Threat Prioritization Plan

Revision

Version 13
9/19/23 2:41 PM

SME

Charles Wilson

Abstract

This document details the process to be used to formally develop threat models and process the results from that activity into actionable issues able to be dispositioned by development teams.

Group / Owner

Security / Systems Requirements Planner

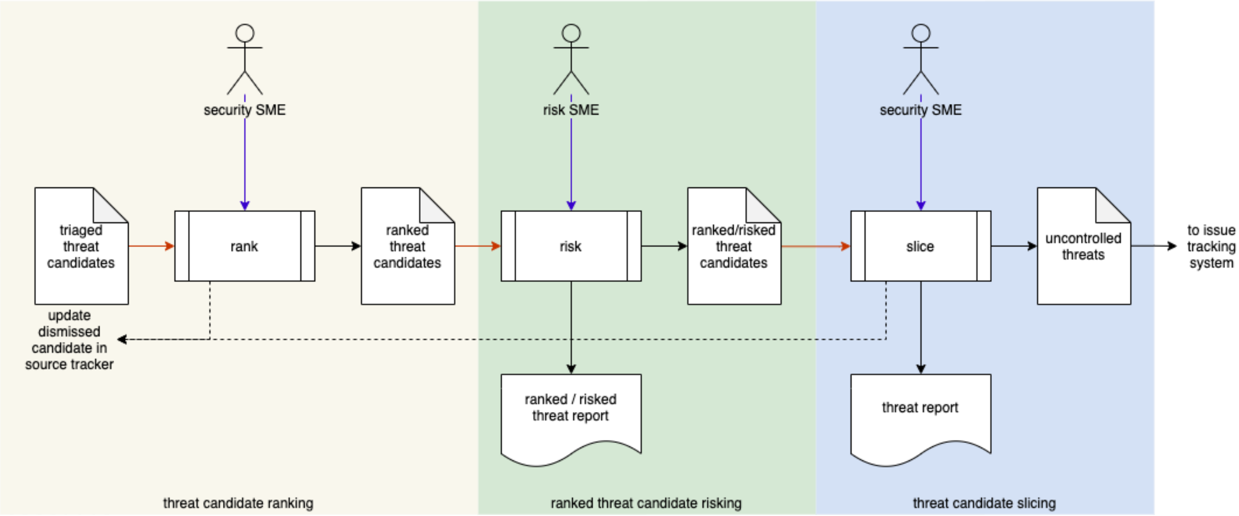
Motivation

This document is motivated by the need to have formal processes in place regarding discovery and disposition of security-related threats to allow for certification of compliance to standards such as **ISO/SAE 21434** and **ISO 26262**.

License

Overview

The following diagram illustrates the process to be used:

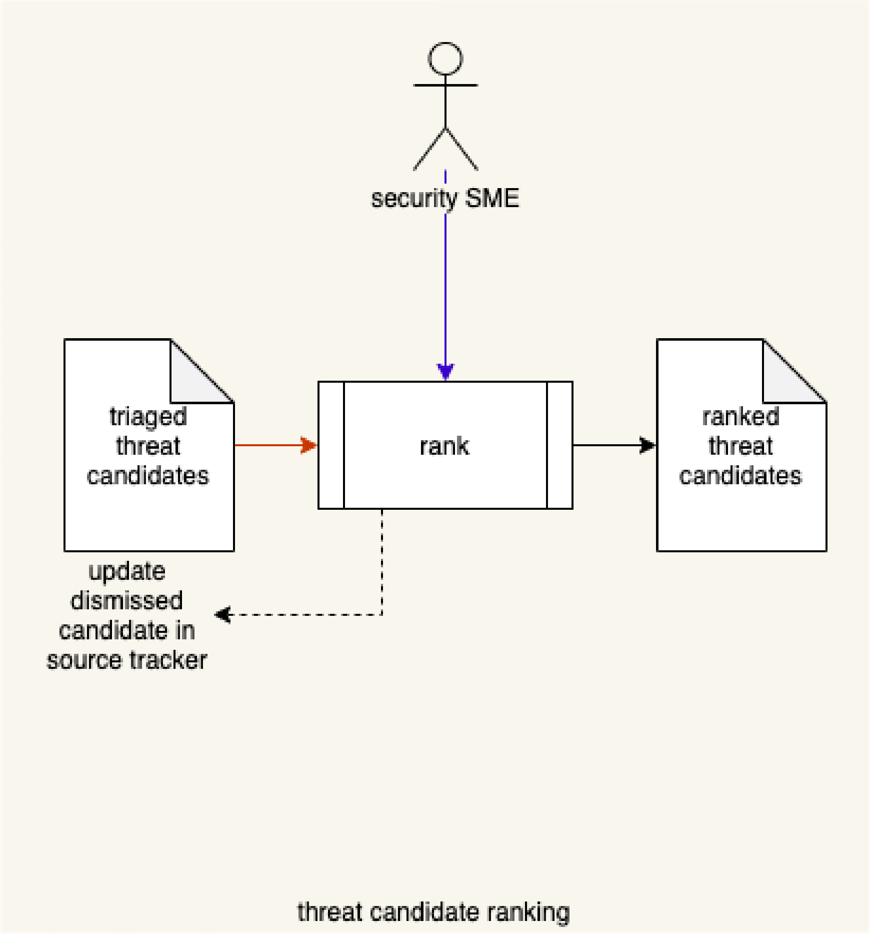


Note: The above methodology follows that described in guidance from NIST SP 800-30 [9].

Process

Threat Candidate Ranking

Inputs	Triaged threat candidates
Outputs	Ranked threat candidates
Participants	Security SME


security SME
triaged threat candidates
rank
ranked threat candidates
update dismissed candidate in source tracker
threat candidate ranking

The **triaged threat candidates** are ranked in order to establish their relative exploitability. This should be done using a standard ranking methodology such as the Common Vulnerability Scoring System (**CVSS**) [5].

The ranking should consider aspects such as:

- Mechanism
- Locality
- Maturity
- Scope
- Required privileges

The ranking system may lend itself to coarse ranking (by range).

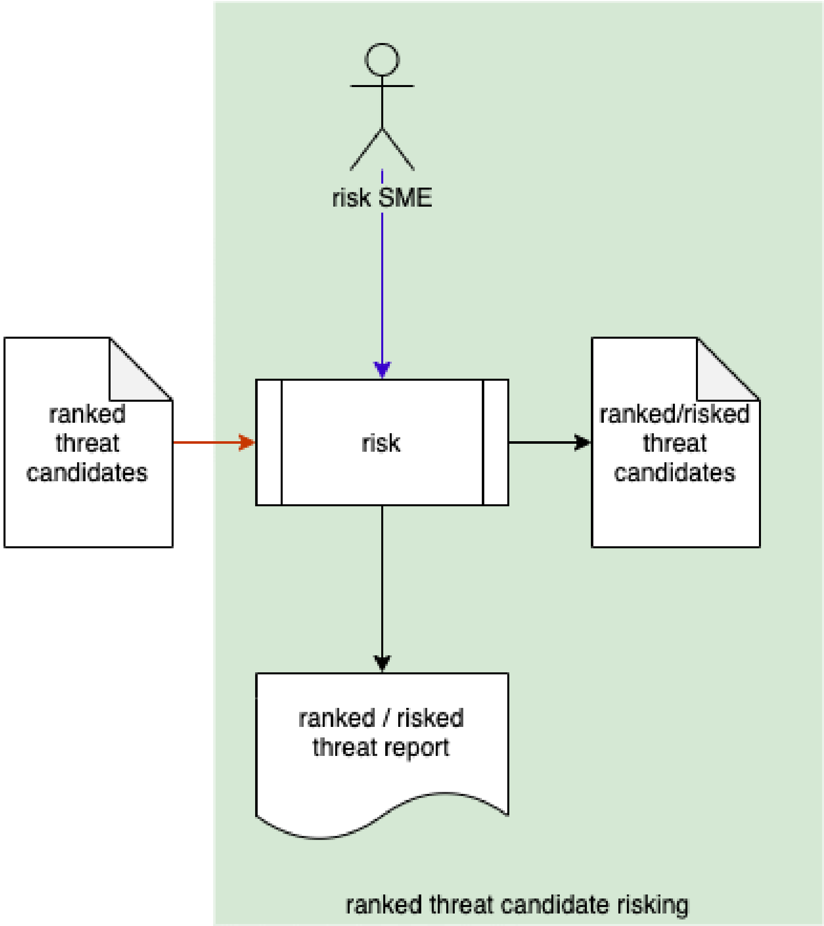
Once ranked, a threshold may be applied to reduce the number of threat candidates needing to be considered in the risk step. If a threshold is applied, the dismissed candidates must be documented in the candidate's source tracker.

Note: The **triaged threat candidates** may be sourced from several activities, including:

- Threat modeling [2]
- Incident response [3]
- Attack surface analysis [4]

Ranked Threat Candidate Risking

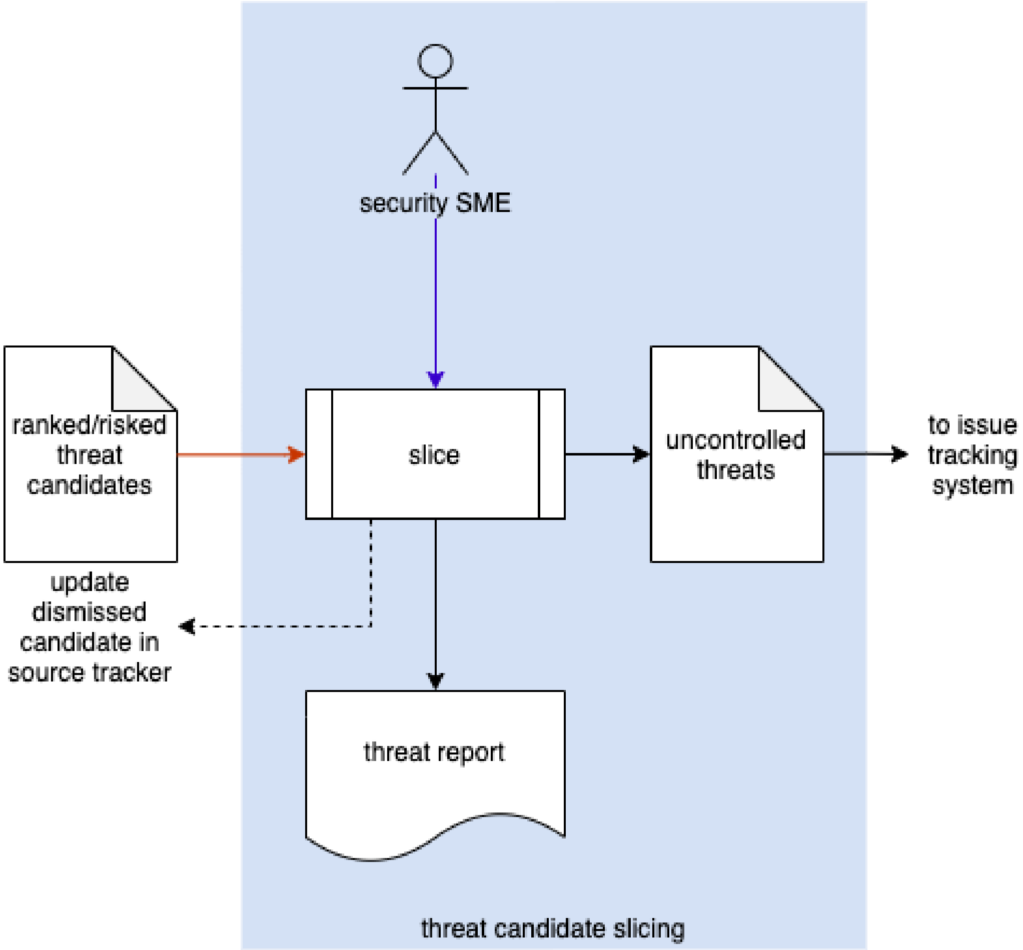
Inputs	Ranked threat candidates
Outputs	Risked threat candidates Ranked / risked threat report
Participants	Risk SME


risk SME
ranked threat candidates
risk
ranked/risked threat candidates
ranked / risked threat report
ranked threat candidate risking

The ranked threat candidates meeting the threshold of consideration are reviewed by the risk SME to determine their severity of harm. A **ranked / risked threat report** is generated.

Threat Candidate Slicing

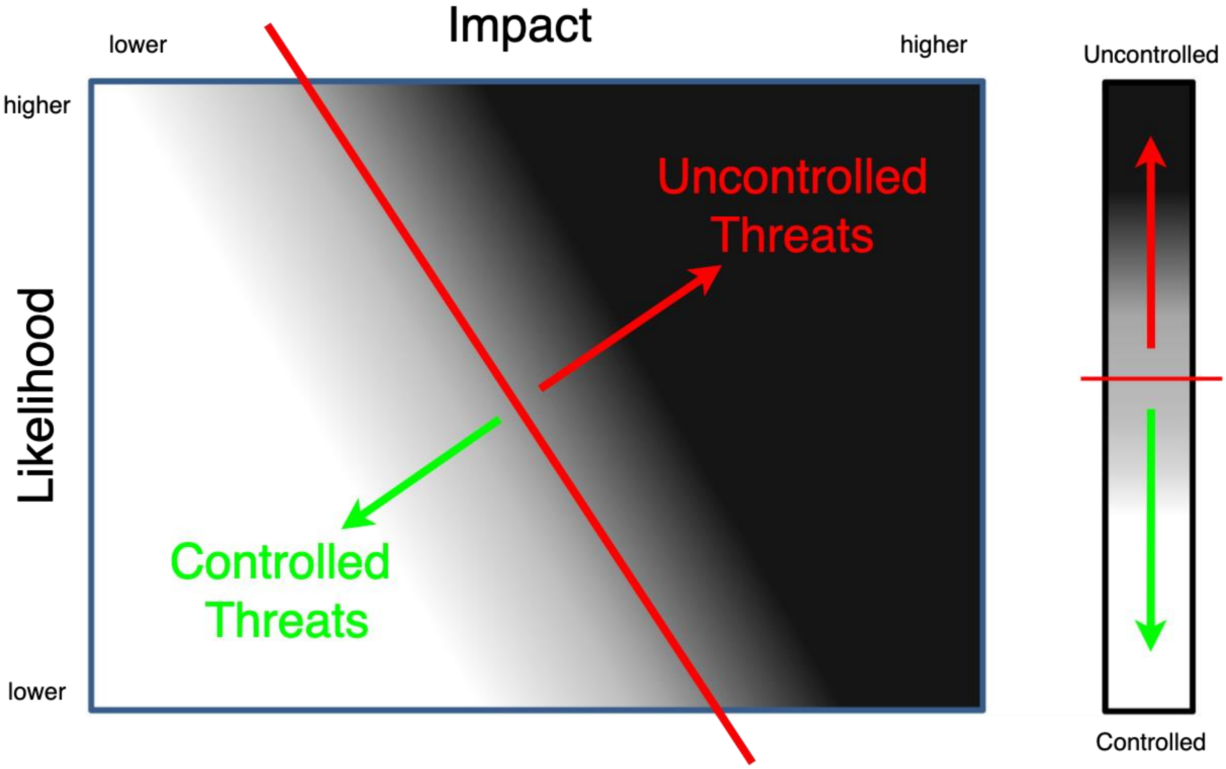
Inputs	Risked threat candidates
Outputs	Uncontrolled threats Threat report
Participants	Security SME



The threat candidates which have been both ranked and risked are sliced (bisected) to determine which ones are considered to have uncontrolled risk. These are designated as uncontrolled threats and forwarded to the **issue tracking system**. If an issue is determined to be controlled, an **update dismissed candidate notification** is sent to the **source tracker** to document this. A **threat report** is generated.

Note: It is the responsibility of the standard issue management processes to dispose of uncontrolled issues applying the standard treatments (avoid, reduce, share, retain). This includes documenting the risk aspects of the issue and the reason for the disposition.

The following diagram illustrates issue slicing.



Note: Adapted from **Postmarket Management of Cybersecurity in Medical Devices** [10].

Here we are showing the values from ranking (likelihood) and risking (impact) as continuous. The level of risk control is also shown as continuous from white (completely controlled) to black (completely uncontrolled). In practice, all of these values are quantized. Finally, our desire is to bisect the space by choosing a minimum level of acceptable risk. This yields a line (risk appetite) through the exploitability-severity space above which threats are deemed to be uncontrolled (in need of mitigation), as indicated with the red line and arrow.

Note: Additional information regarding the mapping of various ranking and risking methodologies into the notation specified by **ISO 21434** can be found in the **Ranked / Risked Threat Report** [7]**.**

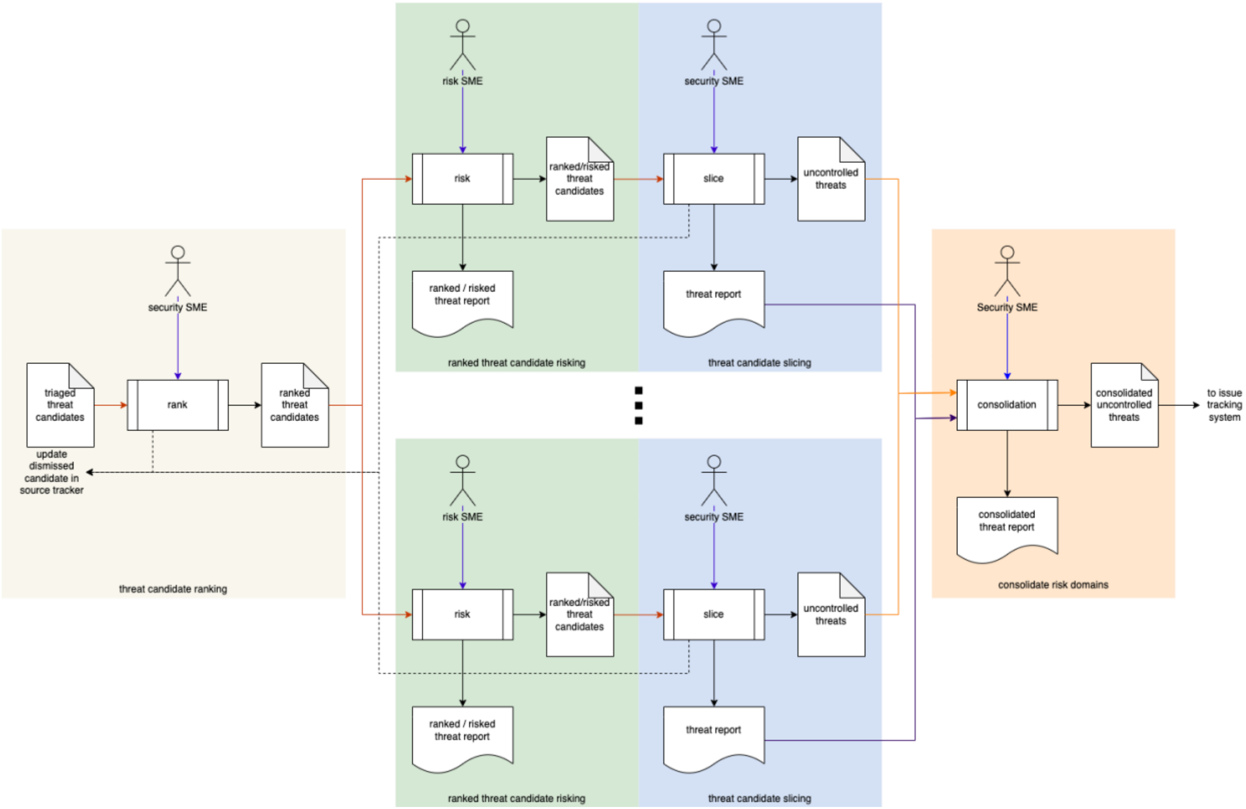
Note: The issue of reporting when multiple risk dimensions are considered, as by **ISO 21434**, is addressed in the **Threat Report** [8]**.**

If a threat candidate is determined to be controlled, it is dismissed and must be documented in the candidate's source tracker. **Uncontrolled threats** will be entered into the defect tracking system for disposition by development.

Note: The bisection line is determined by the organization's risk acceptance level.

Multi-risk Domain Considerations

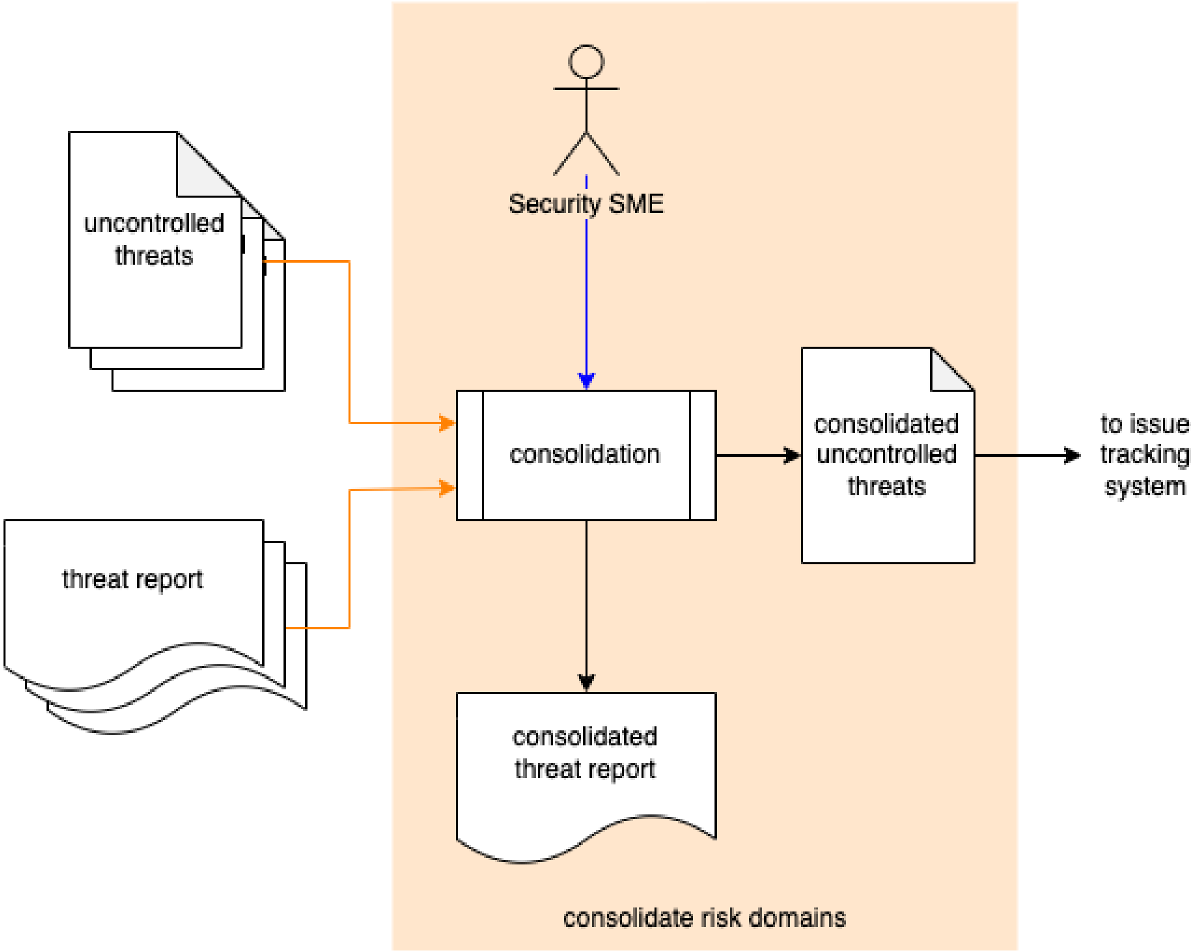
In those situations where multiple risk domains need to be taken into consideration, such as those specified in **EVITA** [11], the following diagram illustrates the process to be used:


risk SME
security SME
risk
ranked/risked threat candidates
slice
uncontrolled threats
ranked / risked threat report
threat report
ranked threat candidate risking
threat candidate slicing
security SME
triaged threat candidates
rank
ranked threat candidates
update dismissed candidate in source tracker
threat candidate ranking
Security SME
consolidation
consolidated uncontrolled threats
to issue tracking system
consolidated threat report
consolidate risk domains
risk SME
security SME
risk
ranked/risked threat candidates
slice
uncontrolled threats
ranked / risked threat report
threat report
ranked threat candidate risking
threat candidate slicing

Here we see that in addition to the risk and slicing processes being replicated for each of the risk domain, the output of these must be consolidated and the threat de-duplicated.

Consolidate Risk Domains

Inputs	Uncontrolled threats (all domains) Threat reports (all domains)
Outputs	Consolidated uncontrolled threats Consolidated threat report
Participants	Security SME



The **uncontrolled threats** and **threat reports** from all risk domains are consolidated by the security SME. This results in the creation of a set of **consolidated uncontrolled threats** and a **consolidated threat report**. The consolidated uncontrolled threats are entered into the **issue tracking system**.

Note: The consolidated uncontrolled threats should be deduplicated**.**

References

1. **Document Management Standard**
   https://en.wikipedia.org/wiki/Document_management_system
2. **Threat Modeling Report** (AVCDL secondary document)
3. **Incident Response Plan** (AVCDL secondary document)
4. **Attack Surface Analysis Report** (AVCDL secondary document)
5. **Common Vulnerability Scoring System**
   https://www.first.org/cvss/
6. **NIST SP 800-39 - Managing Information Security Risk - *Organization, Mission, and Information System View***
   https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
7. **Ranked / Risked Threat Report** (AVCDL secondary document)
8. **Threat Report** (AVCDL secondary document)
9. **NIST SP 800-30 r1 - Guide for Conducting Risk Assessments**
   https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
10. **Postmarket Management of Cybersecurity in Medical Devices**
    https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices
11. **EVITA D2.3 Security requirements for automotive on-board networks based on dark-side scenarios**
    https://zenodo.org/record/1188418/files/EVITAD2.3v1.1.pdf