Compliance Map

Connecting Regulations to Frameworks for Smart Audits

Divya Venkatraman
Vidyaraman Sankaranarayanan

DeepDive Labs
https://www.deepdivelabs.tech/

DeepDive Labs: Who are we?

SINGAPORE-BASED STARTUP PROVIDING DATA & AI SERVICES

1. **Data Competencies**: **Data** Science, Governance, Management, Repositories, and Engineering
2. **AI Competencies:** Advanced Analytics, AI Development & Deployment, Fine tuning LLMs, AI Governance, LLM Workflows, RAG, Agentic Workflows

OUR SERVICES TARGET THREE KEY AREAS

1. Training
2. Solutioning
   a. Bespoke
   b. MicroSaaS products
3. Consulting: Technology & Education

CURRENTLY COOKING

1. Trailblazer boostcamp on GenAI Essentials for Educators
2. Developing MicroSaaS tool RegExperience

Agenda

Compliance Ecosystem Overview

Document mapping & its key challenges

Our Motivation:

1. Previous work: TRACE Framework
2. Advantages of mapping regulation & framework

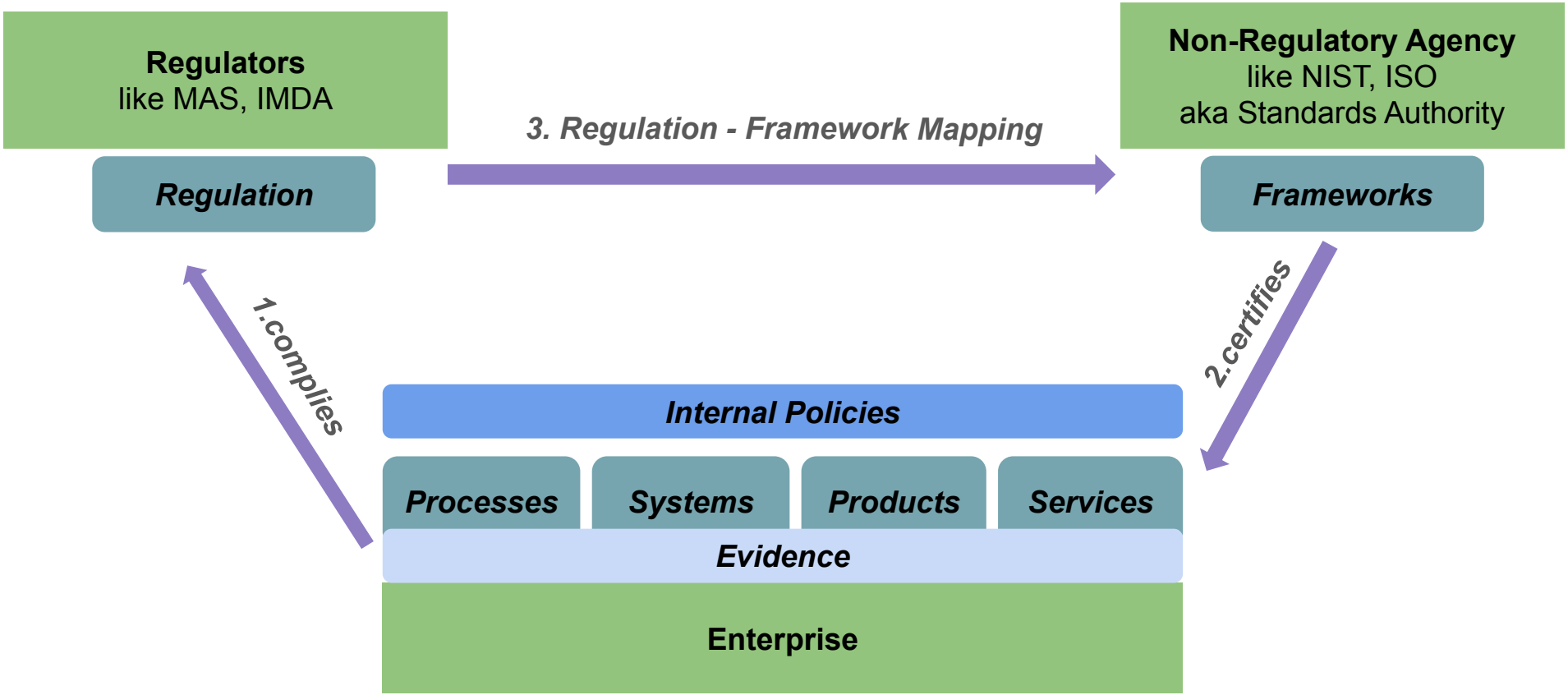
Compliance Map:

1. 4 Step-by-step process
2. Graph Model
3. Neo4j compliance map

Key findings

Q & A

Compliance Ecosystem Overview



Document Mapping Process

Process of ***organizing or structuring information*** to show ***relationships between different parts of a texts*** of two documents.

Key challenge

Lack of structure of different documents to enable mapping

- **Varied Formats**
- **Diverse Information Hierarchy**
- **Multiple Stakeholders**

Motivation

ADDRESSES **STEP 1** IN COMPLIANCE OVERVIEW PROCESS

Technical **R**egulatory **A**ssessment and **C**ompliance **E**valuation (TRACE) Framework

Given a set of **policy & evidence documents**, determine if they satisfy a **regulatory guideline.**

This work was presented at the Computational Legal Studies Conference 2024, held at Singapore Management University (SMU): https://github.com/svidyaraman/TRACE-Framework/

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

DPTM Certification Checklist

This checklist provides a broad outline based on abridged DPTM certification requirements to help organisations gauge their readiness before applying for the DPTM certification. To access the full DPTM certification requirements, organisations would need to apply for the DPTM certification at www.imda.gov.sg/dptm.

Organisations should review their data protection regime using the checklist and having a "yes" answer to all the questions is an indication that the organisation is ready to apply for DPTM.

However, kindly note that answering "yes" to all questions on this checklist **may not necessarily equate to meeting all the DPTM requirements**.

The DPTM assessment will also require the organisation to demonstrate and provide evidence for the following:

- Documented data protection policies and processes; and
- Demonstrate that data protection policies and processes are implemented and practised on the ground.

	Checklist	Yes	PDPC's Reference Advisory Guides/Guides/Templates
Principle 1: Governance and Transparency			
A: Establish data protection policies and practices			
1	Organisation shall have data protection policies and practices approved by management, setting out the organisation's approach to managing personal data (include management of special categories of personal data such as personal data of a sensitive nature) for various stakeholders such as:		• Advisory Guidelines on Key Concepts in the Personal Data Protection Act • Guide to Accountability under the Personal Data Protection Act
	• Employees - Internal data protection policy and notice	☐	• Data Protection Notice Generator (https://apps.pdpc.gov.sg/dp-notice-generator/introduction)
	• Customers, Job applicants, visitors etc - External data protection notices	☐	
	• Third party vendors - Third party agreement for management of the organisation's personal data	☐	• Guide to Managing Data Intermediaries • Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data

https://www.imda.gov.sg/-/media/imda/files/programme/dptm/dptm-checklist.pdf

DPTM Checklist Structure

Principle 1: Governance and Transparency

- Establish data protection policies and practices (10) : Across different stakeholders
- Establish queries, complaints and dispute resolution handling processes (2): Across different stakeholders
- Establish processes to identify, assess and address data protection (3)
- Establish data breach plan (5): Different levels of planning
- Accountability (2)
- Internal Communication & Training (1)

Principle 2: Management of Personal Data

- Appropriate purpose (1)
- Appropriate Consent (2)
- Appropriate Use and Disclosure (4): Across different process
- Compliant Overseas Transfer (2)

Principle 3: Care of Personal Data

- Appropriate protection (4)
- Appropriate Retention and Disposal (5)
- Accurate & complete record (3)

Principle 4: Individual's Rights

- Effect withdrawal of consent (2)
- Provide access and correction rights(4)

NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management Version 1.0 Core

NIST Privacy Framework Core		
Function	Category	Subcategory
IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.	**ID.IM-P1:** Systems/products/services that process data are inventoried.
		ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.
		ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.
		ID.IM-P4: Data actions of the systems/products/services are inventoried.
		ID.IM-P5: The purposes for the data actions are inventoried.
		ID.IM-P6: Data elements within the data actions are inventoried.
		ID.IM-P7: The data processing environment is identified (e.g.,
		ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.

Shading Key:

The Function, Category, or Subcategory aligns with the Cybersecurity Framework, bu

The Category or Subcategory is identical to the Cybersecurity Framework.

https://www.nist.gov/document/nist-privacy-framework-v10-core

NIST Privacy Framework

Information Hierarchy

- **Function**

  *Eg: **Identify**: Develop the organizational understanding to manage privacy risk for individuals arising from data processing.*

  - **Category**

    *Eg: **Inventory and Mapping**: Data processing by systems, products, or services is understood and informs the management of privacy risk.*

  - **Subcategory or Framework Requirement**

    Eg: *Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.*

Function:

- Identify
- Govern
- Control
- Communicate
- Protect

Now… in this work…

Why regulation to framework mapping?

Compliance Management Benefits

- **Comprehensive Compliance:** Maps framework standards to internal policies, identifying overlaps and gaps.
- **Resource Allocation:** Focuses on critical elements of regulations, optimizing time and costs.

Audit & Assessment Readiness

- **Streamlined Audits:** Mapped frameworks enable quicker, efficient compliance reviews.

Improved Communication

- **Enhanced Understanding:** Visual mapping clarifies departmental roles within compliance.

Training & Awareness

- **Targeted Training:** Tailored materials increase staff comprehension of compliance roles

Compliance Mapping Illustrated

DPTM Checklist

Checklist
Principle 1: Governance and Transparency
A: Establish data protection policies and practices
Organisation shall have data protection policies and practices approved by management, setting out the organisation's approach to managing personal data (include management of special categories of personal data such as personal data of a sensitive nature) for various stakeholders such as:

- Employees - Internal data protection policy and notice
- Customers, Job applicants, visitors etc - External data protection notices
- Third party vendors - Third party agreement for management of the organisation's personal data

mapping

NIST Framework

Function
IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.

Category
Inventory and Mapping (ID.IM-P): Data processing by systems, products, or services is understood and informs the management of privacy risk.

Subcategory
ID.IM-P1: Systems/products/services that process data are inventoried.
ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.

Compliance map: 4-step process

1. Process DPTM checklist (Regulation)
2. Process NIST privacy framework
3. Map Regulation to Framework
4. Create compliance map graph

Compliance map: Code walkthrough

1. **Process DPTM checklist**
2. **Process NIST privacy framework**
3. Map regulation to Framework
4. Create compliance map graph

github: https://github.com/divya-deepdivelabs/NODES24

Keep your OpenAI API Key ready!

Contextualized Requirements -> Embedding

```
analysis_prompt = """An item framework requirement from the NIST Privacy Framework is provided below:
{framework_requirements}

This framework requirement is tagged under the function objective:
{functional_objective}

and  category:
{category}

Please give a short succinct contextualized framework requirements that captures the requirement within the context of function
and category. Make sure to include all details from the requirement.
The contextualized framework requirement will be used for the purposes of improved embedding to enable better mapping with regulations.
Answer only with the succinct contextualized framework requirement and nothing else.
"""
```

Framework Requirement:
Systems/products/services that process data are inventoried.

Functional Objective:
Develop the organizational understanding to manage privacy risk for individuals arising from data processing.

Category:
Data processing by systems, products, or services is understood and informs the management of privacy risk.

Contextualized requirement:
Maintain a comprehensive inventory of all systems, products, and services that process data to enhance organizational understanding and management of privacy risks associated with data processing activities.

Reference: [Introducing Contextual Retrieval \ Anthropic]

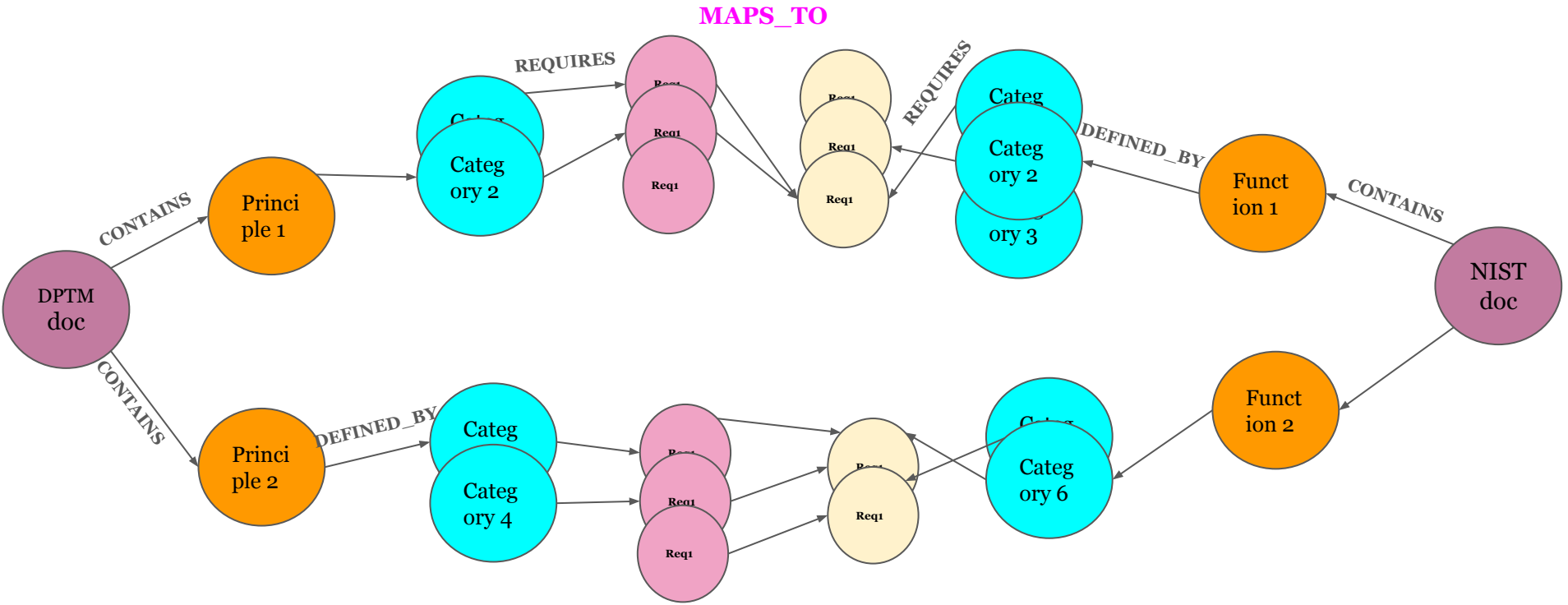
Compliance map: Code walkthrough

1. Process DPTM checklist
2. Process NIST privacy framework
3. **Map regulation to Framework**
4. **Create compliance map graph**

Keep your OpenAI API Key ready!

github: https://github.com/divya-deepdivelabs/NODES24

Graph model


MAPS_TO
REQUIRES
REQUIRES
CONTAINS
CONTAINS
CONTAINS
DEFINED_BY
DEFINED_BY
DPTM doc
Princi ple 1
Princi ple 2
Categ ory 2
Categ ory 4
Categ ory 2
Categ ory 3
Categ ory 6
Funct ion 1
Funct ion 2
NIST doc
Req1
Req1
Req1
Req1
Req1
Req1

Review Results: Top Framework Requirements

1. TOP NIST Framework Requirements
   a. Count of MAPS_TO range from 25 to 1
2. Cypher:

```
MATCH
(n:NISTRequirements)<-[r:MAPS_TO]-()
RETURN
n.Code,n.Description,COUNT(r) ORDER
BY count(r) DESC
```

Top 3 NIST Requirements

1. Legal, regulatory, and contractual requirements regarding privacy are understood and managed: **GV.PO-P5**
2. Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place. **CT.PO-P3**
3. Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes,practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place. **CM.AW-P1**

Not mapped NIST Requirements

- # NIST Framework requirements: 100
- # NIST Framework requirements mapped to Reg Requirements: 49
- # NIST Framework requirements mapped to Reg Requirements: 51
- Example of Framework requirements not mapped:
  - ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated
  - ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements communicated.
  - ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias

Comparison of *close* NIST Framework Requirements

CT.DM-P3: Data elements can be accessed for **alteration.**

The organisation shall document and implement appropriate protection measures to prevent unauthorised access, collection and use of its personal data in its possession or under its control, which may include establishing contractual agreements with third parties to whom personal data is transferred to, to ensure reasonable security arrangements to protect personal data are in place.

The organisation shall provide information to individuals on the mechanism for correction request and keep records of all such requests.

The organisation shall provide information to individuals on the mechanism for access requests and keep records of all requests.

CT.DM-P4: Data elements can be accessed for **deletion**.

The organisation shall document and implement appropriate protection measures to prevent unauthorised access, collection and use of its personal data in its possession or under its control, which may include establishing contractual agreements with third parties to whom personal data is transferred to, to ensure reasonable security arrangements to protect personal data are in place.

The organisation shall implement measures (with appropriate contractual provisions) to ensure outsourcing of disposal, destruction or anonymisation of personal data by third party service providers is in accordance with data protection obligations.

The organisation shall have documented policies, processes and mechanisms for the disposal, destruction or anonymisation of all personal data held by the organisation and its third parties.

The organisation shall provide information to individuals on the mechanism for access requests and keep records of all requests.

Key Learnings

- We mapped DPTM Requirement to NIST Privacy Framework
- Mapping of the documents is aided by setting an information hierarchy for both documents
  - Function
  - Category (under function)
  - Requirements
- Building the contextual framework requirements played a key role in context-aware encoding the requirements
- Analysis shows that the mapping are relevant.

Future work

Typically, regulations are unstructured. The information hierarchy:

Function ⇒ Category ⇒ Requirements

can be used to parse regulations to extract information

- Currently working to map MAS TRM with NIST 800-53
- For improved mapping, we would like to dive into the specifics of a requirement for different stakeholders especially
  - Internal like employees, management etc. vs
  - External like job seekers, third party vendors etc.

- Follow us on LinkedIn for regular updates https://www.linkedin.com/company/deepdive-labs/

- If you are interested to explore document mapping for other use cases, write to us hello@deepdivelabs.tech