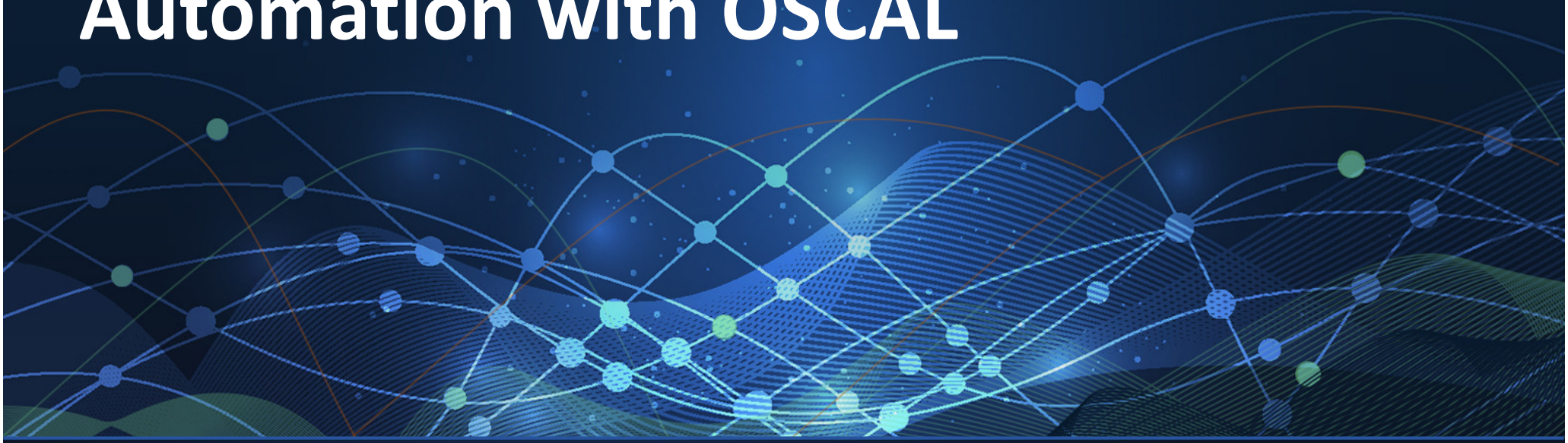
BloSS@M: Security Assessment Automation with OSCAL



National Institute of Standards and Technology
U.S. Department of Commerce

ITL/CSD/OSCAL Team

3rd OSCAL Workshop

Why do we need BloSS@M?

Agencies need

- to acquire software.
- allocate software licenses.
- securely operate and manage the software in their environment.
- understand the impact of that software on their environment.

What is BloSS@M?

A proof-of-concept software asset management system that:

- Enables upward aggregation, downward distribution, and sharing of software assets
- Proposes a mutual trust system where agencies deploy peer nodes in a multi-agency consortium
- Is built using Hyperledger Fabric's permissioned blockchain
- Demonstrates security assessment automation & continuous ATO with OSCAL

Why DevSecOps?

National Institute of Standards and Technology
U.S. Department of Commerce

ITL/CSD/OSCAL Team

3rd OSCAL Workshop

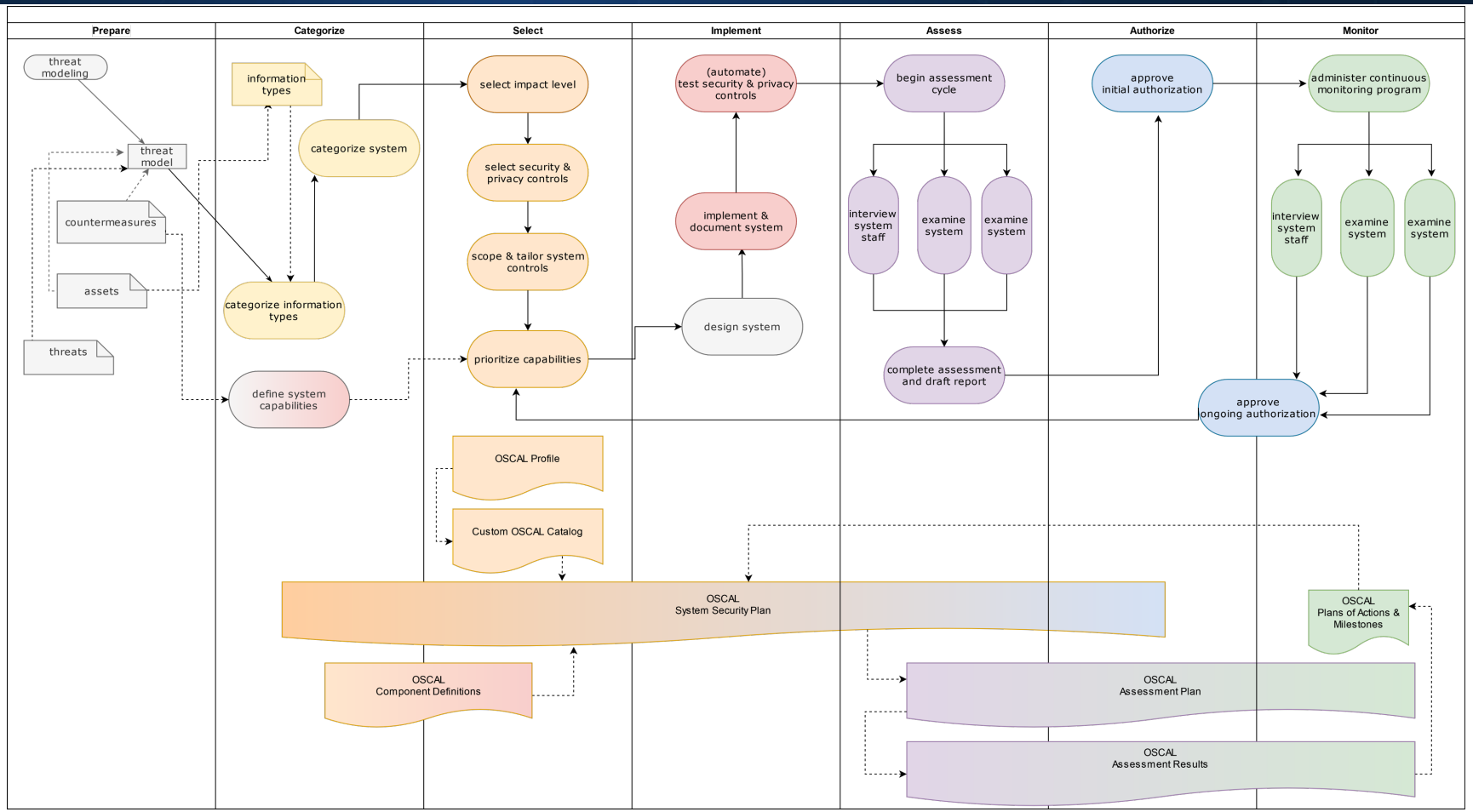
How do Sec across Dev and Ops?

- Why do we secure first?
- How do we secure first?
- What do we secure first?

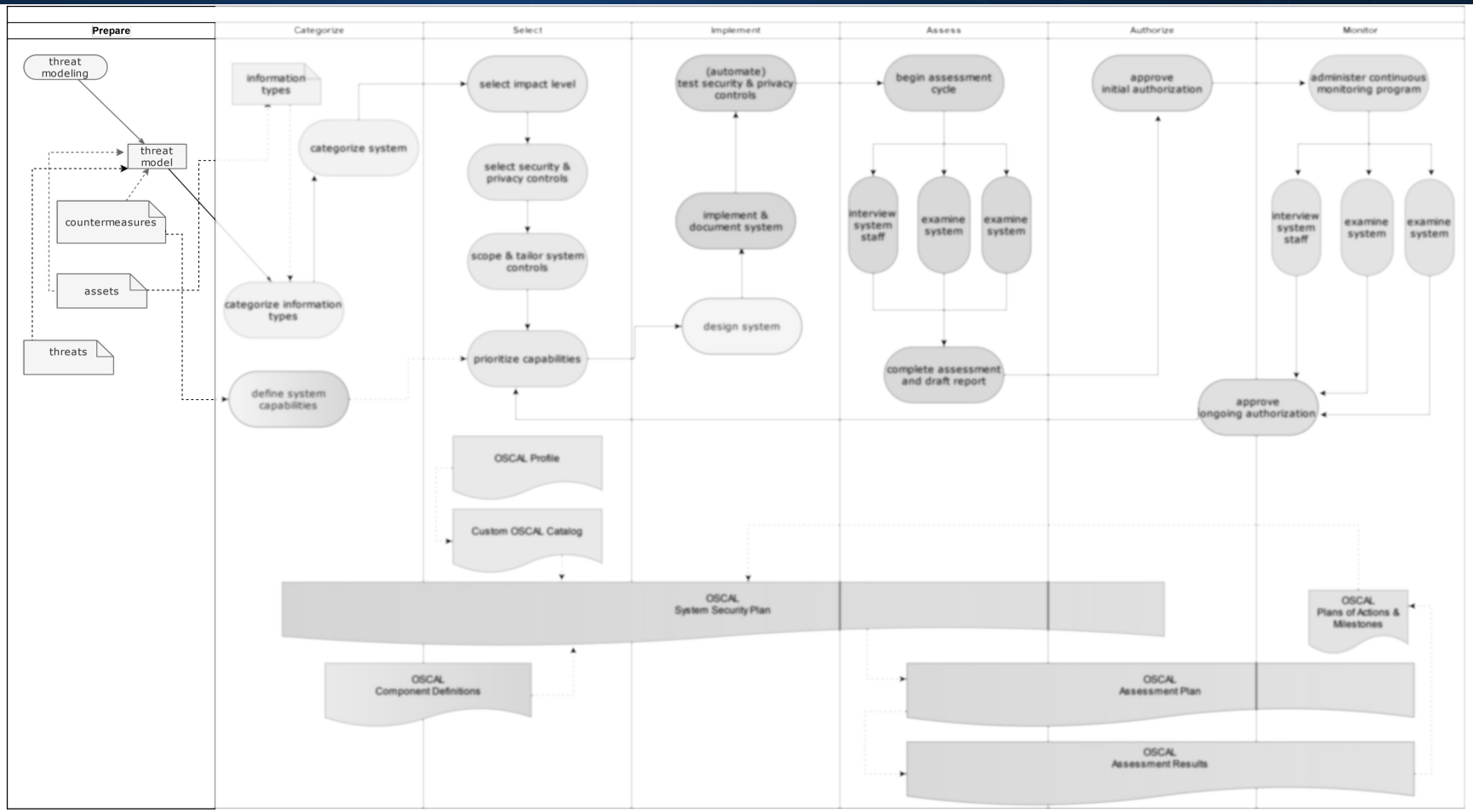
- What are the attack steps we need to defend against?
- What are capabilities and sub-capabilities to protect against attack steps?
- What are the security controls do we select and how do we automate pre-assessment?

Source: Automation Support for Security Control Assessments (NIST IR 8011)

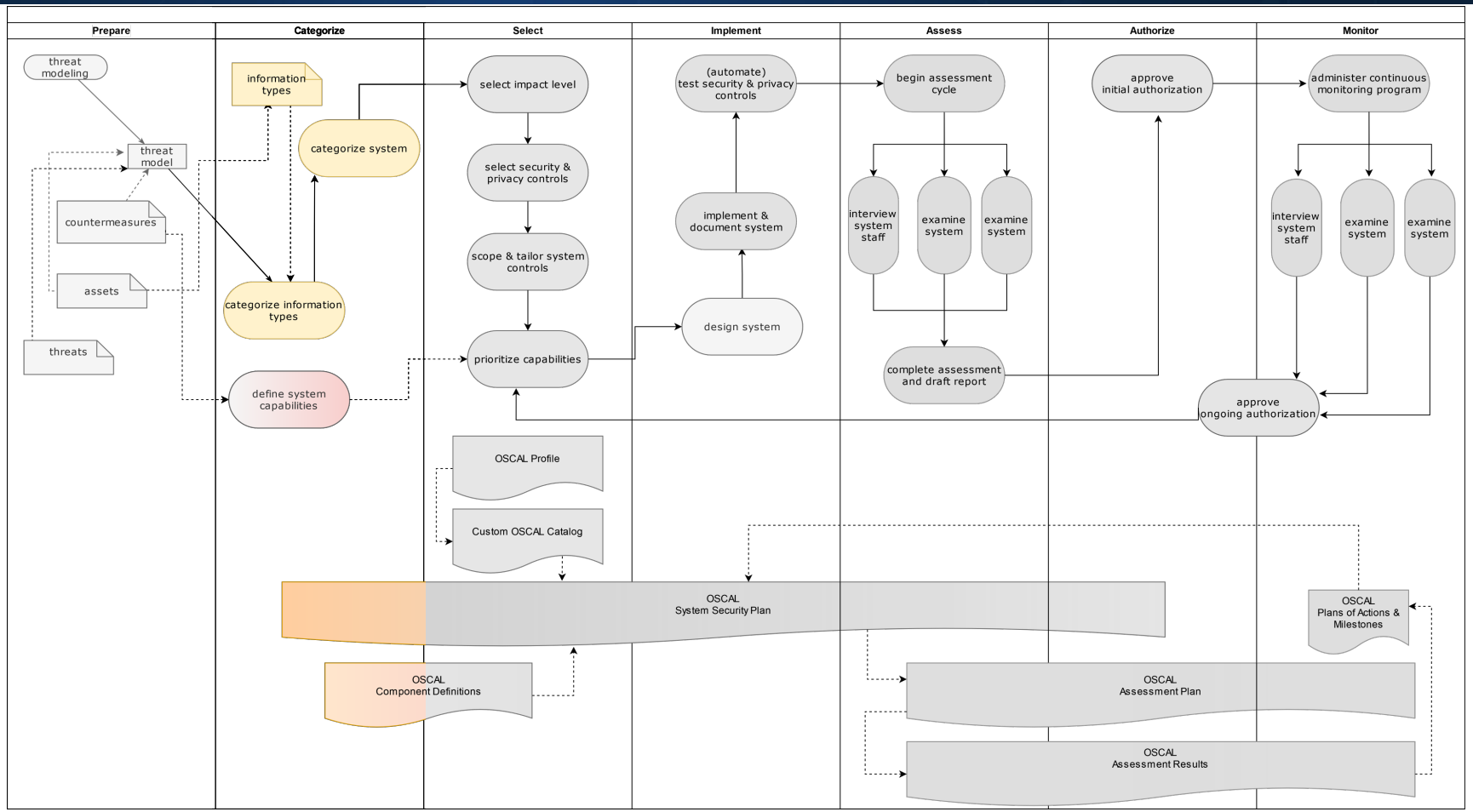
The Best SDLC: DevSecOps with OSCAL



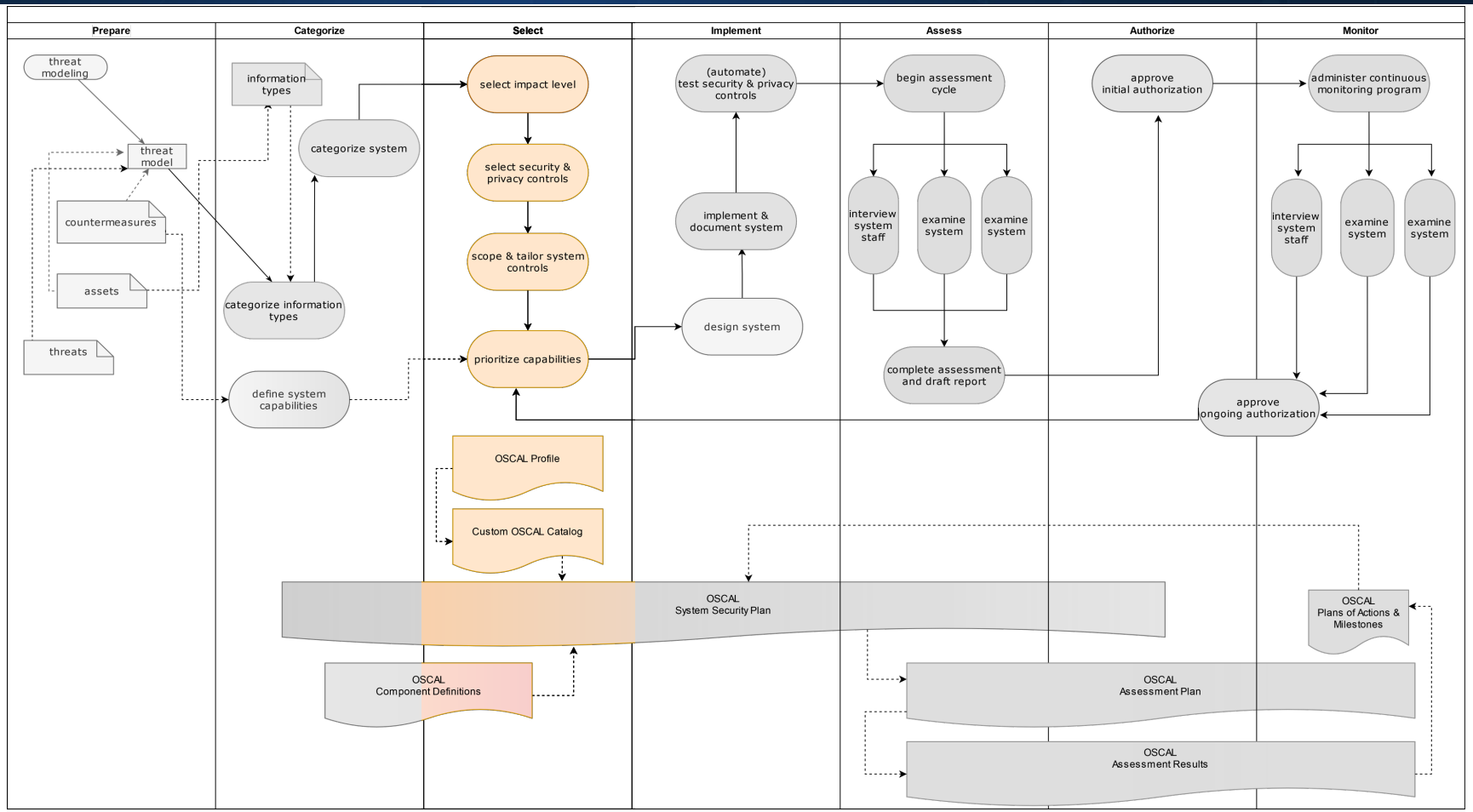
Prepare


Prepare
Categorize
Select
Implement
Assess
Authorize
Monitor
threat modeling
threat model
countermeasures
assets
threats
information types
categorize system
categorize information types
define system capabilities
select impact level
select security & privacy controls
scope & tailor system controls
prioritize capabilities
(automate) test security & privacy controls
implement & document system
design system
begin assessment cycle
interview system staff
examine system
examine system
complete assessment and draft report
approve initial authorization
administer continuous monitoring program
interview system staff
examine system
examine system
approve ongoing authorization
OSCAL Profile
Custom OSCAL Catalog
OSCAL System Security Plan
OSCAL Component Definitions
OSCAL Assessment Plan
OSCAL Assessment Results
OSCAL Plans of Actions & Milestones

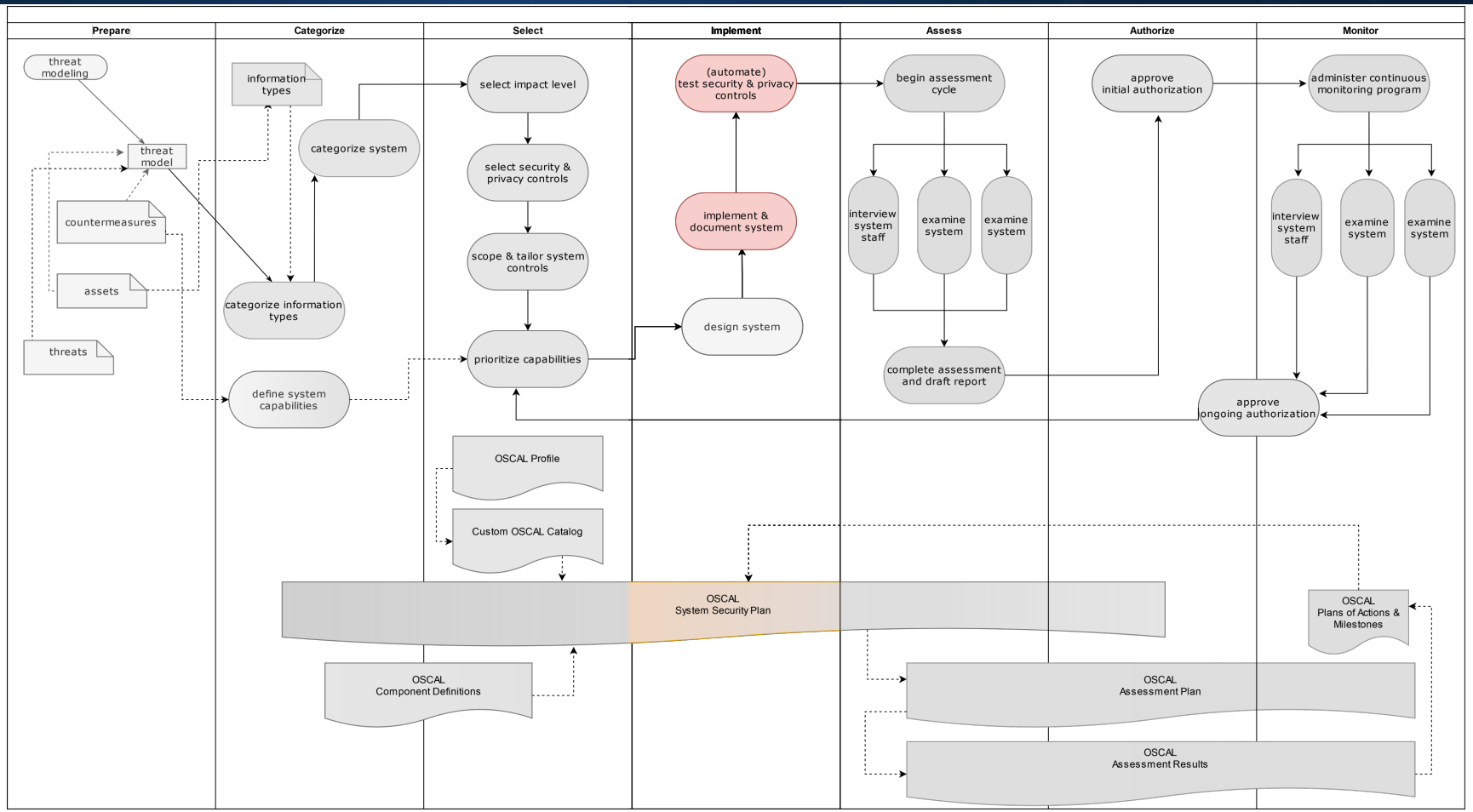
Categorize


Prepare
Categorize
Select
Implement
Assess
Authorize
Monitor
threat modeling
threat model
countermeasures
assets
threats
information types
categorize system
categorize information types
define system capabilities
select impact level
select security & privacy controls
scope & tailor system controls
prioritize capabilities
(automate) test security & privacy controls
implement & document system
design system
begin assessment cycle
interview system staff
examine system
examine system
complete assessment and draft report
approve initial authorization
administer continuous monitoring program
interview system staff
examine system
examine system
approve ongoing authorization
OSCAL Profile
Custom OSCAL Catalog
OSCAL System Security Plan
OSCAL Component Definitions
OSCAL Assessment Plan
OSCAL Assessment Results
OSCAL Plans of Actions & Milestones

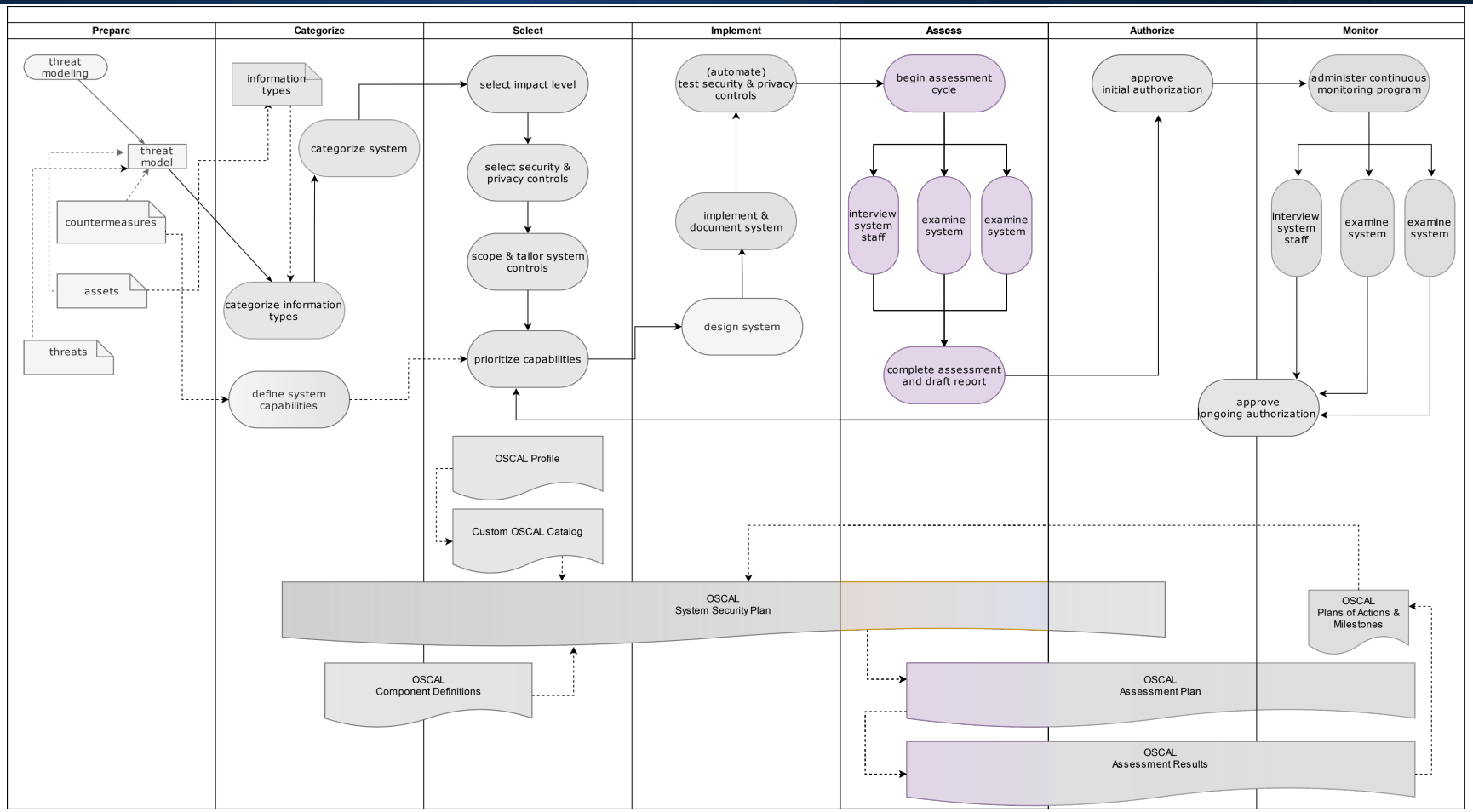
Select


Prepare
Categorize
Select
Implement
Assess
Authorize
Monitor
threat modeling
threat model
countermeasures
assets
threats
information types
categorize system
categorize information types
define system capabilities
select impact level
select security & privacy controls
scope & tailor system controls
prioritize capabilities
(automate) test security & privacy controls
implement & document system
design system
begin assessment cycle
interview system staff
examine system
examine system
complete assessment and draft report
approve initial authorization
administer continuous monitoring program
interview system staff
examine system
examine system
approve ongoing authorization
OSCAL Profile
Custom OSCAL Catalog
OSCAL System Security Plan
OSCAL Component Definitions
OSCAL Assessment Plan
OSCAL Assessment Results
OSCAL Plans of Actions & Milestones

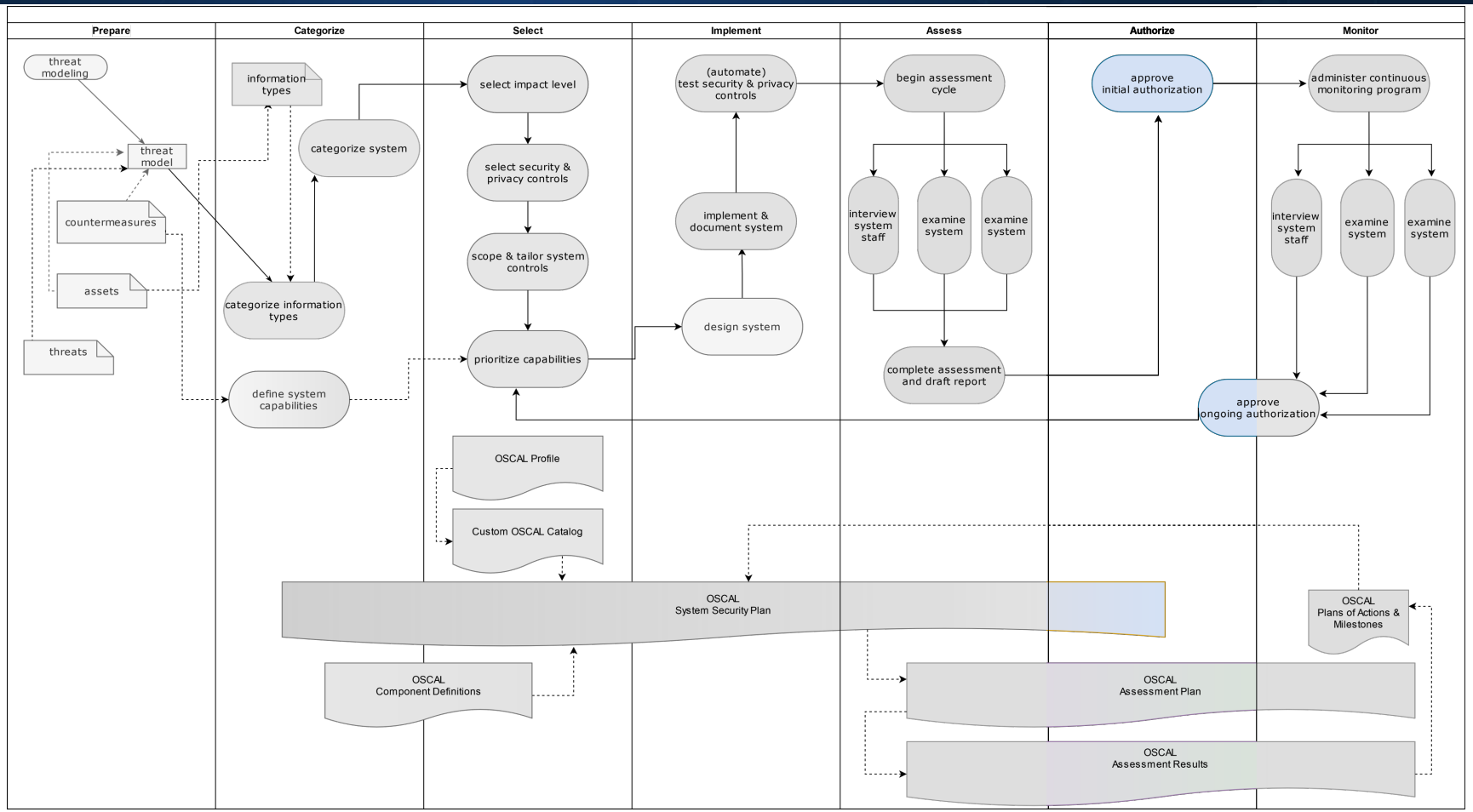
Implement


Prepare
Categorize
Select
Implement
Assess
Authorize
Monitor
threat modeling
threat model
countermeasures
assets
threats
information types
categorize system
categorize information types
define system capabilities
select impact level
select security & privacy controls
scope & tailor system controls
prioritize capabilities
(automate) test security & privacy controls
implement & document system
design system
begin assessment cycle
interview system staff
examine system
examine system
complete assessment and draft report
approve initial authorization
administer continuous monitoring program
interview system staff
examine system
examine system
approve ongoing authorization
OSCAL Profile
Custom OSCAL Catalog
OSCAL System Security Plan
OSCAL Component Definitions
OSCAL Assessment Plan
OSCAL Assessment Results
OSCAL Plans of Actions & Milestones

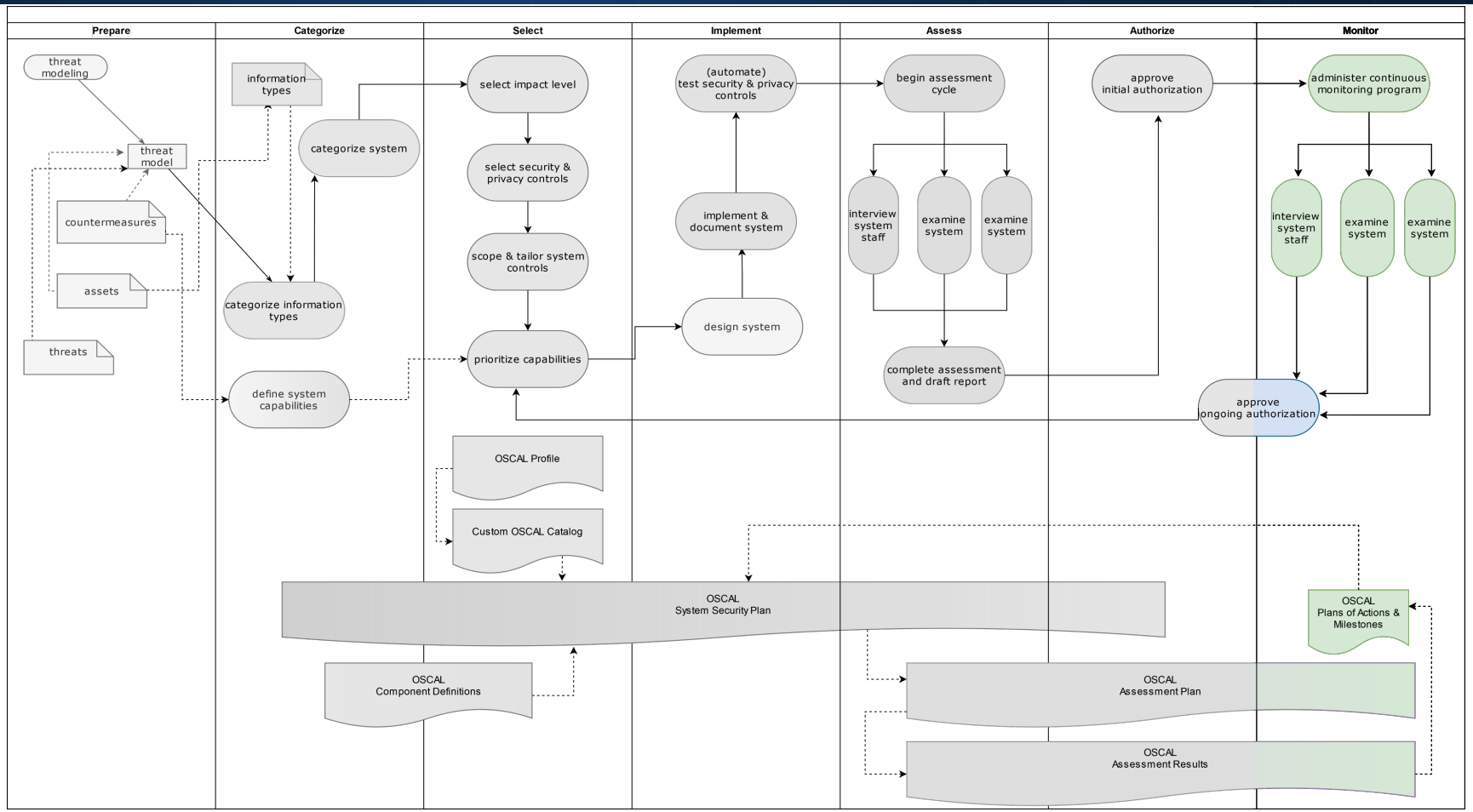
Assess


Prepare
Categorize
Select
Implement
Assess
Authorize
Monitor
threat modeling
threat model
countermeasures
assets
threats
information types
categorize system
categorize information types
define system capabilities
select impact level
select security & privacy controls
scope & tailor system controls
prioritize capabilities
(automate) test security & privacy controls
implement & document system
design system
begin assessment cycle
interview system staff
examine system
examine system
complete assessment and draft report
approve initial authorization
administer continuous monitoring program
interview system staff
examine system
examine system
approve ongoing authorization
OSCAL Profile
Custom OSCAL Catalog
OSCAL System Security Plan
OSCAL Component Definitions
OSCAL Assessment Plan
OSCAL Assessment Results
OSCAL Plans of Actions & Milestones

Authorize


Prepare
Categorize
Select
Implement
Assess
Authorize
Monitor
threat modeling
threat model
countermeasures
assets
threats
information types
categorize system
categorize information types
define system capabilities
select impact level
select security & privacy controls
scope & tailor system controls
prioritize capabilities
(automate) test security & privacy controls
implement & document system
design system
begin assessment cycle
interview system staff
examine system
examine system
complete assessment and draft report
approve initial authorization
administer continuous monitoring program
interview system staff
examine system
examine system
approve ongoing authorization
OSCAL Profile
Custom OSCAL Catalog
OSCAL System Security Plan
OSCAL Component Definitions
OSCAL Assessment Plan
OSCAL Assessment Results
OSCAL Plans of Actions & Milestones

Monitor


Prepare
Categorize
Select
Implement
Assess
Authorize
Monitor
threat modeling
threat model
countermeasures
assets
threats
information types
categorize system
categorize information types
define system capabilities
select impact level
select security & privacy controls
scope & tailor system controls
prioritize capabilities
(automate) test security & privacy controls
implement & document system
design system
begin assessment cycle
interview system staff
examine system
examine system
complete assessment and draft report
approve initial authorization
administer continuous monitoring program
interview system staff
examine system
examine system
approve ongoing authorization
OSCAL Profile
Custom OSCAL Catalog
OSCAL System Security Plan
OSCAL Component Definitions
OSCAL Assessment Plan
OSCAL Assessment Results
OSCAL Plans of Actions & Milestones

Contact Us

blossom@nist.gov

National Institute of Standards and Technology
U.S. Department of Commerce

ITL/CSD/OSCAL Team

3rd OSCAL Workshop