cyber Threat Intelligence Program Part 2