TRACE: A Framework to Assist Auditors in Evaluating Regulatory Compliance

Vidyaraman Sankaranarayanan
DeepDive Labs
Singapore
vidyaraman@deepdivelabs.tech

Divya Venkatraman
DeepDive Labs
Singapore
divya@deepdivelabs.tech

ABSTRACT

Regulations, like the MAS TRM Guidelines for Cloud Outsourcing, operate with the force of the law. To ensure compliance, organizations develop internal policy documents aligned with regulatory requirements and mandate adherence by internal teams. These teams provide evidence of compliance through policy and evidence documents. During audits, compliance is assessed by auditors who evaluate whether the policy and evidence meets regulatory standards. In this paper, we introduce TRACE, a **T**echnical **R**egulatory **A**ssessment and **C**ompliance **E**valuation framework to assist in the compliance judgement. TRACE offers two main contributions: first, Compliance Mapping, which frames the evaluation problem as a mapping between regulatory, policy, and evidence documents, allowing for Large Language Model (LLM) techniques to assist in the process. Second, Regulatory Prompting, derived from Legal Syllogism Prompting, provides an initial judgement of compliance to support human auditors in their decision-making process. We report the results of testing the TRACE framework on the Data Protection Trustmark (DPTM) certification requirements published by the IMDA in Singapore, using publicly available privacy policies as policy/evidence documents.

KEYWORDS

Regulatory Guidelines, Compliance Evaluation, LLM;
Streamlining audit workflow, Regulatory Prompting

1. INTRODUCTION

Regulatory guidelines are meant to provide safeguards for critical services such as banking, and protect fundamental human rights, such as privacy. These guidelines, while not a law, operate with the force of the law, which means they have the same binding legal authority as laws passed by a legislative body (such as a parliament or congress). For example, banks in Singapore need to be compliant with regulations such as the Technology Risk Management (TRM) Guidelines for Cloud Outsourcing published by the Monetary Authority of Singapore (MAS) [8]. As part of their compliance procedures, banks create policy documents and mandate teams to follow these policies. Teams within the organization follow these policies and provide proof of their adherence through a set of evidence documents.

Evaluating if these policies and processes adhere to the regulatory requirements is done by different roles, such as an internal compliance officer in an organization, or an auditor in an external auditing company or the regulator themselves.[1] The audit process involves understanding the regulation and its requirements, both in letter and in spirit, analyzing the internal policies and processes of the organization, and finally making a judgement call if they satisfy the regulatory requirements. Depending on the context, a compliance officer may choose to be comprehensive and evaluate *all* the requirements while an external auditor may choose to randomly sample a smaller set for evaluation. During an audit, an auditor makes a compliance judgement by evaluating whether the policy and evidence documents together satisfy the regulatory requirements. If the auditor determines that these documents meet the requirements, the FSI is considered compliant with the regulation. The process is currently mostly manual, as different clauses need to be read and mapped across different documents. There are multiple challenges in the process of compliance evaluation.

Here we illustrate two of the top challenges:

- **Lack of Structure:** Regulatory documents are not always well structured. They are free form and can have any ontology. For example, outsourcing guidelines like the MAS TRM [8] or the Malaysian RMiT [1] have topics under data resilience, encryption, etc. Privacy-oriented regulations like GDPR, PDPA have topics around the rights of subjects, concepts like controllers and processors, etc. The stakeholders in regulations are different and sometimes a single requirement may encompass multiple stakeholders.
- **Different Types of Documents:** Requirements in a single regulation often require multiple policy and evidence documents. In some cases, the policy and the evidence sections may be in the same document itself. For example, a requirement to ensure all data subjects are made aware of their rights may be worded in a single sentence, but targeted at different stakeholders, like employees, customers and job applicants. Multiple policy documents would address this 'single' requirement since each of the documents would be applicable to different stakeholders. Based on the regulation requirement, evidence can be transcripts of interviews, or policy updates on a webpage or analytical dashboard

[1] Herein 'compliance officer' and 'auditor' are used interchangeably in this paper

1.1 Contributions

The compliance evaluation process as described above can be framed as a language task and is hence a good use case for the application of LLMs. In this work, we present **TRACE**, a **T**echnical **R**egulatory **A**ssessment and **C**ompliance **E**valuation framework to assist in the compliance judgement. This paper has two principal contributions:

1. **Compliance Mapping:** The compliance evaluation problem is framed as a mapping of the sections of different artifacts, viz., the regulation, the policy, and the evidence documents, so that LLM based techniques can be applied for assisting in the evaluation process.
2. **Regulatory Prompting:** A "Regulatory Prompting" technique, derived from Legal Syllogism Prompting, provides an initial judgment call for compliance, which can then be used as an assistance for human judgement.

These technical contributions are codified into the TRACE framework. Throughout this paper, we will use the Data Protection Trustmark (DPTM) [4] as an example. While the DPTM is not a regulatory requirement, it has a set of well-defined requirements, and a set of certified organizations that publish their privacy policies which enables us to evaluate the TRACE framework.

2. TRACE FRAMEWORK

The TRACE framework is a structured set of steps designed to facilitate the audit process, whether conducted by compliance officers or external auditors. It systematically guides the mapping of regulatory documents to policy documents and further to evidence documents. The framework consists of the following steps:

1. **STEP #1: EXTRACTION OF REQUIREMENTS:** The first step involves identifying the regulatory document that serves as the foundation for assessing compliance and extracting a detailed list of requirements from it. These requirements form the basis for subsequent validation by the compliance officer. It is important to note that outputs generated by the Large Language Models (LLMs) in this process must be manually verified by a human to ensure accuracy.
2. **STEP #2: COMPLIANCE MAPPING:** *Regulation-to-Policy Mapping*: In the second step, the framework focuses on identifying relevant sections within the policy and evidence documents that correspond to the regulatory requirements identified in Step 1. This is achieved by prompting the LLM to locate sections within each policy document that are related to these regulatory requirements. Optionally, the identified sections can expanded by adding a context window of 500 characters before and after the relevant text, providing a comprehensive view to be used in further analysis.
3. **STEP #3: REGULATORY PROMPTING:** *Judgement on Policy*: The final step involves making a compliance judgement based on the information gathered in the previous steps. We use a "Regulatory Prompting" technique, derived from the work on Legal Syllogism Prompting [7]. Specifically:

    - we define a "major premise" in the prompt as the regulatory requirement
    - we define a "minor premise" in the prompt as the assertion in the policy documents, and
    - we define a "judgement" to be evaluated if the policy assertion satisfies the regulatory requirement.

    This template is applied to determine if a policy document aligns with a subset of the regulatory requirements. As a second phase, the same prompt can be used to determine if an evidence document supports the assertions in a policy. Sometimes the policy and the evidence documents may be the same (or elements of the policy and evidence can be found in the same document), so a single pass with a regulatory prompt is sufficient[1]. The outcome of this analysis is a judgement—categorized as **`MET`**, **`NOT MET`**, or **`PARTIALLY MET`** – accompanied by notes on the sufficiency and appropriateness of the evidence provided.

By following these steps, the TRACE framework ensures a thorough and systematic audit process, enhancing the accuracy and reliability of compliance assessments. These steps are illustrated in Figure 1.

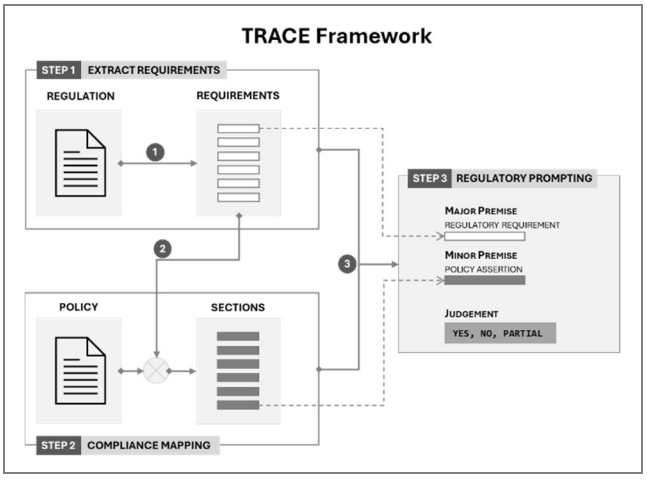

Figure 1: TRACE framework

[1] Herein, policy and evidence documents are referred to interchangeably, though in practice they have a clear distinction in content and purpose.

A formal definition of a regulatory document, a policy (and evidence) document, and the compliance mapping process is shown in appendix A.

3. IMPLEMENTING TRACE

There are different ways in which the framework can be used to aid the audit process. These involve implementing the steps with Chain-of-Thought (CoT) [9] prompting technique with different prompt templates and combinations. A Chain-of-Thought (CoT) [9] prompt involves guiding the model through a structured, step-by-step reasoning process to arrive at a decision. In this prompt, the auditor is instructed to follow a detailed, multi-step process: extracting regulatory requirements, mapping them to policy clauses, and then making a judgement based on this mapping. Each step builds upon the previous one, leading to a final output that includes a compliance judgement, an explanation, and a suggestion for evidence type, which aligns with the CoT approach [9]. In this section we illustrate two approaches to implementing the TRACE framework. The complete prompts with the JSON formatting and the regulatory prompting template are available at `https://github.com/svidyaraman/TRACE-Framework`.

3.1. Single-step prompt

The TRACE inspired Single-step prompt is a single prompt for all the three steps in the framework. It is equivalent to uploading the regulation, policy and evidence documents into the ChatGPT interface and providing a single Chain-of-Thought (CoT) [9] prompt to do all the steps. A summary of the prompt is shown in Figure 2.

STEP #1	**SINGLE STEP PROMPT**

- YOU ARE AN AUDITOR RESPONSIBLE FOR EVALUATING DATA PROTECTION REGULATIONS IN SINGAPORE.
- YOUR TASK IS TO EXTRACT DATA PROTECTION REQUIREMENTS FROM THE DATA PROTECTION TRUSTMARK CHECKLIST AND MATCH THEM TO THE RELEVANT CLAUSES IN THE PROVIDED POLICY DOCUMENT.
- BASED ON THIS MAPPING, YOU NEED TO PROVIDE A COMPLIANCE JUDGEMENT (**MET, NOT MET, PARTIALLY MET**), AN EXPLANATION FOR EACH JUDGEMENT, AND SUGGEST THE TYPE OF EVIDENCE REQUIRED, ALL FORMATTED IN A SPECIFIC JSON STRUCTURE.

Figure 2: Summarized Single-Step Prompt

Advantage: The systematic workflow of TRACE helps to provide a Chain-of-Thought (CoT) prompt [9] to help achieve the objective.

Disadvantage: As mentioned earlier, all these documents (regulatory, policy and evidence) are long form. Hence systematic mapping of *all* regulatory requirements to policy sections (evidence) is not possible because of restrictions in the number of output tokens. Furthermore, the results are not reproducible over multiple runs of the prompt.

This approach is best used for a small category of regulations, with a smaller policy or evidence document, for quick validations of assertions.

3.2. Workflow Prompting

The workflow prompting approach is inspired by the TRACE framework. Here each step in the TRACE framework is elaborated as a Chain-of-Thought (CoT) prompt [9]. Figure 3 shows a summarized prompt for each of the steps.

STEP #1	**REQUIREMENTS EXTRACTION PROMPT**

- AS AN AUDITOR ASSESSING PRIVACY REGULATIONS IN SINGAPORE, YOUR TASK IS TO EXTRACT AND ANALYZE ALL REGULATORY REQUIREMENTS FROM THE DATA PRODUCTION TRUSTMARK (DPTM) CHECKLIST PROVIDED IN THE DOCUMENT.
- YOU NEED TO IDENTIFY EACH CHECKLIST ITEM'S CATEGORY, SUBCATEGORY, APPLICABLE STAKEHOLDER, AND THE CORRESPONDING POLICY DOCUMENT DETAILS FOR THE CATEGORY **"{CATEGORY_OF_INTEREST}"**.
- THE EXTRACTED INFORMATION SHOULD BE FORMATTED INTO A STRUCTURED JSON FORMAT, ADHERING STRICTLY TO THE SPECIFIED GUIDELINES.

STEP #2	**COMPLIANCE MAPPING PROMPT**

- AS AN AUDITOR ASSESSING PRIVACY REGULATIONS IN SINGAPORE, YOUR TASK IS TO EXTRACT CLAUSES FROM THE ORGANIZATION'S POLICY DOCUMENT THAT CORRESPOND TO SPECIFIC REGULATORY REQUIREMENTS.
- YOU MUST READ THROUGH THE ENTIRE POLICY DOCUMENT AND IDENTIFY THE EXACT CLAUSES THAT ALIGN WITH EACH REGULATORY REQUIREMENT LISTED.
- THE RESULTS SHOULD BE PRESENTED IN A STRUCTURED JSON FORMAT, DETAILING THE REGULATORY REQUIREMENT DESCRIPTION, THE CORRESPONDING POLICY CLAUSES, AND THE POLICY CATEGORY.

STEP #3	**REGULATORY PROMPTING**

- AS AN AUDITOR ASSESSING PRIVACY REGULATIONS IN SINGAPORE, YOUR TASK IS TO DETERMINE IF AN ORGANIZATION'S POLICY DOCUMENTATION ALIGNS WITH SPECIFIC REGULATORY REQUIREMENTS.
- USING THE PROVIDED REGULATORY REQUIREMENT AS THE MAJOR PREMISE AND THE CORRESPONDING POLICY DOCUMENTATION AS THE MINOR PREMISE, YOU NEED TO MAKE A JUDGEMENT (**NOT MET, PARTIALLY MET, MET**) AND PROVIDE AN EXPLANATION FOR IT.
- ADDITIONALLY, SUGGEST THE TYPE OF EVIDENCE NEEDED TO VERIFY COMPLIANCE, AND PRESENT THE FINDINGS IN A STRUCTURED JSON FORMAT.

Figure 3: Summarized 3-Step Prompt

Advantage: The workflow prompting approach has the advantage of providing reproducible results. Since the output is provided for each of the steps in the workflow, there is also an audit trail of the reasoning steps, and hence it allows us to backtrack to

find out a missed regulatory requirement, or a missed policy section, or an incorrect judgement.

Disadvantage: An obvious disadvantage is this approach requires multiple calls to the LLM. Depending on the length of the regulatory document, and the number of policy / evidence documents, a single step would require multiple calls to the LLM, along with some engineering work to split the input documents appropriately, and finally merge the outputs.

	WORKFLOW PROMPTING	SINGLE-STEP PROMPTING
DEFINITION	*Each step in the* TRACE *framework is elaborated as a Chain-of-Thought prompt*	*All the three steps in the* TRACE *framework are provided as a single Chain-of-Thought prompt*
ADVANTAGES	• provides reproducible results • provides an audit trail of the reasoning steps	• useful for validation of snippets of regulatory requirements
DISADVANTAGES	• requires multiple calls to the LLM (higher cost)	• complete compliance mapping is not possible due to limited number of output tokens • results are not reproducible over multiple runs

Table 1. Comparison of Single-step and Workflow Prompting

4. TESTING

We have validated the TRACE framework using the DPTM certification requirements [4] published by the IMDA in Singapore. This document is used in lieu of a regulatory document for testing purposes. A description of the DPTM from the website [4]: *The Data Protection Trustmark (DPTM) is a voluntary enterprise-wide certification for organizations to demonstrate accountable data protection practices.* The DPTM website also has a list of certified organizations [5], so we were able to get the privacy policies from their websites of these organizations, to be used as the policy / evidence document. In addition, we were also able to get the privacy policy specific to job applicants from the public website. This enabled us to do a two-phase testing on the TRACE framework.

DOCUMENTS USED

- Regulatory document: DPTM certification requirements available here [4]. As a ground truth, we manually derived the list of requirements from the DPTM (a total of 50 requirements)
- Policy document: privacy policy from DBS [2] and Grab [3] website.
- Evidence document: privacy policy for *job applicants* from DBS and Grab career page

4.1. Single-step Prompt: Results

The single step prompt shown in Figure 2 was first executed with the DPTM certification and the privacy policy of DBS and Grab as input documents. Although this prompt had both Chain-of-Thought [9] and Regulatory Prompting techniques, the results were very poor due to the small output token. Specifically:

1. Only five requirements were extracted from the prompt
2. Every run had a different set of requirements, and equivalent policy sections extracted from privacy policy for each run.
3. Judgements were **`PARTIALLY MET`** or **`MET`** depending on the runs indicating the regulatory prompting technique worked as expected.

4.2. Workflow Prompting: Results & Insights

Table 2 shows the results of each step in the workflow prompting approach.

INPUT	OUTPUT
STEP #1: Regulatory requirements were extracted using the DPTM document as an input along with the step#1 prompt specified in Figure 3	**31** requirements were extracted from the DPTM
STEP #2: For Compliance Mapping, we provided the DPTM requirements list that were manually extracted (totaling 50 requirements, instead of only the 31 that were extracted in step #1).	**ALL** the 50 requirements were mapped to appropriate policy sections. • Some of the clauses around **Consent** were not found in the privacy policy for Grab
STEP #3: The Regulatory Prompt in Figure 2 was executed with the manually extracted regulatory requirements as the *major premise*, and the compliance mapped policy assertions (i.e., the relevant policy section) as the *minor premise*, and the output as a judgement if the (policy) assertion satisfied the (regulatory) requirement.	**JUDGEMENTS** for most regulatory requirements were **`PARTIALLY MET`** due to lack of supporting comprehensive policies. • For Grab privacy policy: **`MET: 1`**, **`NOT MET: 8`** and **`PARTIALLY MET: 41`**. • For DBS privacy policy, they were **`NOT MET: 3`** and **`PARTIALLY MET: 47.`**

Table 2. Workflow Prompting Results

An analysis of the results revealed these insights:

1. The only requirement that was **`MET`** for Grab was around overseas transfers: "*The organization shall establish processes to assess and ensure that the personal data that is transferred overseas is accorded a standard of protection that is comparable to that under the PDPA."* with an explanation of the judgement as "*The policy documentation explicitly*

states that when transferring personal data from the Home Country to an Alternate Country, the organization will ensure that the recipient in the Alternate Country is obliged to protect the personal data at a standard of protection comparable to that under applicable laws, which aligns with the regulatory requirement of ensuring a comparable standard of protection as under the PDPA." There were no mentions of overseas transfers in the DBS policy.

2. For the requirements around notices to job applicants, the judgement in step #3 with the privacy policy from the website (for both Grab and DBS) were marked as **`PARTIALLY MET`**; however, when the compliance mapping and the regulatory prompt were run with the added evidence of the privacy policy for job applicants **along with the context**, the requirement that mandated publication and communication of the privacy policy to the job applicant was marked as **`MET`** for both Grab and DBS.
3. The requirements extraction & compliance mapping step extracted appropriate categories and corresponding sections from the privacy policy, namely Data Protection, Training, Data Protection Impact Assessment (DPIA), etc.
4. Since the privacy policies we used were meant for public consumption, procedures around Data breach were not explicitly mentioned, but they were still inferred from the context during the compliance mapping process and were correctly determined that its **`PARTIALLY MET`**.
5. Many nuances were also clearly explained between the two privacy policies. We call out the ones under the Data Breach category for illustration:
   - Grab Policy: "*We will take reasonable legal, organisational and technical measures to ensure that your Personal Data is protected. This includes measures to prevent Personal Data from getting lost, or used or accessed in an unauthorised way."*
   - DBS Policy: "*In addition, should we be aware that your data has been compromised and is, or likely to result in significant harm to you, we will notify you and advise on the possible steps to protect yourself from further potential harm."*

     The compliance mapping process in the Grab policy stated it ensured taking "reasonable measures" while in the DBS policy it found that "notification" was assured. Neither mention data breach management, but the inference that they were related to data breach management was correctly made.

4.3. Limitations & Challenges

The testing for the TRACE framework has been done with a view to validate the approach from an academic standpoint, and a few major limitations need to be noted for the industry applications:

1. None of the judgements for the compliance of any company towards the DPTM is an accurate picture, since the actual audit and certification process is bound to have a number internal policy and evidence documents, which we do not have access to. Hence it should be noted that a judgement (**`MET`**, **`NOT MET`**, or **`PARTIALLY MET`**) should be interpreted only in the limited academic sense for framework evaluation, not actual compliance.
2. We only tested privacy policies of two companies, DBS and Grab (chosen since they are well known in Singapore). More than 100 companies have the DPTM certification, and the same testing can be performed on them to understand their compliance with DPTM.
3. There is no proof of completeness, i.e., although we can extract a set of requirements from a regulatory document and perform compliance mapping, they need to be validated as 'complete' by a human. There is no guarantee that the requirements are completely extracted from the document (through LLM prompting alone).
4. Practical engineering challenges remain around parsing documents, While OpenAI allows for PDF document analysis by simply uploading a document, support for embedded images is still pending. So, evaluating evidence documents that may have screenshots of configurations are not possible today via the LLM interface; instead, separate parsing components needs to be present for handling images (and in general, unsupported formats).

5. CONCLUSION

In this paper, we have proposed the TRACE framework to evaluate compliance of an organization with a regulation, based on artifacts like policy and evidence documents. The framework is a sequence of steps involving extraction of requirements from a regulation, and then performing a compliance mapping to derive sections of a policy or evidence document relevant to the regulatory requirements, followed by a regulatory prompting technique to get a compliance judgement.

We used the DPTM document for tactical testing of the framework. The testing validated the basic contributions of the TRACE framework, viz., compliance mapping and regulatory prompting. The single step prompting technique was less effective for the DPTM document, but the workflow prompting technique was effective for getting relevant sections and judgements for the regulatory requirements. A second order validation of the regulatory prompting technique was obtained when we provided the second job-seeker related privacy policy to the regulatory requirements. From a framework standpoint, the second policy document could be considered as an evidence document for the initial privacy policy. Further work in this area are as follows:

- We plan to integrate Retrieval Augmented Generation (RAG) techniques along with prompting to extract a complete set of mutually exclusive requirements from long documents.
- The regulatory prompting technique needs to be updated to include standards for judgement. For example, satisfiability of an audit evidence is codified with different standards, e.g., "Sufficient Appropriate Audit Evidence" per the Singapore Standards on Auditing, SSA 500 [6]. There are multiple standards for the satisfiability of an audit evidence, and the Regulatory prompt can be updated to provide those standards as a basis for the judgement.

REFERENCES

[1] Bank Negara Malaysia (BNM). 2023. Risk Management in Technology (RMiT) Policy Document. Retrieved from https://www.bnm.gov.my/documents/20124/938039/PD-RMiT-June2023.pdf

[2] DBS Bank Ltd. 2024. DBS Privacy Notice. Retrieved from https://www.dbs.com/privacy/default.page

[3] Grab Holdings Inc. 2024. Grab Privacy Notice. Retrieved from https://www.grab.com/sg/terms-policies/privacy-notice/

[4] Infocomm Media Development Authority (IMDA). 2024. Data Protection Trustmark (DPTM). Retrieved from https://www.imda.gov.sg/how-we-can-help/data-protection-trustmark-certification

[5] Infocomm Media Development Authority (IMDA). 2024. Directory of DPTM-Certified Organizations. Retrieved from https://www.imda.gov.sg/-/media/imda/files/programme/dptm/dptm-certified-organisation.pdf

[6] Institute of Singapore Chartered Accountants (ISCA). 2021. Singapore Standard on Auditing, SSA 500. Retrieved from https://isca.org.sg/docs/default-source/audit-assurance/aa-standards/ssa-500-(dec-2021).pdf?sfvrsn=54c32185_2

[7] Jiang, C., and Yang, X. 2023. Legal Syllogism Prompting: Teaching Large Language Models for Legal Judgment Prediction. In Proceedings of the Nineteenth International Conference on Artificial Intelligence and Law (ICAIL '23). Association for Computing Machinery, New York, NY, USA, 417–421. https://doi.org/10.1145/3594536.3595170

[8] Monetary Authority of Singapore (MAS). 2021. Guidelines on Risk Management Practices – Technology Risk. Retrieved from https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines

[9] Wei, J., Wang, X., Schuurmans, D., Bosma, M., Ichter, B., Xia, F., Chi, E. H., Le, Q. V., and Zhou, D. 2024. Chain-of-thought prompting elicits reasoning in large language models. In Proceedings of the 36th International Conference on Neural Information Processing Systems (NIPS '22). Curran Associates Inc., Red Hook, NY, USA, Article 1800, 24824–24837.

[10] Zhang, X., and Brown, P. 2023. LongWriter: Unleashing 10,000+ Word Generation from Long Context LLMs. arXiv preprint arXiv:2408.07055v1. Retrieved from https://arxiv.org/abs/2408.07055v1

APPENDIX A: TRACE FRAMEWORK FORMALIZATION

Compliance Mapping

In this section, we frame the compliance evaluation problem as a mapping problem of different sections of the regulation and the policies and evidence documents.

Regulation: A Regulation is the source document published by a regulator.
For conciseness, let ***R*** represent a specific **regulation** and S_r represent the set of all **sections** within regulation *r*.

$$S_r = \{ s_1, s_2, s_3, ..., s_n \}$$

For each section $s_i \in S_r$, let Q_{si} represent the set of all **Requirements** within section s_i.

$$Q_{si} = \{ q_{i1}, q_{i2}, q_{i3}, ..., q_{im} \}$$

So, a regulation **R** can be defined as a pair:

$$\mathbf{R} = (S_r, \{ Q_{si} \mid s_i \in S_r \})$$

The entire set of all requirements in a regulation is:

$$Q_r = \bigcup (Q_{si})$$

To illustrate with the DPTM:

- sections would be the principles mentioned in the document, such as “Governance and Transparency”, “Management of Personal Data”, etc.
- Titles and Specific requirements within each section would be “Establish data protection policies and practices”, “Establish queries, complaints and dispute resolution handling processes”, etc.

A complete tree structure of the DPTM is given in appendix B for illustration.

Policy Document: A Policy document is created by an organization with the aim of complying with a regulation. This document consists of internal sections that are intended to address specific regulatory requirements. In practice, multiple policy documents are authored to address the requirements (in different sections) of a single regulation. For example, the privacy policy of an organization, available publicly in most organizations, addresses some of the requirements of the DPTM checklist, for stakeholders like external users, job applicants, etc.

- Let **P** represent all **Policy Documents:**

$$\mathbf{P} = \{ p_1, p_2, \ldots, p_n \}$$

- Let S_p represent the set of all **internal sections** within a policy document **p**:

$$S_p = \{ s_{p1}, s_{p2}, s_{p3}, \ldots \}$$

- A policy document **p** is a set of its component sections:

$$\mathbf{p} = \{ S_p \}$$

Evidence Document: An evidence document is defined as an artifact that’s provided by the organization to prove its adherence to the regulation. In practice, the evidence document proves its adherence to an internal policy document, which in turn, derives its content from the regulatory requirements. For example, a privacy policy of an organization, available on its public website, is also an evidence document for certain provisions of the DPTM, like providing contact information for privacy queries, etc.

- Let **E** represent all **Evidence Documents**

$$\mathbf{E} = \{ e_1, e_2, \ldots, e_k \}$$

- Let S_e represent the set of all **internal sections** within a evidence document **e**.

$$S_e = \{ s_{e1}, s_{e2}, s_{e3}, \ldots \}$$

- Analogous to the definition of a policy document, an evidence document **e** is a set of its component sections:

$$\mathbf{e} = (\mathbf{S_e})$$

Mapping of Sections to Requirements: Assuming that each policy document **p** addresses one or more requirements from regulation **R**, this relationship can be represented by a function:

- **f: P → P(**Q_r**)**,
  where **f(p)** $\subseteq$ Q_r represents the subset of requirements that the policy document **p** is intended to address (or alternatively, represents the sections in **p** that satisfy some of the requirements in **R**).
- Similarly, **g: E → E(**Q_r**)**
  where **g(e)** $\subseteq$ Q_r represents the subset of requirements that the evidence document **e** is intended to address.

"Satisfies" Operator: We define a new operator **"satisfies" (⊨)** to represent the relationship where a policy satisfies a subset of the requirements.

- A policy **p** satisfies a subset of requirements ($Q'_r \subseteq Q_r$) if **all sections** of the policy satisfy the requirements in $\mathbf{Q'_r}$.

$$p \vDash Q'_r \iff \forall\, s_{pi} \in p,\ f(s_{pi}) \subseteq Q'_r$$

The analogous statement holds true for an evidence document **e**.

$$e \vDash Q'_r \iff \forall\, s_{ei} \in e,\ g(s_{ei}) \subseteq Q'_r$$

Compliance: Given the inputs, a regulation **R**, a set of policy documents **P**, and a set of associated evidence documents **E**, an organization is said to be compliant if all the requirements in the regulations are satisfied through a combination of the policy documents and evidence documents. Hence the compliance evaluation problem is defined as finding the existence of a mapping function ***f***, and ***g***, such that (**P**, **E**) ⊨ **R.**

$$(\mathbf{P}, \mathbf{E}) \vDash \mathbf{R}\ ,\ \forall\, \mathbf{S_e} \in \mathbf{E},\ \forall\, \mathbf{S_p} \in \mathbf{P}\ \textit{if}\ \exists\, \boldsymbol{f}(S_p) \subseteq \mathbf{Q'_r}\ ,\ \boldsymbol{g}(S_e) \subseteq \mathbf{Q'_r}\ \forall\, \mathbf{Q_r}$$

Regulatory Prompting

The Regulatory prompting technique is derived from the Legal Syllogism Prompting [7], where a major and minor premise are explicitly provided, and a judgement is requested from the LLMs. We adapt this prompting technique for the TRACE framework:

- A regulatory requirement is considered as a major premise
- A section of the policy with a relevant assertion towards the regulatory requirement is considered as an minor premise
- A judgement is requested if the assertion satisfies the requirement

This is used in step 3 of the algorithm in Figure 3.

Validating the existence of the mapping functions

To validate the existence of the mapping functions ***f***, and ***g***, we need to find (at least) one mapping from the sections of the policy to the requirements in the regulations with the following steps:

1. Find the requirements $\boldsymbol{Q_r}$ in the regulation **R**
2. For every policy (and evidence) document, delineate into appropriate sections.
3. Evaluate satisfiability of each section in the policy (and evidence) document for every requirement $\boldsymbol{Q_r}$.

Figure 4 illustrates the steps as an algorithmic sequence of steps based on this formalism.

INPUT:

REGULATION **R**, POLICY DOCUMENTS **P**, EVIDENCE DOCUMENTS **E**

OUTPUT:

EXISTENCE OF MAPPING FUNCTIONS **F** AND **G**: TRUE OR FALSE

EXTRACT REQUIREMENTS FROM REGULATION

1. Use LLMs to analyze Regulation **R** and extract the set of requirements $\mathbf{Q_r}$.
   $\mathbf{Q_r} = \{q_1, q_2, \ldots, q_n\}$

PRELIMINARY SATISFIABILITY CHECK AND SECTION DELINEATION

2. For each document $\mathbf{d \in \{P \cup E\}}$:
   - **2.1.** Use prompt engineering to directly evaluate satisfiability of **d** for each $\mathbf{q \in Q_r}$.
   - **2.2.** Record results of satisfiability evaluation (Note: Judgement calls are expected to be liberal).
   - **2.3.** Use results to delineate **d** into sections $\mathbf{S_d = \{s_1, s_2, \ldots, s_m\}}$ that potentially match $\mathbf{Q_r}$.

SATISFIABILITY CHECK USING REGULATORY PROMPTING

3. **FOR** each requirement $\mathbf{q \in Q_r}$ **AND** each section $\mathbf{s \in S_d}$:
   - **3.1.** Consider **q** as the major premise
   - **3.2.** Consider **s** as the minor premise
   - **3.3.** Use LLM to judge if **s** satisfies **q** based on premises
   - **3.4.** Record judgement and reasoning

VALIDATE EXISTENCE OF MAPPING FUNCTIONS

4. **IF:** $\mathbf{\exists\ s \in S_d}$ such that **s** satisfies **q** for every $\mathbf{q \in Q_r}$:
   - **4.1.** Confirm existence of at least one mapping function $\boldsymbol{f}$: $\mathbf{S_d \rightarrow Q_r}$: **OUTPUT TRUE**
   - **4.2.** Declare organization compliant.
5. **ELSE:** Declare organization non-compliant.

Figure 4: Algorithm: Existence of Mapping Functions *f* and *g* for Compliance Check

APPENDIX B: TREE STRUCTURE OF THE DPTM

PRINCIPLE 1: GOVERNANCE AND TRANSPARENCY

- A: Establish data protection policies and practices
  - 1. Data protection policies approved by management
  - 2. Communicate data protection policies to stakeholders
  - 3. Review, update, and monitor compliance of policies
- B: Establish queries, complaints, and dispute resolution handling processes
  - 4. Policies on handling queries/complaints
- C: Establish processes to identify, assess, and address data protection
  - 5. Risk and impact assessments
  - 6. Documented DPIA and action plans
  - 7. Data Protection by Design
- D: Establish a data breach management plan
  - 8. Data breach management plan and communication
- E: Accountability
  - 9. Appoint a competent Data Protection Officer (DPO)
  - 10. DPO roles and responsibilities
- F: Internal Communication and Training
  - 11. Training programs for staff

PRINCIPLE 2: MANAGEMENT OF PERSONAL DATA

- A: Appropriate Purpose
  - 1. Policies for relevant and reasonable data collection
- B: Appropriate Consent
  - 2. Notifications on data collection purposes
  - 3. Obtaining fresh consent for new purposes
- C: Appropriate Use and Disclosure
  - 4. Policies on obtaining consent and using data
  - 5. Maintain a Data Inventory Map
- D: Compliant Overseas Transfer
  - 6. Assessing overseas data transfers
  - 7. Contractual measures for third-party transfers

PRINCIPLE 3: CARE OF PERSONAL DATA

- A: Appropriate Protection
  - 1. Document and implement protection measures
  - 2. Retention policy and schedules
  - 3. Communicate retention policies
  - 4. Disposal, destruction, or anonymization of data
- B: Appropriate Retention and Disposal
  - 5. Cease retention of unsolicited data
  - 6. Measures for third-party data disposal
- C: Accurate and Complete Records
  - 7. Verify and ensure data accuracy and completeness
  - 8. Communicate corrections to third parties

PRINCIPLE 4: INDIVIDUAL'S RIGHTS

- A: Effect Withdrawal of Consent
  - 1. Policies on handling withdrawal requests
  - 2. Information on withdrawal mechanisms
- B: Provide Access and Correction Rights
  - 3. Handling and responding to access requests
  - 4. Mechanism for access requests
  - 5. Handling and responding to correction requests
  - 6. Mechanism for correction requests