Security in knowledge

Privacy Compliance and Oversight in the National Security Context

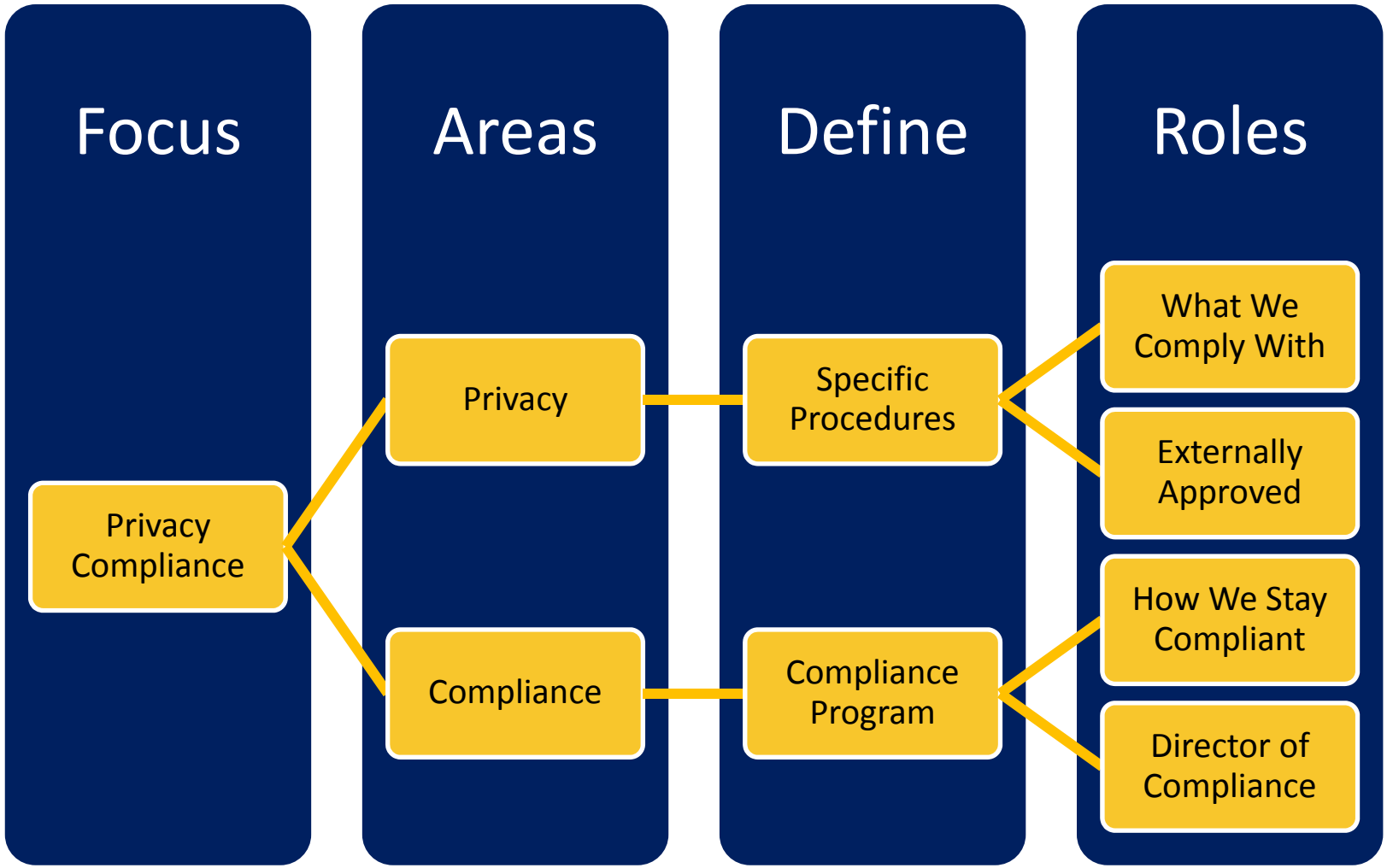
John DeLong

Director of Compliance
National Security Agency

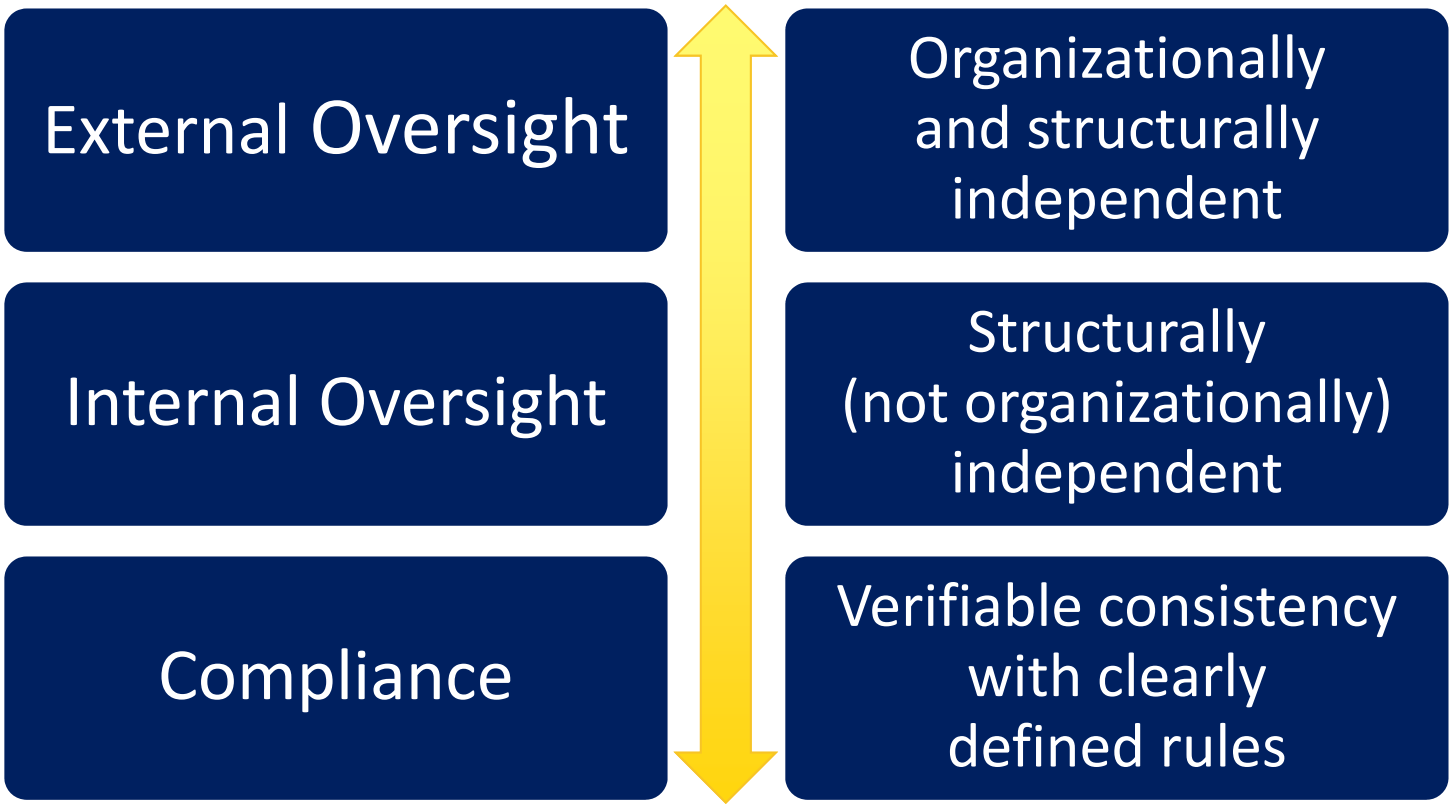
RSA CONFERENCE 2013

Session ID: GRC-R33
Session Classification: Intermediate

High-Level Privacy Compliance Taxonomy



Compliance and Oversight



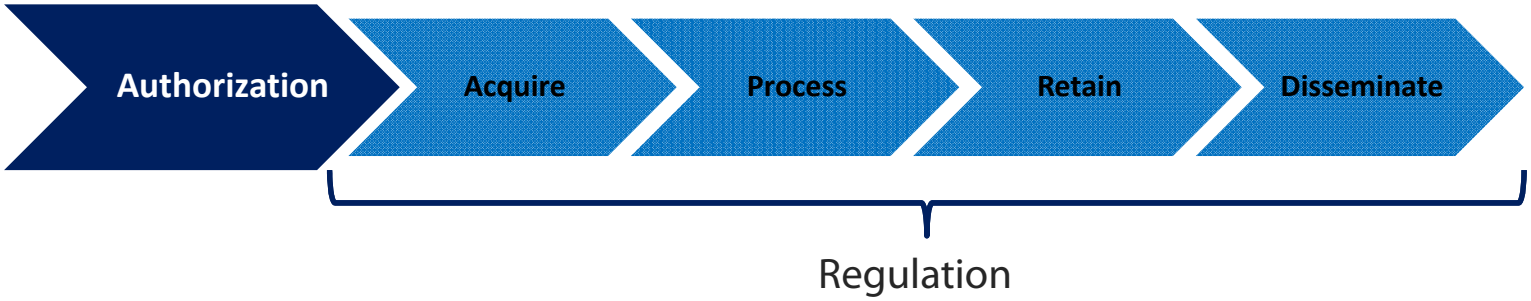
Minimization Procedures (High Level)

- Specific procedures
- Adopted externally
- Reasonably designed
- In light of the purpose or technique of the particular surveillance
- To minimize the acquisition and retention and prohibit the dissemination of U.S. persons information
- Consistent with need of U.S. to obtain, produce, and disseminate foreign intelligence

Authorization and Regulation

1. Describe
2. Authorize + Regulate
3. Operate
4. Evaluate

- Specific procedures
- Adopted externally
- Reasonably designed
- In light of the purpose or technique of the particular surveillance
- To minimize the acquisition and retention and prohibit the dissemination of U.S. persons information
- Consistent with need of U.S. to obtain, produce, and disseminate foreign intelligence



Four Phases of Compliance

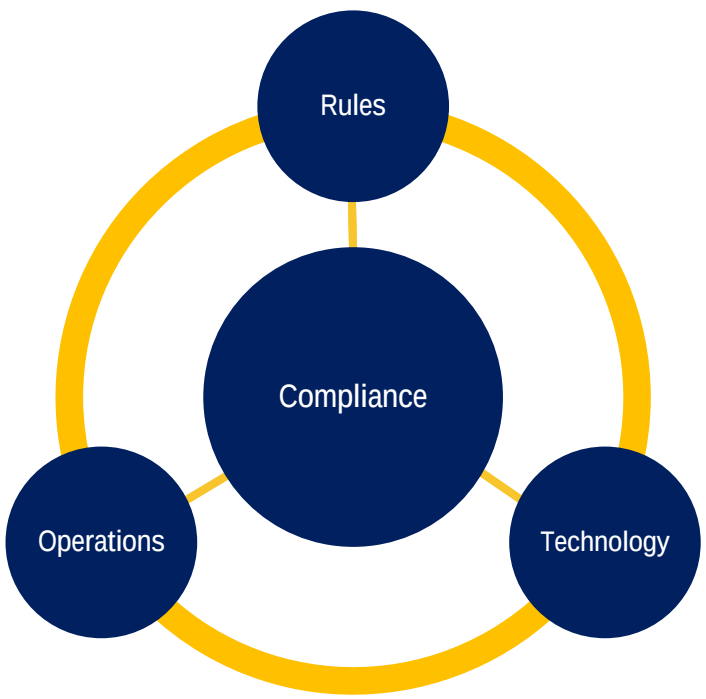
The Mission Compliance Program must take into account and tie together all four steps

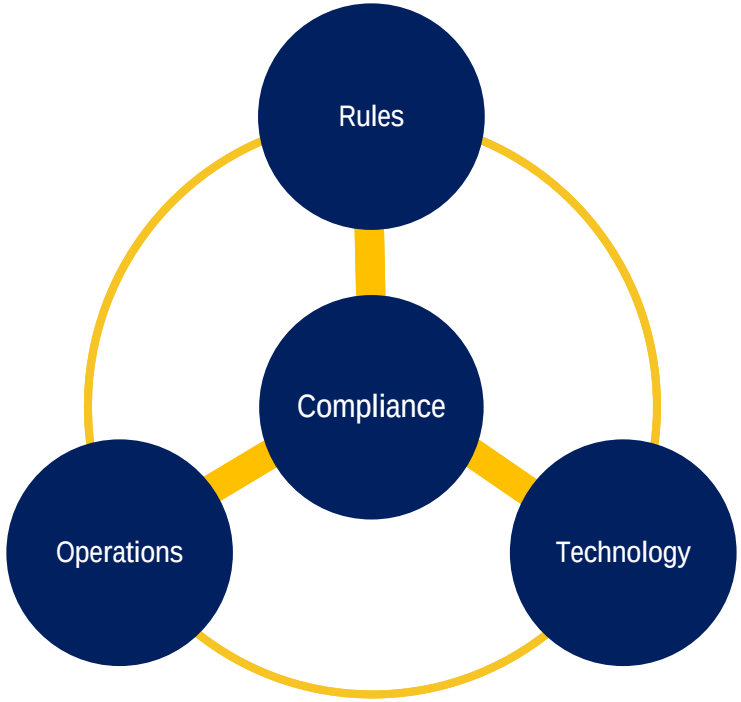
1. **Descriptions** (often complex) must be accurate and at the right level of granularity
2. **Specific authorizations and regulation** (specific procedures) must be the "root" of all activities conducted
3. **Operations and Technology** must be consistent with approved procedures, over time and through change
4. **Evaluations** done in light of each of the previous steps

Documentation Accuracy (Governance)

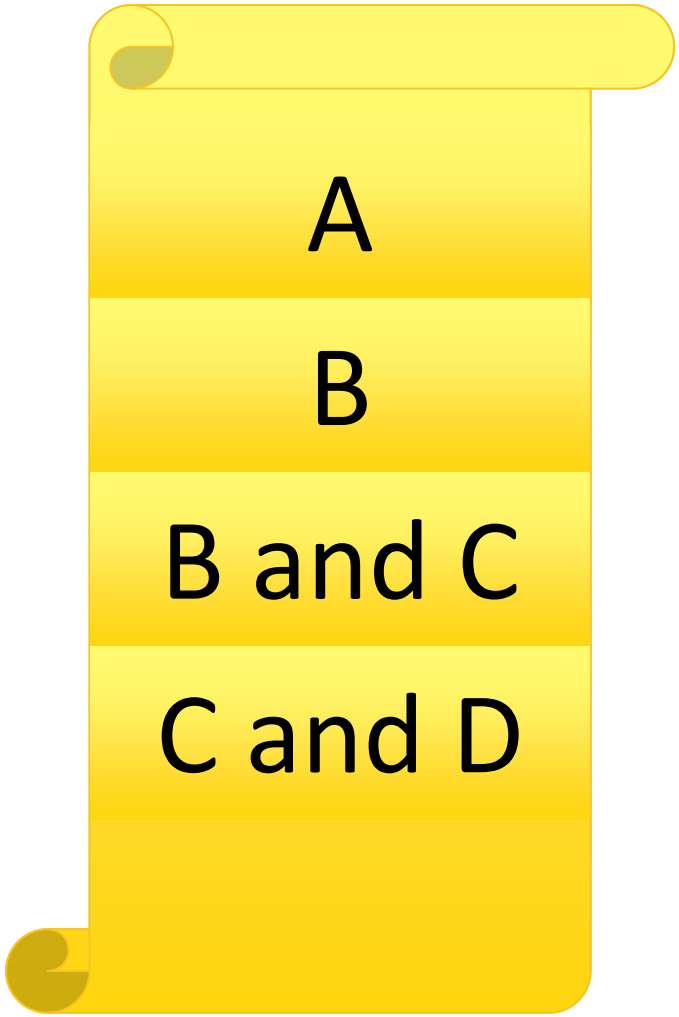
Security in knowledge

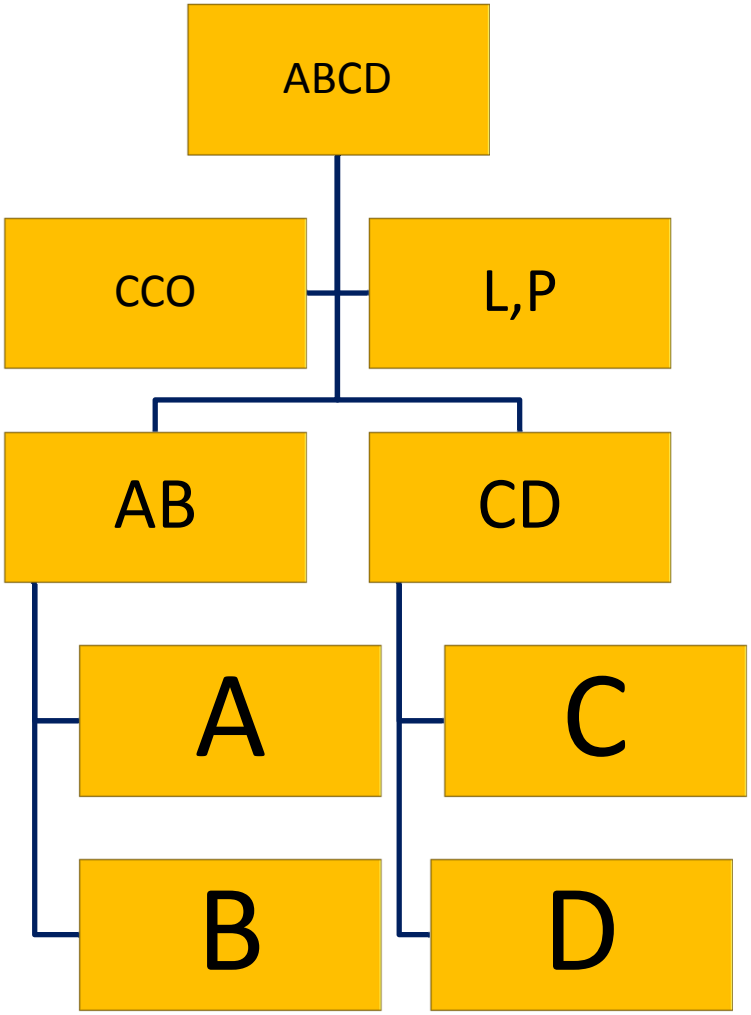
Two Models of Interaction



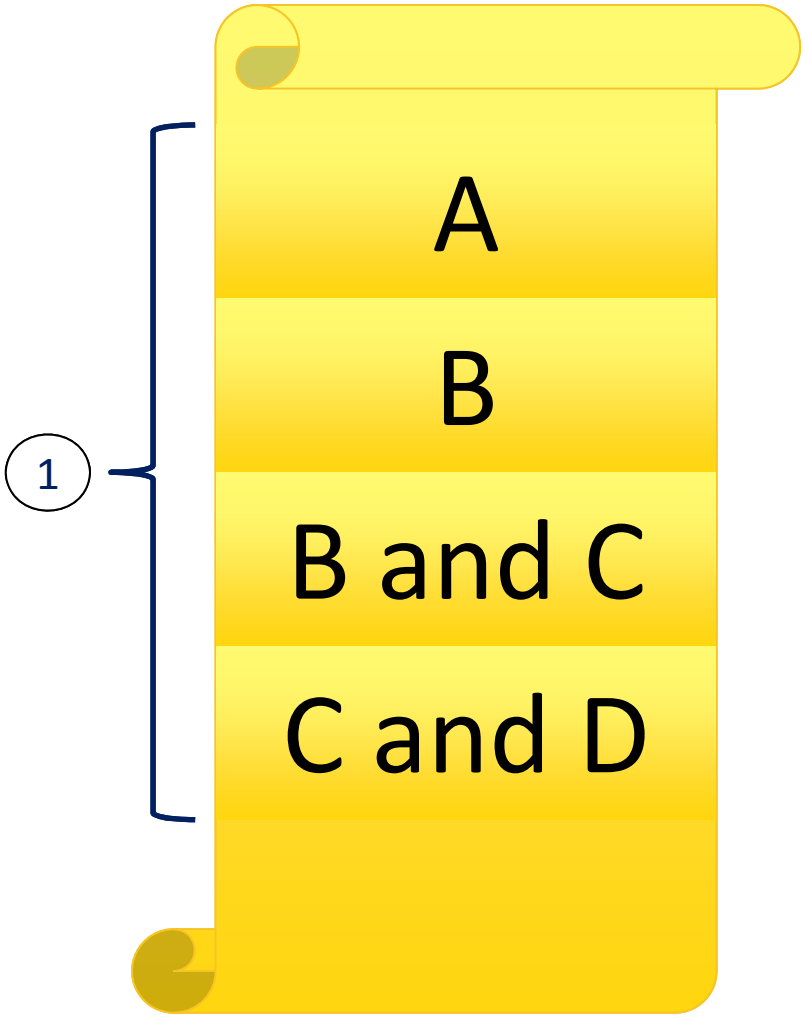


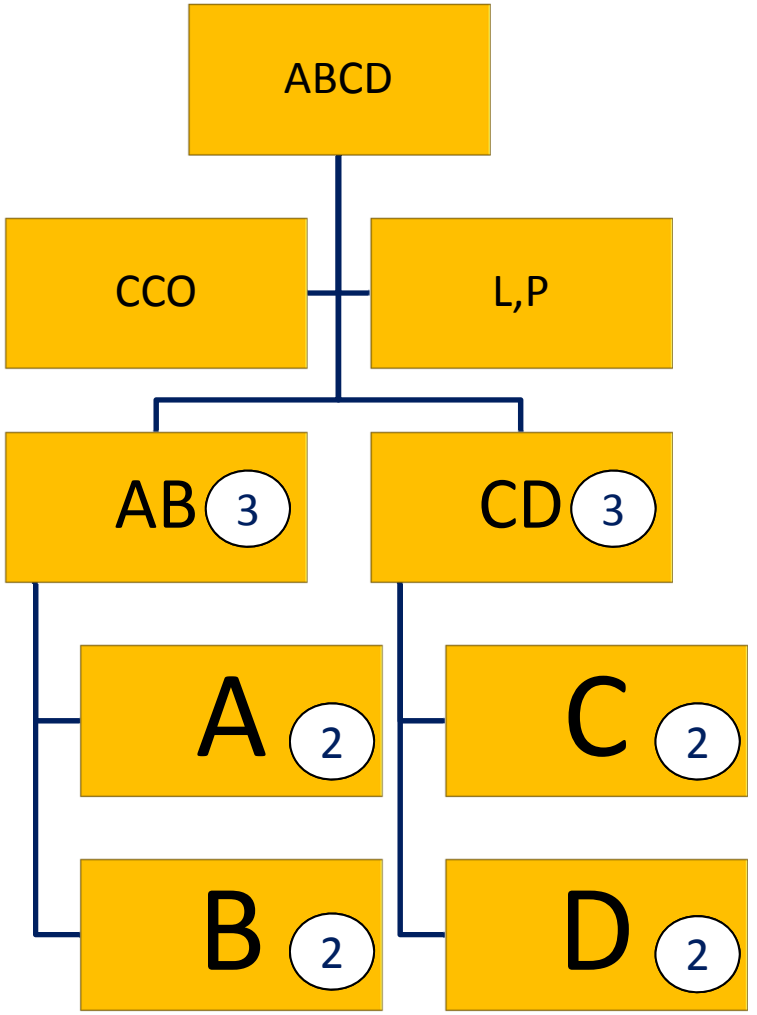
Documentation Accuracy (In Practice)





Documentation Accuracy (In Practice)

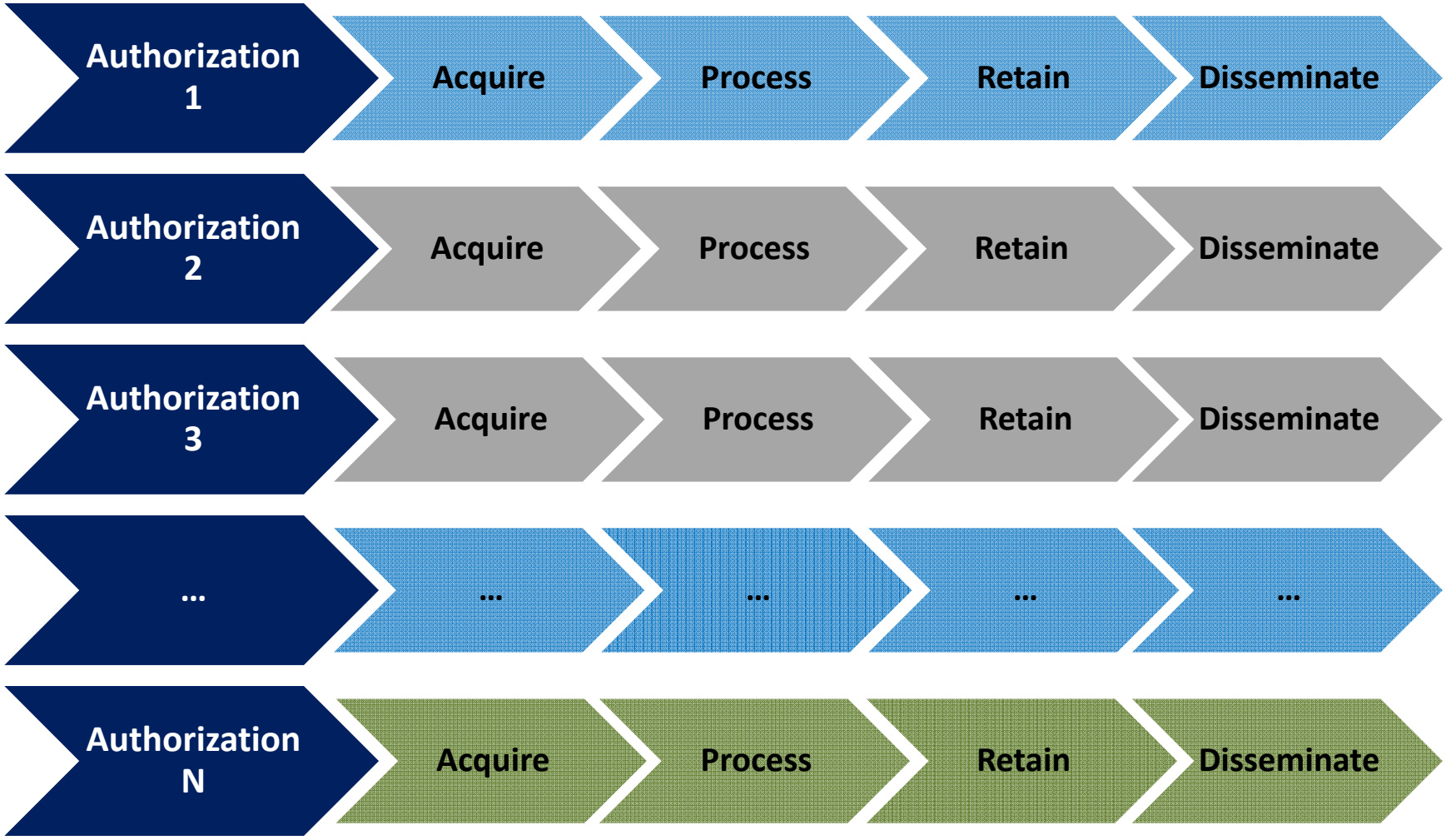




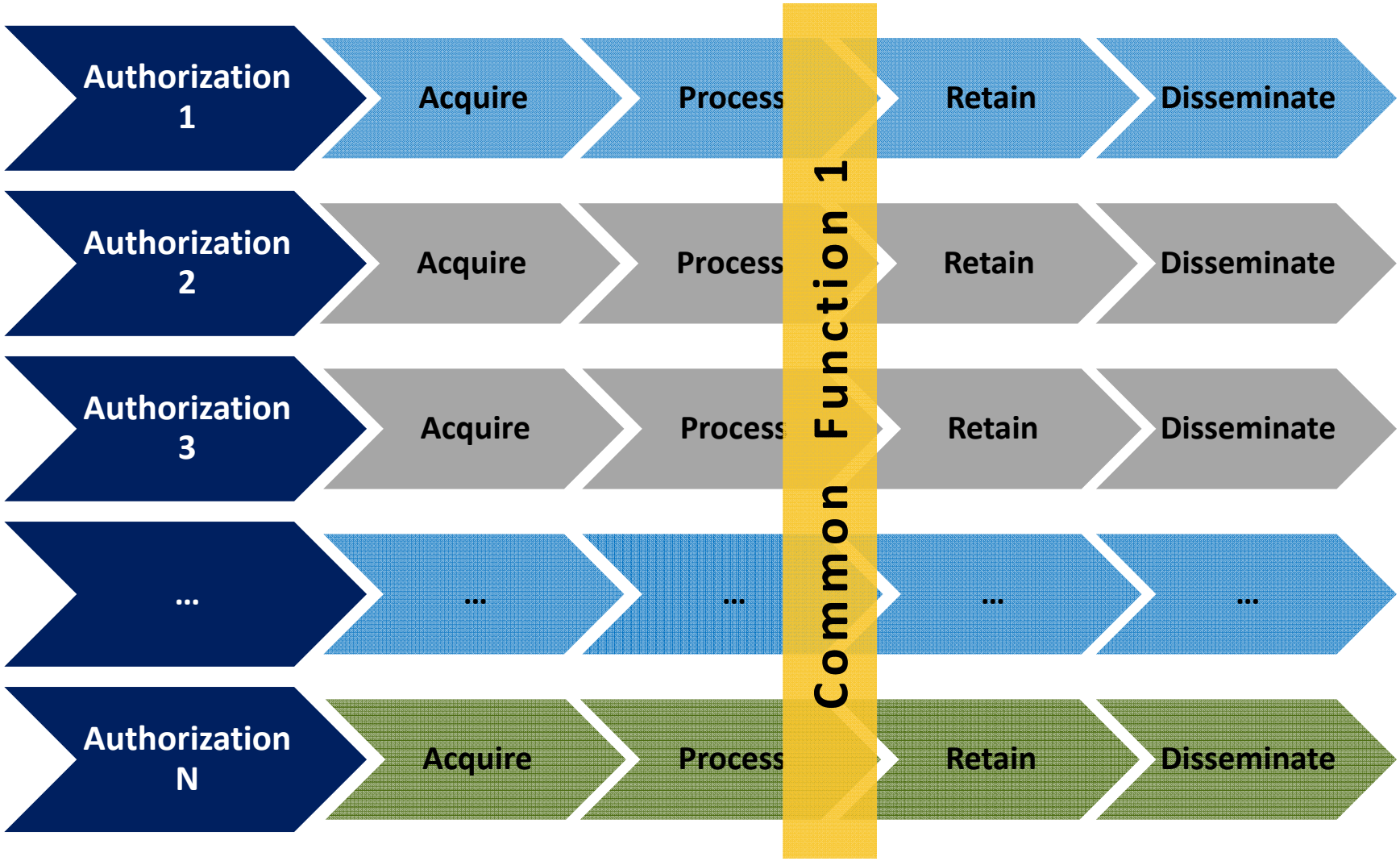
Functional Approach (Risk Management)

Security in knowledge

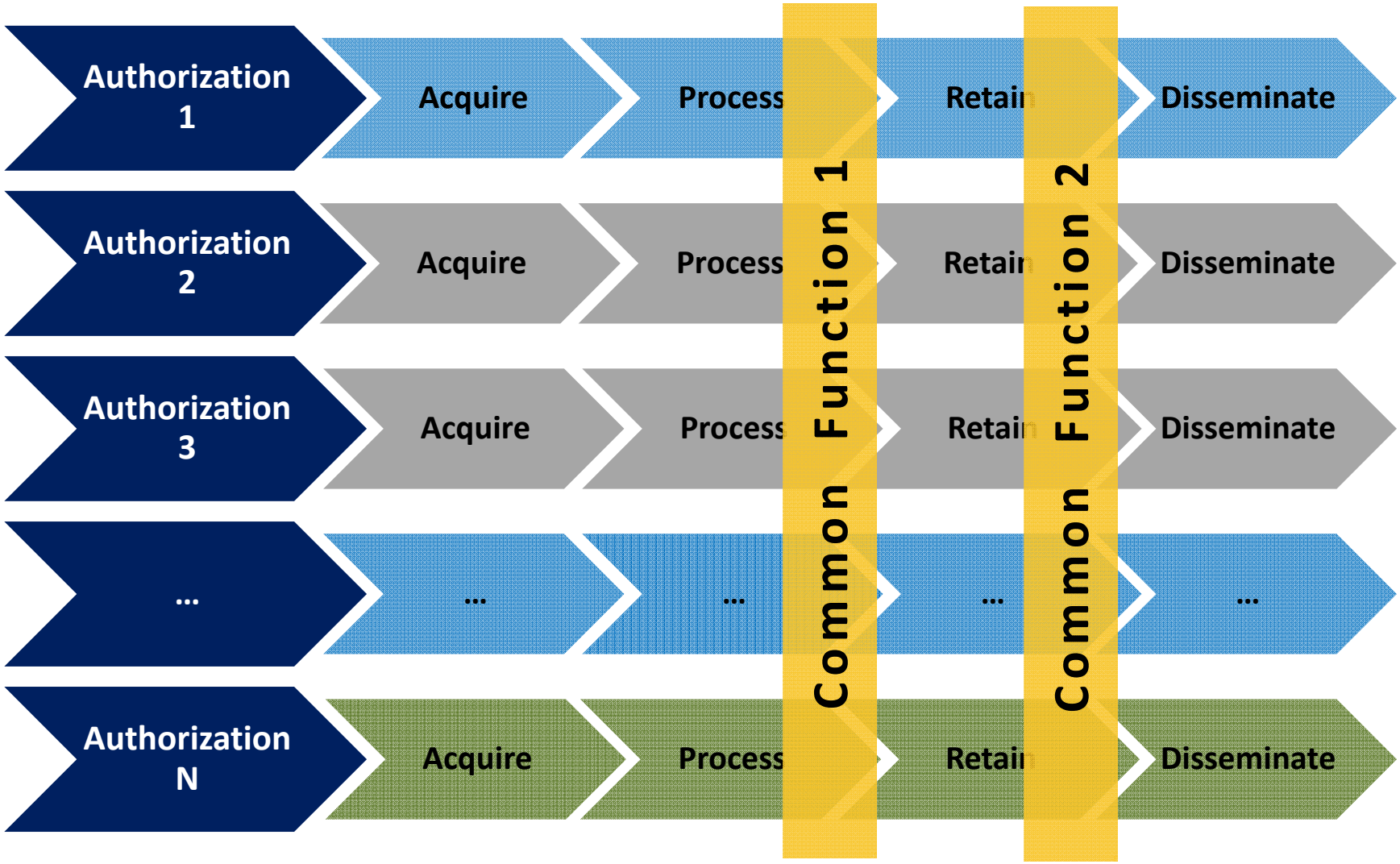
Authorizations and Procedures



Authorizations and Procedures



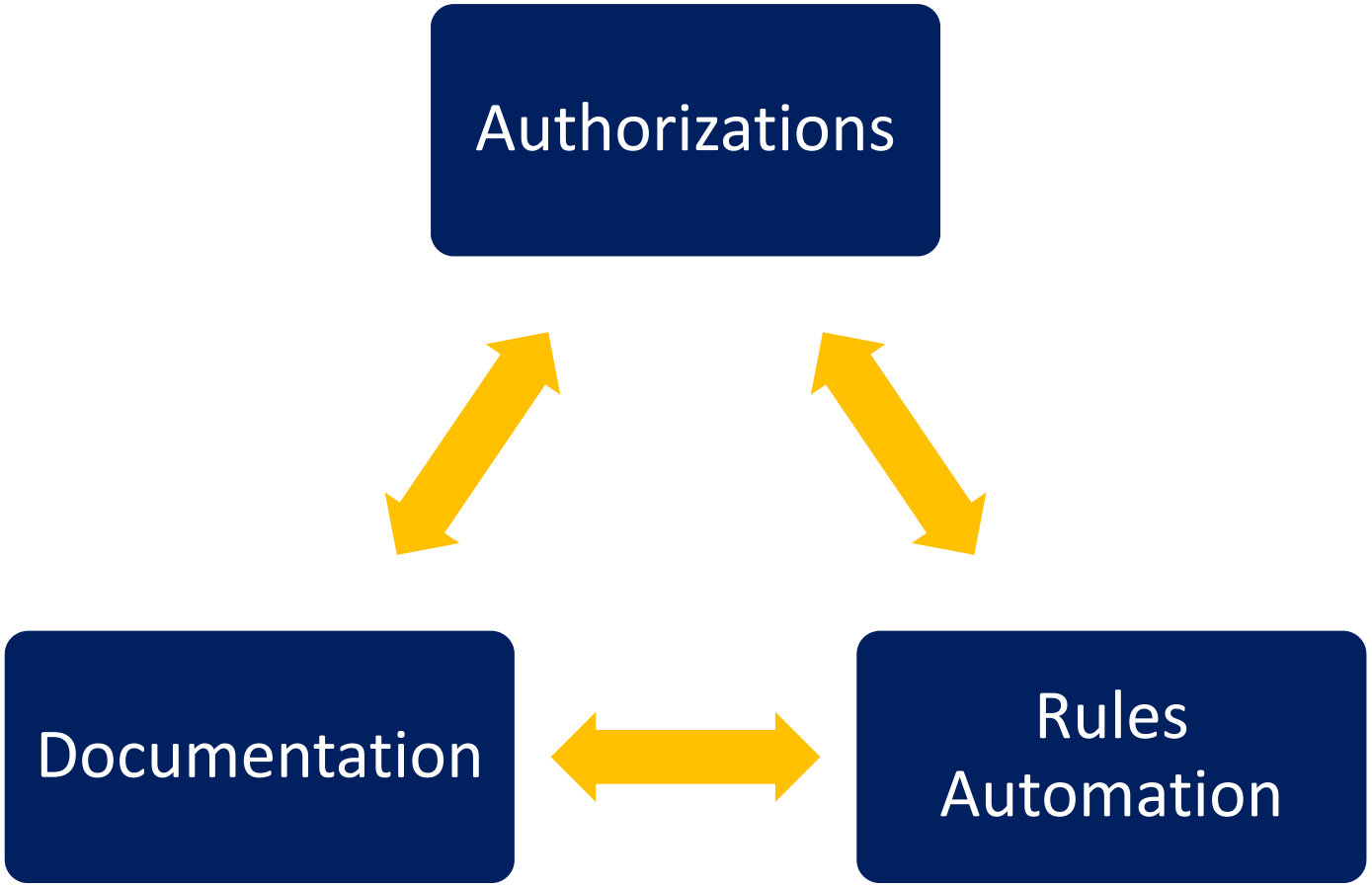
Authorizations and Procedures



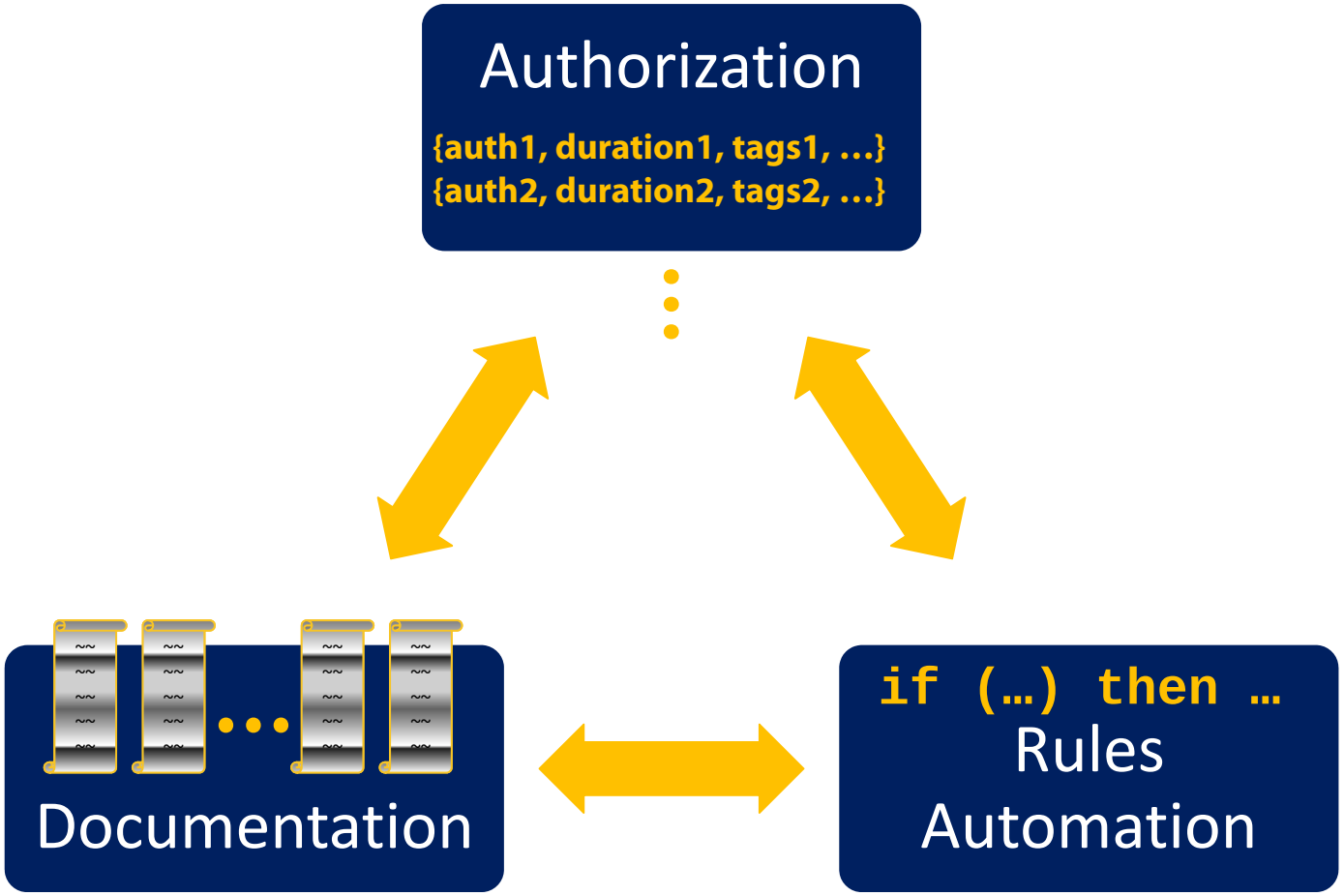
Rules Architecture (Compliance++)

Security in knowledge

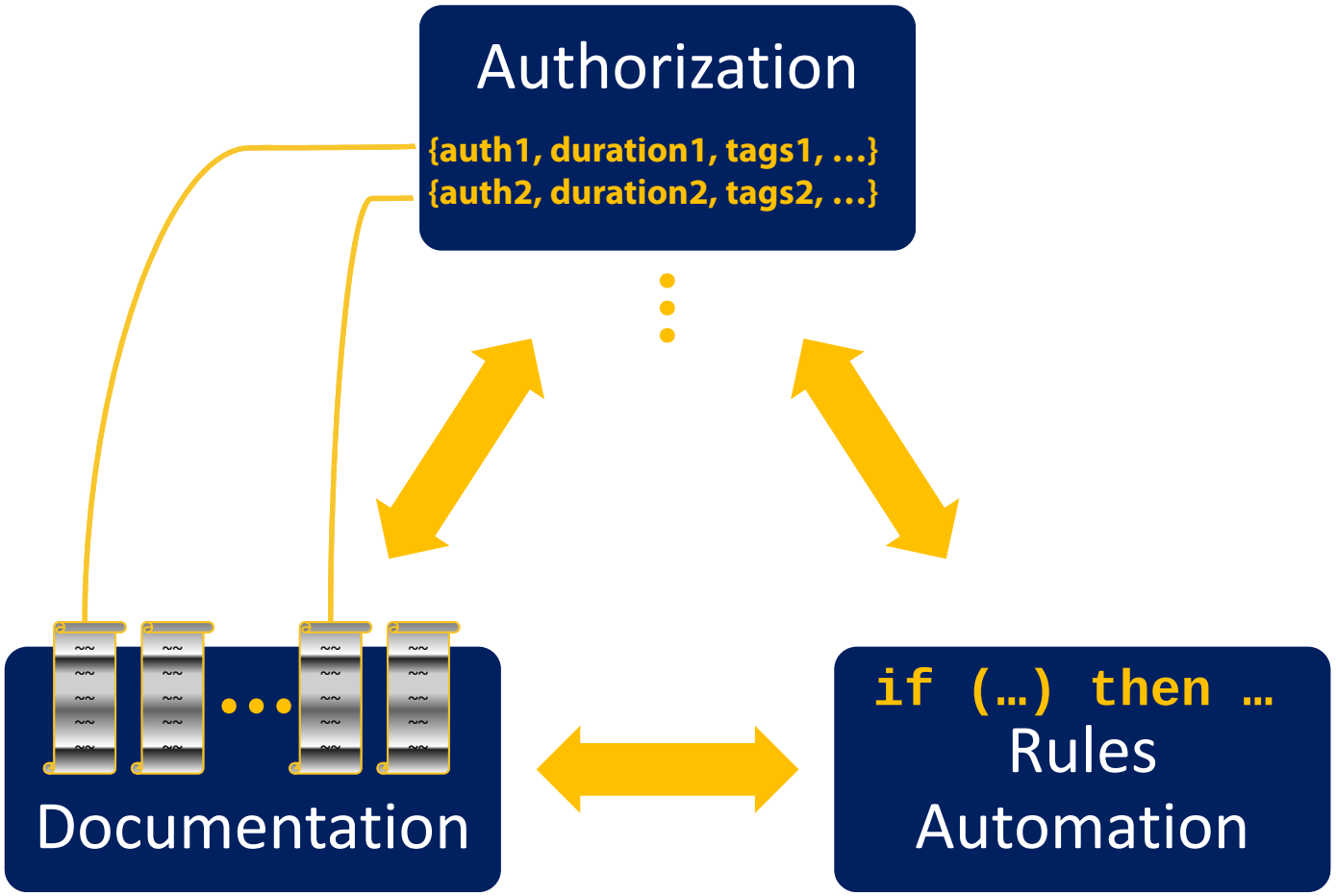
Rules Architecture (High Level)



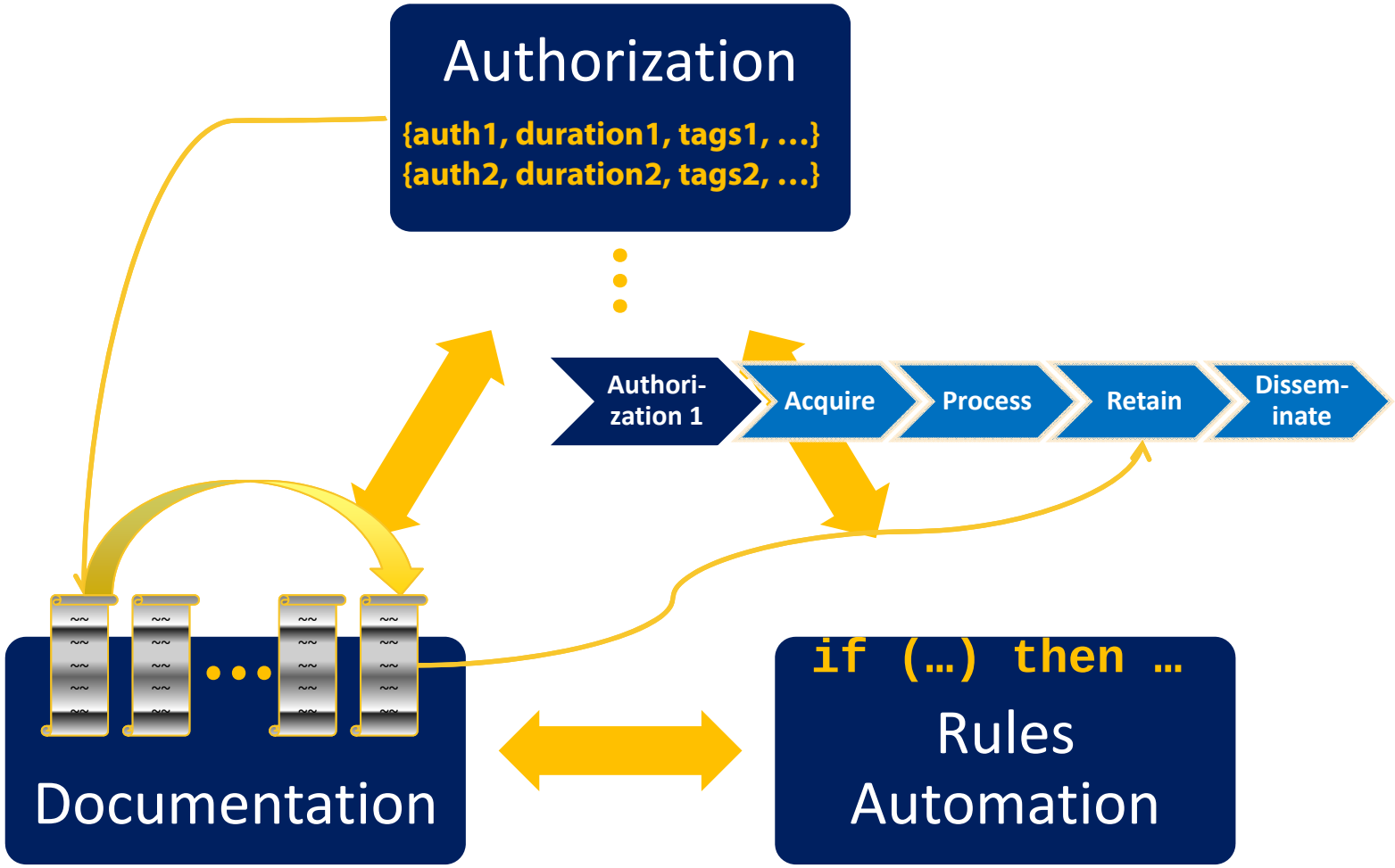
Rules Architecture (More Detail)



Authorizations Link to Documents



Automation Connects Documentation and Authorization



Rules Architecture Comparison

	Documentation	Authorizations	Rule Automation
Primary Users	People	People, Systems	Systems, People
Predominant Work Roles	Legal, Policy, Compliance, Operations, Technology	Operations, Technology, Compliance, Policy, Legal	Technology, Operations, Compliance, Policy, Legal
Loading Time	Fast	Fastest	Faster
Transaction / Access Time	Human speed	Fast	Very Fast
Interfaces	GUI, System	GUI, System	System, GUI

Summary

Against the backdrop of constant technology change:

1. **Build Conduits**: Prioritize controls that build and maintain *direct* connections among legal, policy, operations, and technology.
   - As a compliance professional, avoid becoming those conduits.
2. **Consider a Functional Approach**: Identify where systems and people fit into the overall operations.
   - Design, implement, and monitor controls more functionally, across multiple regulatory slices.
3. **Tag the Data Smartly**: A rules architecture supports an efficient and effective use of a tagged-data regime.
   - This allows proper data-handling to be successful even with constant technology change.