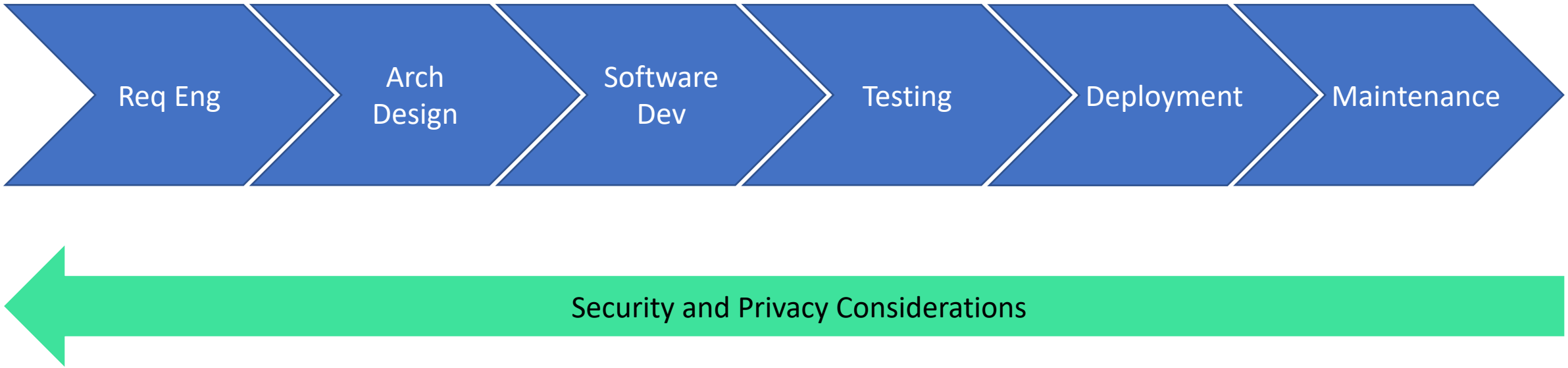
Privacy Shift Left: A Machine Assisted Threat Modeling Approach

Kristen Tan and Vaibhav Garg

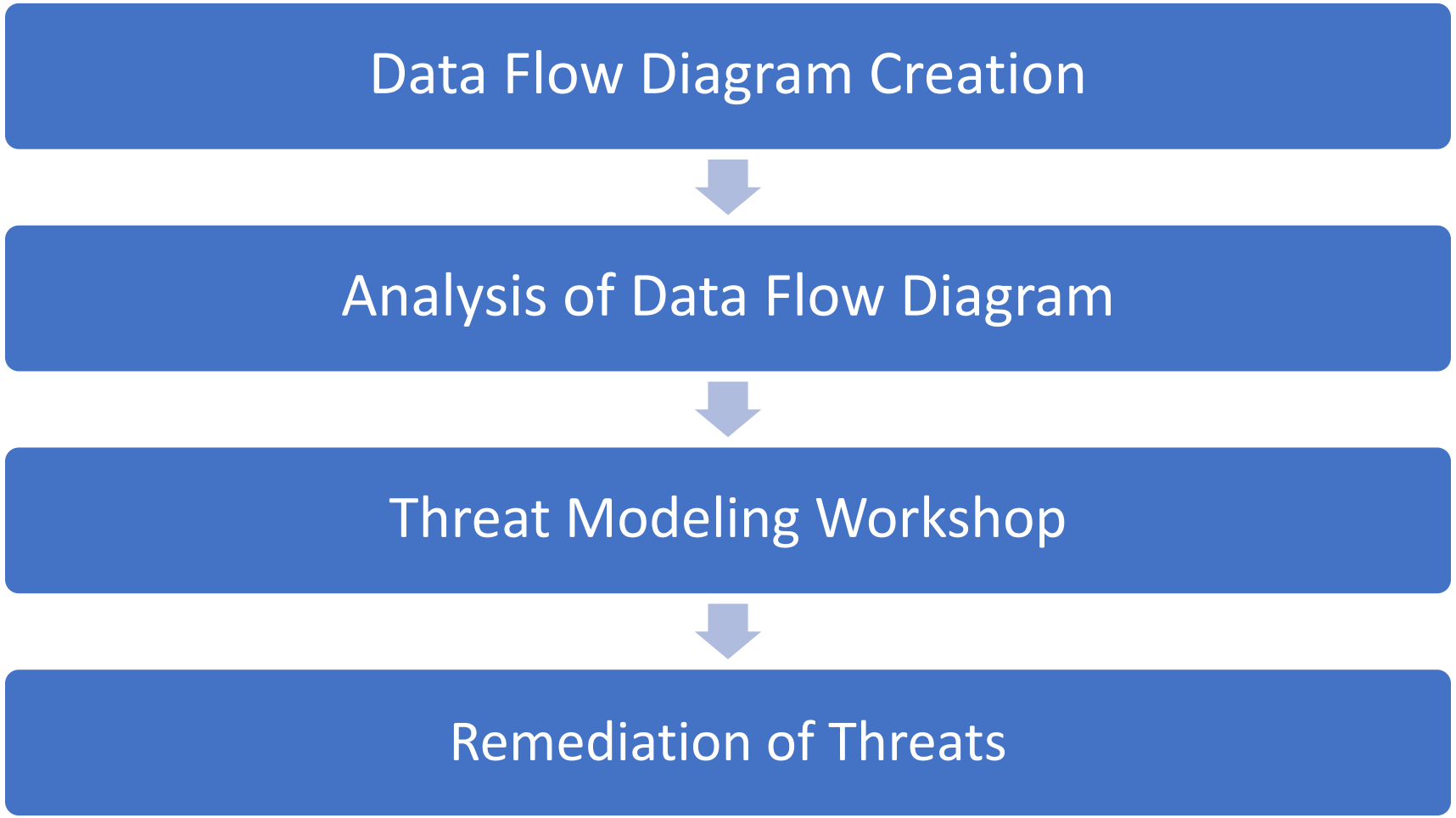
Comcast Cable

SHIFTING SECURITY AND PRIVACY LEFT



COMCAST

HOW THREAT MODELING WORKS



COMCAST

THREAT MODELING FRAMEWORKS

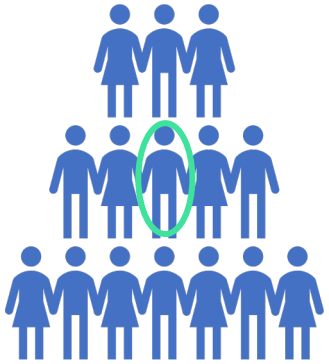
STRIDE

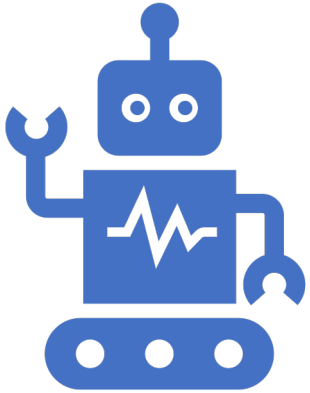
- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

LINDDUN

- Linkability
- Identifiability
- Non-repudiation
- Detectability
- Disclosure of Information
- Unawareness
- Non-compliance

THREAT MODELING CHALLENGES AND SOLUTIONS





Challenges

Solution

COMCAST

TOOL SELECTION

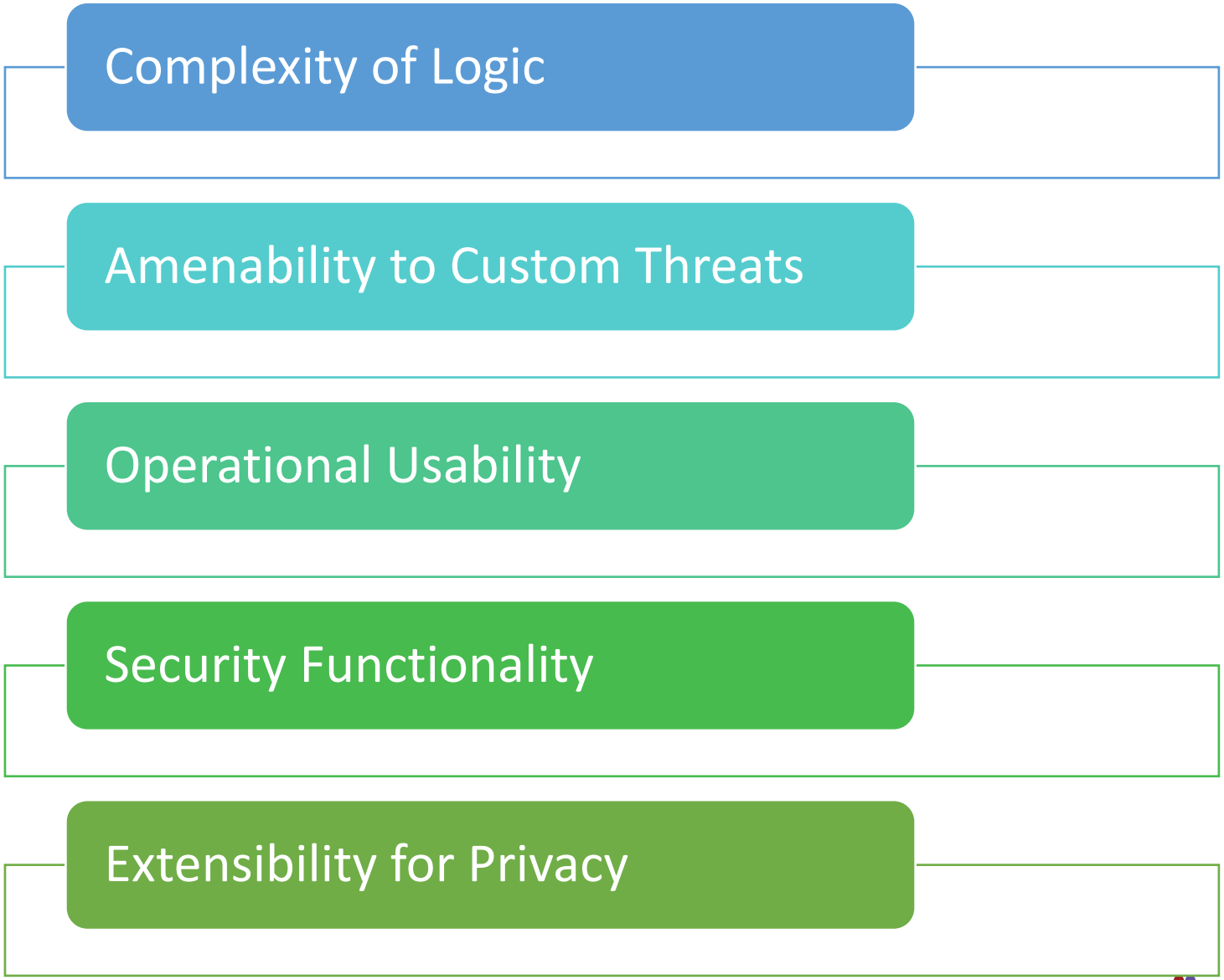



Inclusion Criteria


Search Details

COMCAST

DEFINITION/ APPLICATION OF EVALUATION CRITERIA



COMCAST

	Current Solution (Traditional TM)	CAIRIS	Threats Manager Studio	Threatspec	PyTM	Threat Dragon	Threagile
Complexity of Logic	0	0	0	-1	1	-1	1
Amenability to Custom Threats	0	-1	1	1	1	-1	1
Operational Usability	0	-1	-1	1	0	1	0
Security Functionality	0	-1	-1	-1	-1	1	1
Extensibility for Privacy	0	-1	0	0	1	1	1
	0	**-4**	**-1**	**0**	**2**	**1**	**4**

COMPARATIVE ANALYSIS OF TOOLS

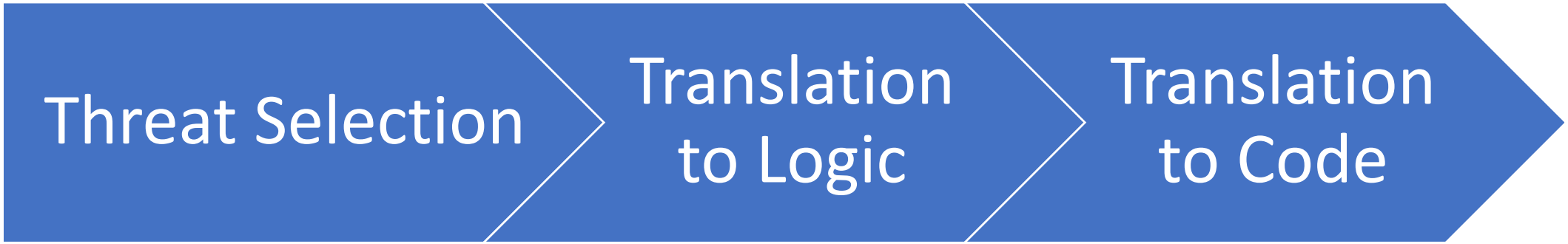
CUSTOM PRIVACY THREAT LIBRARY SOURCES

LINDDUN GO

OWASP TOP 10

LEGAL & REGULATORY

INTEGRATING A CUSTOM PRIVACY THREAT INTO THREAGILE



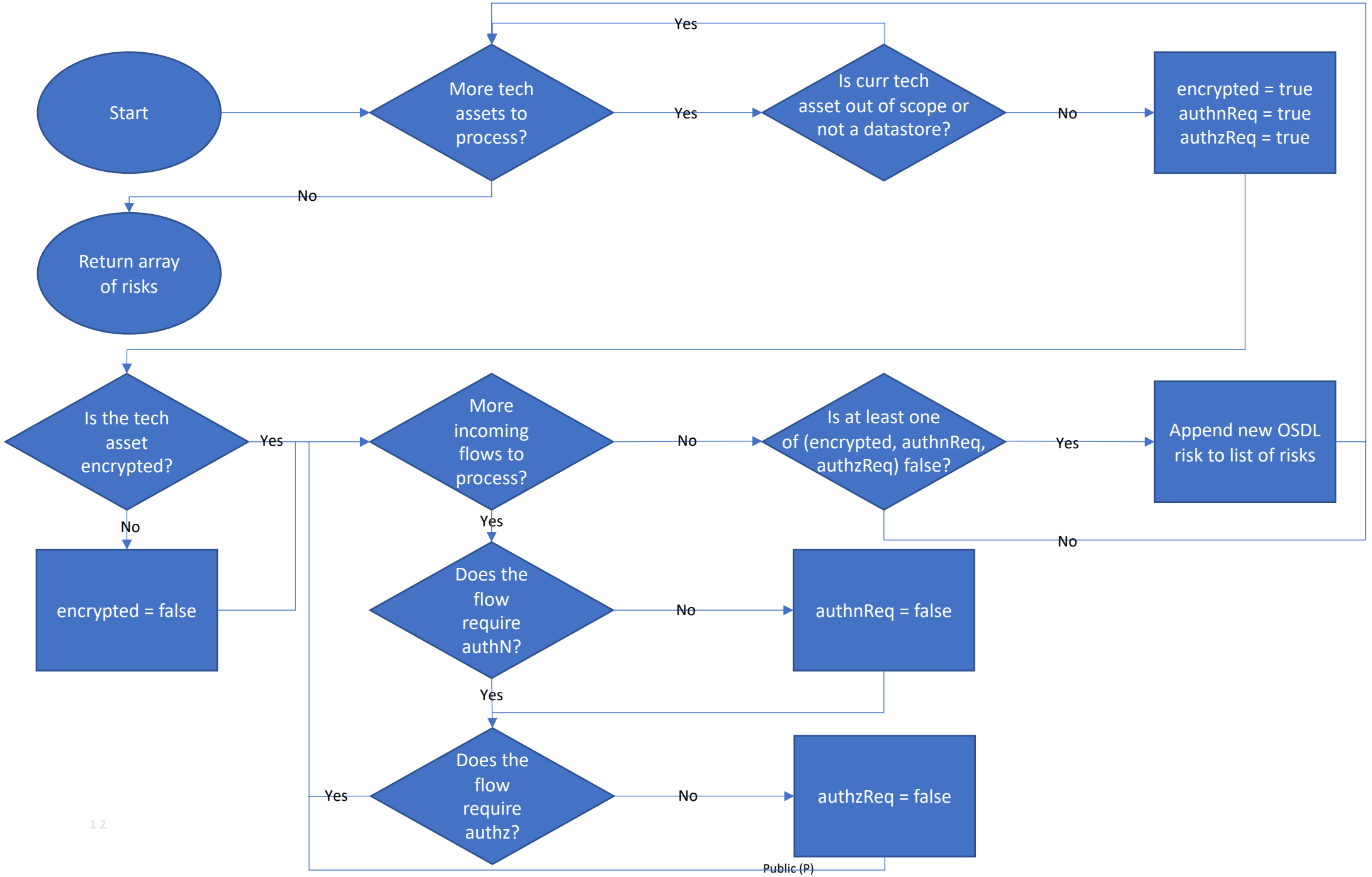
COMCAST

THREAT SELECTION

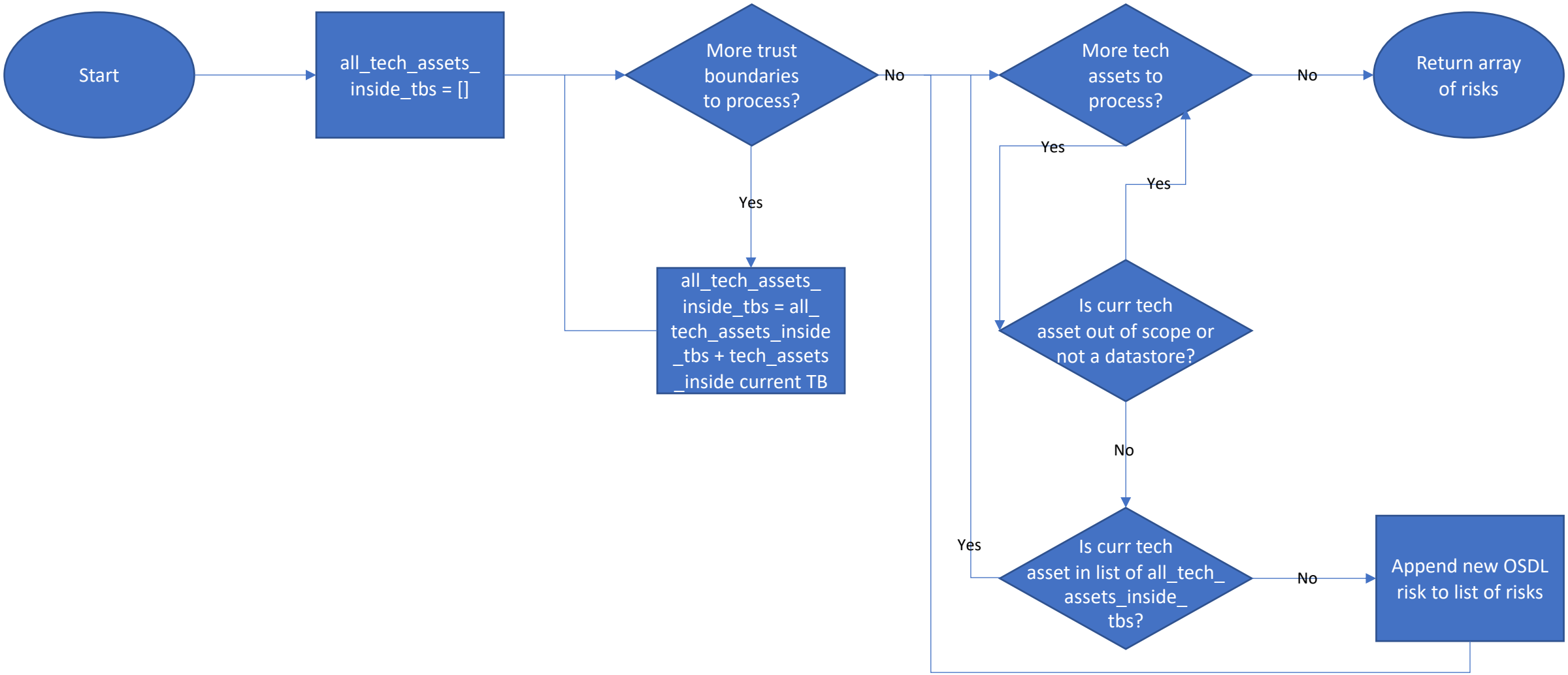
Operator-sided Data Leakage

- Source
  - OWASP Top 10 Privacy Threats
- Definition
  - “Failure to prevent the leakage of any information containing or related to user data, or the data itself, to any unauthorized party resulting in loss of data confidentiality. Introduced either due to intentional malicious breach or unintentional mistake e.g. caused by insufficient access management controls, insecure storage, duplication of data or a lack of awareness.”

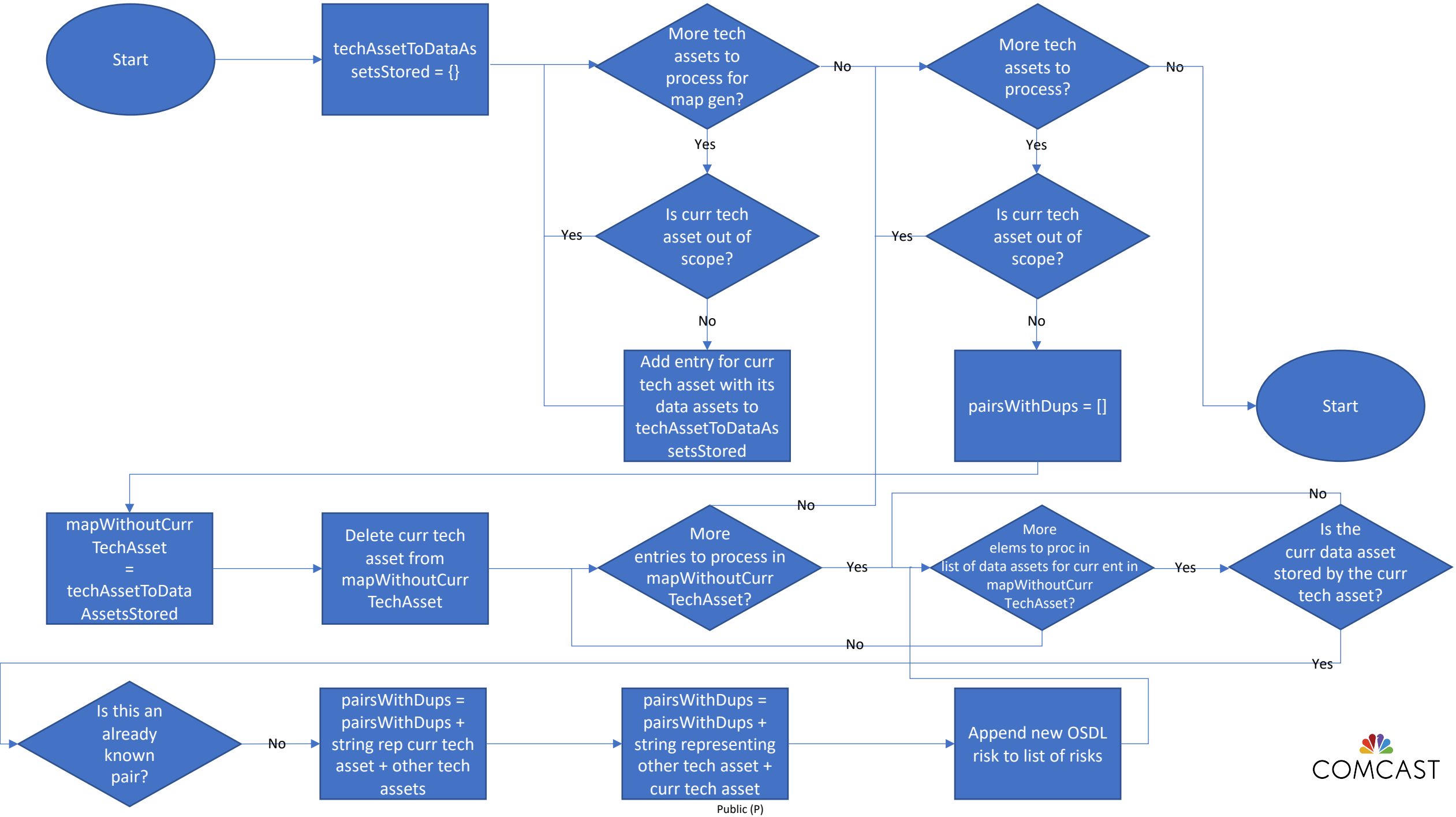
COMCAST



COMCAST



COMCAST


Start
techAssetToDataAssetsStored = {}
More tech assets to process for map gen?
No
Yes
Is curr tech asset out of scope?
Yes
No
Add entry for curr tech asset with its data assets to techAssetToDataAssetsStored
More tech assets to process?
No
Yes
Is curr tech asset out of scope?
Yes
No
pairsWithDups = []
Start
mapWithoutCurrTechAsset = techAssetToDataAssetsStored
Delete curr tech asset from mapWithoutCurrTechAsset
More entries to process in mapWithoutCurrTechAsset?
No
Yes
More elems to proc in list of data assets for curr ent in mapWithoutCurrTechAsset?
Yes
No
Is the curr data asset stored by the curr tech asset?
No
Yes
Is this an already known pair?
No
pairsWithDups = pairsWithDups + string rep curr tech asset + other tech assets
pairsWithDups = pairsWithDups + string representing other tech asset + curr tech asset
Append new OSDL risk to list of risks

TRANSLATION TO CODE – OSDL INSECURE STORAGE

```go
func (r operatorSidedDataLeakageInsecureStorageRiskRule) GenerateRisks() []model.Risk {
    risks := make([]model.Risk, 0)

    // ---------- OWASP Check - Insecure Storage ----------

    // Get a list of ALL the Technical Assets that DO sit behind a trust boundary
    all_tech_assets_inside_tbs := make([]string, 0)
    for _, trustBoundary := range model.ParsedModelRoot.TrustBoundaries {
        all_tech_assets_inside_tbs = append(all_tech_assets_inside_tbs, trustBoundary.TechnicalAssetsInside...)
    }

    for _, techAsset := range model.ParsedModelRoot.TechnicalAssets {
        if techAsset.OutOfScope || techAsset.Type != model.Datastore { // ignore the technical asset if it has been marked as out of scope
            continue
        }

        // If a Datastore is NOT behind a Trust Boundary, raise a risk
        if !(stringInSlice(techAsset.Id, all_tech_assets_inside_tbs)) {
            risks = append(risks, createRisk(techAsset))
        }
    }

    return risks
}
```


COMCAST

THANK YOU!

https://corporate.comcast.com/ccs-research

COMCAST