3 One example…

This section exercises an example of an essay, taking as focus the generic part “0 The Context” of the Lecture Notes…

3.1 Story: When the Wind Changed Direction

In early 2022, a state-owned public transport operator, **Tranvia Regional**, embarked on an ambitious digital journey. Inspired by a national strategic plan for digital transition and urged by political stakeholders eager to show rapid results, the operator announced a digital transformation programme to "reimagine mobility through data and cloud". The CEO, a former advisor in digital policy, assembled a fast-moving team of external consultants and declared the project a “flagship of smart governance.”

Internally, however, staff were puzzled. The transformation announcement came with no reference to the company's long-standing operational model. No preliminary studies or stakeholder mapping were conducted. Union representatives requested clarity on job impacts and were told “automation will support you, not replace you.” The statement was not backed by any formal engagement.

One early initiative under this programme involved outsourcing core mobility data to a cloud analytics platform, with the goal of implementing predictive maintenance and optimising route planning. Within six months, legacy data archives were uploaded, but no one had clarified who owned the data or how it would be governed. Regional policymakers began asking why public service data was now hosted by an international vendor with little local footprint.

As the political winds shifted in late 2022, a new regional secretary questioned the legitimacy of the programme’s procurement choices. A special audit revealed the absence of an overarching management system, no integration with existing risk and compliance frameworks, and a lack of internal documentation explaining key decisions. Public outrage followed, not over the technology itself, but over the opacity and misalignment with the operator’s public service obligations.

The CEO resigned. A transitional governance board was created. The new leadership paused the programme and initiated a participatory process to define what "transformation" should mean for Tranvia Regional, rooted in its public value mission. They began revisiting foundational issues: how governance has evolved, what forms public service takes in the digital era, and how history and institutional legacy shape what change is even possible.

3.2 Case Title: Estonia’s Digital Leap and Its Limits

Estonia is widely cited as a model of digital governance. Since the early 2000s, it has developed a robust ecosystem of e-government services, underpinned by the X-Road data exchange layer, digital ID cards, and the principle of once-only data collection. These innovations enabled near-universal online service access, from voting to prescriptions. The system was hailed globally as a digital state prototype.

Yet, in 2017, the country faced a severe challenge: researchers discovered vulnerabilities in the cryptographic keys used in ID cards, threatening the foundation of digital trust. The Estonian government acted swiftly, revoking and reissuing over 800,000 certificates. The incident revealed how deeply public services had come to rely on digital tools (and how fragile trust could become when technology outpaced institutional preparedness).

The case raised questions about systemic risk, cross-border reliance (the ID technology involved a Dutch supplier), and how governance models must evolve to handle digital interdependence. Estonia’s response, while ultimately effective, revealed the tension between digital ambition and the need for institutional memory, stakeholder understanding, and legal robustness.

Relevant Lecture Notes Sections:

- 0.1 – Organisations as Socio-Technical Constructed Systems
- 0.4 – Timeline of Business Organisations and Governance
- 0.5 – Corporate Collapses and the GRC Response
- 0.6 – Timeline of Public Services
- 0.7 – A Glimpse of the IT Ecosystem
- 0.13 – Legal Systems and Normative Layers
- 0.9 – Timeline of IT in Business and Governance of IT

Classification:

- **Cause**: Excessive reliance on vendor-specific cryptography, without resilient oversight
- **Consequence**: Mass revocation of digital identities; loss of public trust; global reputational scrutiny
- **Results**: Strengthened governance mechanisms; improved institutional and legal reflexes; reaffirmed commitment to digital public value

External Links:

- https://www.ft.com/content/874359dc-925b-11e7-a9e6-11d2f0ebb7f0
- https://www.zdnet.com/article/estonias-id-card-scrisis-how-e-states-poster-child-got-into-and-out-of-trouble/
- https://e-estonia.com/card-security-risk/
- https://en.wikipedia.org/wiki/Once-only_principle

3.3 Three persona did it…

weak…	*…medium…*	*…very good*
Q1.1 – Relation to "The Context"		
This story is about an organisation trying to innovate using cloud and data. It relates to the course because they did it in the public sector. The CEO wanted to show a new vision and got consultants to do that. But people inside didn't understand what was happening and it created conflict.	*This story shows a public institution that tried to become "cloud-first" but ignored its context, requirements for compliance, and its own organisational legacy.*	*The story shows how digital change in the public sector can fail when institutional memory and stakeholder dynamics are ignored. It relates to the idea that organisations are shaped not just by their current goals but by their internal history, culture, and legal structure.*
Q1.2 – Lessons		
We can learn that change is not easy, and even good technology can fail if it is not properly introduced or people don't accept it. It's also important to plan better and make sure workers are not surprised.	*One lesson is that having a **<113> Management System** helps ensure changes are managed in an integrated and transparent way. Another is that real transformation requires **<207> Stakeholder Engagement**, not just hiring consultants and making announcements.*	*A lesson is that robust **<113> Management Systems** are essential for ensuring transparency, fallback plans, and coherence across governance levels. Other lesson is that change must consider **<219> Governance and Organisational Culture**, especially in public sector settings. A third, often missed, is that without **<124> Strategic Alignment**, cloud adoption becomes a superficial rebranding, not a systemic improvement.*
Q1.3 – Concept Map		
Shows effort but misuses the idea of "lessons" by staying vague ("change is not easy") and without connecting to deeper institutional causes. No relevant glossary concepts are used, and no cause-effect relationships or actor roles are established in the map. The answer lacks structural interpretation of how governance or systems work (what the theme is about…).	At least two valid glossary concepts (<113>, <207>) and a reasonable interpretation. The map includes terms like "resistance," "consultants," and "cloud," with some cause-effect arrows (e.g., "lack of engagement → internal conflict"), but is light in structure and doesn't reflect broader concepts like institutional trust or strategic alignment. A solid attempt, but not yet mature or integrative.	**Glossary Coverage**: Accurately applies multiple glossary concepts (<113>, <219>, <124>, <207>, <105>) with clear thematic relevance. **Map Logic**: Consultants lacked <124> → misfit with public mission. No <207> → internal backlash. Absent <113> → no governance fallback → CEO exit. lack of <207> → cultural resistance → failure of <124>; absence of <113> → no accountability structure → political fallout. **Structure and Flow**: Uses organisational actors (e.g., consultants, CEO, internal staff) as nodes; defines relationships as directional outcomes. **Theme 0 Awareness**: Understands the *contextual foundation* of institutional change, that systems are not just technical, but also political and cultural constructs.
Q2.1 – Relation to "The Context"		
This case is about Estonia, a very advanced country in technology. They had a problem with their digital ID cards. This is related to the course because it shows what happens when something digital breaks in government.	Estonia's case fits the theme because it shows how digital identity is not only a technical issue, but also a public and legal responsibility. It reveals that even in advanced digital states, systems can fail if there is too much trust in vendors and not enough risk planning.	Estonia's ID crisis exposed the risks of outsourcing trust and the need of robust institutional safeguards.
Q2.2 – Lessons		
One lesson is that even countries with good technology can have problems. Another lesson is that they reacted quickly, so that shows leadership is important in digital things.	One lesson is the need for strong **<210> Vendor and Contract Management** (the cryptographic issue came from an external supplier). Another is that **<216> Information Security** must be built into public trust frameworks, not just technical design.	**<216> Information Security** must be embedded not just in technical protocols, but in institutional mechanisms for accountability and resilience. **<213> Legal and Regulatory Compliance** must address cross-border dependency risks (Estonia used Dutch cryptographic libraries without equivalent domestic oversight). **<105> Risk Orientation** must be continuously updated in digital governance, especially for public infrastructure with critical citizen dependency.

Q2.3 – Concept Map		
The cmap stays at surface level. “Leadership” is discussed abstractly, and there’s no understanding of legal or institutional dependencies. The cmap fails to use glossary concepts such as <216> (Information Security) or <210> (Vendor and Contract Management), and no structural analysis of causes or institutional response is mapped.	Good use of <210> and <216>, and partially structured map that includes “vendor risk → identity crisis” and “gov response → partial trust recovery.” The logic is present but remains siloed (the cmap is more a three than a web). No clear integration with broader governance ideas (e.g., <219>, <213>) or historical reflection. Feels like a Theme 2 answer repurposed for Theme 0 (not wrong, but… a sign of potential cross-theme confusion).	**Glossary Concepts Used**: <216>, <213>, <210>, <105>, <219> **Structural Mapping**: Vendor flaw (<210>) → trust breach. Inadequate <105> → no early mitigation. Strong <219> culture allowed recovery. Delegated trust to vendor (<210>) → flaw discovered → <216> exposed Missing anticipatory <105> → no early mitigation path | <213> failed to reflect real transnational exposure → emergency regulatory intervention | <219> shows institutional reflex: transparent state response → partial trust repair The map reflects maturity by showing both the breakdown and the recovery trajectory, using concept-rich vocabulary. It demonstrates understanding of foundations: *systems are contextual, historical, and socio-political* (not just digital).
Q3.1 + Q3.2 – Seminar Discussion		
Why is digital transformation sometimes difficult?	*Can legacy systems and institutional culture stop organisations from achieving digital transformation?*	*How can ignoring institutional memory, legal frameworks, or stakeholder legitimacy undermine digital transformation in public organisations and public services?*
Because many organisations find it hard to change. It’s important to talk about this in class so we understand the problems.	*This is relevant because both the story and the case showed that past systems and decisions shape how new things can be done. In public organisations, culture and trust also seem very important, and not everyone sees change the same way. This question could help the class reflect on how much of the past we should keep when planning the future.*	*This reflects core ideas. It links directly to failures in both the story and the case and encourages debate on how context shapes governance. Concepts like <219> and <124> are central.*
The question is not wrong but is vague and too general to guide structured debate. The justification doesn’t refer to any concept or dynamic from the course (e.g., governance, institutional memory, public legitimacy). No clear link to the theme or to organisational context as a structuring constraint.	Solid question that invites discussion, though not highly original. Reasonable justification showing awareness of the course’s focus on organizations and context. Would benefit from explicitly naming glossary concepts or referring to governance, stakeholders, or socio-technical dynamics.	The question is precise, multidimensional, and anchored in course concepts. The justification shows excellent understanding of the theme and integrates glossary concepts insightfully. Encourages debate and cross-sector comparison. Demonstrates strong critical thinking.