Information Systems Management and Security

Essays

Version: V01

Contents

1 Assignment: Thematic Essays

For each of Essays 1 to 4, each student must submit a report following the requirements and guidelines below.

- **Textual answers** must be submitted via the *Google Form* provided in *Fenix* for each deliverable. Note that the character limits for each item (including spaces and punctuation) must be respected.
- **Concept maps, which must be easily readable and clearly structured,** must be submitted as a PDF file uploaded to *Fenix*. The file must be named with the student's number only, and contain a single A3-sized page, in vertical orientation. The page in this PDSF file must include, at the top, the student's number and name, followed by:
  - the concept map for **Q1.3**
  - and then the concept map for **Q2.3**.

1.1 What to deliver (always consider the perspective of the theme)

- **Q1 – Story Analysis:** Select one story from the *Stories Collection* and analyse it.
  - **Q1.1** (15%) How is the story related to the theme? *(Max 400 characters)*
  - **Q1.2** (15%) What lessons can be drawn from the story? *(Max 400 characters)*
  - **Q1.3** (15%) Create a concept map illustrating the story analysis, supporting your answers above.
- **Q2 – Case Analysis:** Select one (see the descriptions and other elements in the Lecture Notes):
  1. Maersk and the Quiet Catastrophe
  2. Colonial Pipeline and the Long Weekend
  3. ING and the Agile Transformation
  4. OpenAI and the Boardroom Shockwave
  5. The NHS Email Storm
  6. The SEF Migration Debacle
  7. Germany's E-ID Infrastructure Confusion
  8. France's Health Data Hub Delay
  9. Sonos App Overhaul Fallout
  - **Q2.1** (15%) How is the case related to the theme? *(Max 400 characters)*
  - **Q2.2** (15%) What lessons can be drawn from the case? *(Max 400 characters)*
  - **Q2.3** (15%) Create a concept map illustrating the case analysis, supporting your answers above.
- **Q3 – Seminar Discussion Prompt:**
  - **Q3.1** (5%) Propose a discussion question related to the theme for use in the seminar. *(Max 100 characters)*
  - **Q3.2** (5%) Justify the relevance of the proposed issue from the perspective of the theme. *(Max 400 characters)*
- **Qx – Use of Tools:** We assume students may use generative language services to support their essays, or any other relevant aids (e.g. software, peer support, coaching). Describe what had you used and your experience with that.

1.2 NOTES:

- For each essay, choose a story and a case that clearly relate to the theme (reusing the same story or case across themes is not permitted).
- Learn about concept maps: https://cmap.ihmc.us/
- Be aware that a good map:
  - Is clear, structured, and connects concepts with accurate links that form valid assertions.
  - Should centre around at least one main concept and ideally show a rich web of ideas, not just a tree.
  - Use colour, shapes, and layout to support reading and emphasis.
  - Use a maximum of 12 concepts
  - Use concepts from the reference list whenever possible:
    - Must use core course terminology with correct identifiers of the terms form the reference glossary (e.g., <id> concept-name).
    - New concepts must be clearly defined in the first related answer.

1.3 Grading reference

Score	Relation to Theme (Qx.1)	Lessons (Qx.2)	Concept Map (Qx.3)
0	Off-topic or missing	No lessons, irrelevant	Not submitted or nonsense
1	One vague mention; no justification	One idea, no course link	Minimal map, incoherent or unclear
2	Two weak points, superficial	Two issues, unclear structure	Few elements, weak structure
3	One governance + one management concept, partial terminology	Two relevant risks/practices, moderate clarity	Mostly correct; lacks depth
4	Clear distinction of issues; good terminology	Two well-explained issues with references	Structured and coherent; clear actor-responsibility links
5	Excellent use of concepts (and identifiers), insightful framing	Strong analysis with frameworks, terminology, and context	Conceptually rich and visually clear; demonstrates synthesis

2 Stories Collection

2.1 Story: ArcoMed cloud-first

ArcoMed is a regional public health provider in southern Europe, managing several hospitals and health centres. Two years ago, its leadership embraced a cloud-first strategy, aligned with national digital health ambitions. The CIO, politically well-connected, secured fast-track approval to migrate critical systems — including electronic health records and imaging platforms — to an external vendor's cloud infrastructure.

The project was applauded as visionary, but governance was shallow. No Data Protection Impact Assessment (DPIA) was performed, and procurement decisions bypassed formal consultation with clinical or operational leads. Internal staff described the initiative as "done to us, not with us." Though the system initially improved access and reporting, responsibility for local resilience was unclear — internal IT believed the vendor handled backup; the vendor insisted local fallback was ArcoMed's job.

Then came the crisis: a targeted cyberattack disrupted the vendor's cloud platform. For over 36 hours, all clinical systems were inaccessible. Staff had to scramble to find incomplete paper backups. Elective surgeries were cancelled. News outlets framed it as a digital governance failure.

The CIO publicly blamed the vendor, citing the service-level agreement (SLA). The vendor countered that key risk mitigation steps — including local restoration mechanisms — were never implemented by ArcoMed's internal IT. The Chief Medical Officer, blindsided by the extent of the disruption, criticised the lack of shared planning. Union representatives called the episode "a consequence of managerial opacity."

Now, the Board has requested an independent review of governance maturity, project accountability, and the internal management system that allowed such blind spots. Political pressure is mounting for increased transparency and for clearer roles in digital transformation oversight.

2.2 Story: ArcoMed cloud migration

ArcoMed, a regional public health provider, launched a flagship cloud migration initiative, moving its electronic health records and imaging systems to an external provider's cloud platform. The project, led by the CIO and supported by national digital health agendas, aimed at rapid innovation and increased efficiency.

However, the initiative lacked a structured governance of IT framework. No DPIA (Data Protection Impact Assessment) was performed. Strategic oversight of IT risk, vendor accountability, and fallback mechanisms remained unclear. While the CIO held operational power, no decision-rights matrix or formal alignment mechanisms ensured coherence between business governance and IT governance structures.

When a cyberattack disabled the cloud infrastructure, clinical operations collapsed for over 36 hours. Internal IT teams lacked fallback access, and vendors denied responsibility for local recovery. Clinical leadership had not been involved in the planning or testing of resilience protocols.

After the event, a governance review revealed a weak separation of strategic and operational concerns, absence of formal role mapping (e.g., no RACI structure), and immaturity in the institution's governance of IT posture. The Board and the regional health authority now face scrutiny for not ensuring the CIO's initiatives were framed within robust, institution-wide IT governance practices — including vendor risk management, system criticality mapping, and compliance traceability.

2.3 Story: ArcoMed ransomware

ArcoMed, a regional public health provider, had transitioned key hospital systems — including electronic records and imaging services — to a third-party cloud platform. The shift promised agility and lower maintenance, but internal IT operations were insufficiently restructured to cope with the new architecture.

Operational readiness was minimal: local backups were outdated, service restoration protocols were undocumented, and disaster recovery procedures were never tested. Monitoring and alerting tools were fragmented. No incident response playbook linked operational roles across clinical and IT teams.

When the cloud vendor suffered a ransomware attack, all services were lost for over 36 hours. Staff attempted to recover from scattered, incomplete backups. Elective surgeries were postponed. Communications between IT operations and hospital units broke down.

The vendor pointed to standard SLA clauses and disclaimed responsibility for local contingency measures. Internal IT staff, caught between unclear escalation paths and absent fallback infrastructure, were unprepared to mitigate the crisis.

Post-crisis audits exposed serious flaws in ArcoMed's IT service management (ITSM) practices: no change management log, outdated configuration documentation, and no formalised operational risk registry. Leadership demanded a complete overhaul of IT operations, including adoption of incident management frameworks (e.g., ITIL), and sector-appropriate resilience protocols.

2.4 Story: VisioRetail AI Misfire

When the CEO of **VisioRetail**, a mid-sized European chain of home goods stores, declared that the company would become "AI-driven by design," it caught the attention of both the press and investors. The announcement followed a costly pandemic-era dip in performance and was part of a turnaround strategy led by an ambitious CTO, Carolina Riva, recently poached from a Silicon Valley startup.

Carolina had strong technical credentials and a bold plan: to integrate machine learning models for demand forecasting, optimise supply chain logistics, and implement a generative AI-powered chatbot to replace most human customer service. She insisted on agile implementation and hired a boutique AI consultancy with no retail background but a flashy demo. The CIO, an internal veteran named Nuno Esteves, raised concerns about legacy system compatibility, but was sidelined early in the project.

One year in, results were mixed. The chatbot struggled with multilingual support and failed to handle refunds correctly. The AI forecasts ignored weather effects and local holidays, resulting in bizarre stock allocations. Warehouse efficiency actually declined due to over-reliance on automated triggers that bypassed human intuition.

Meanwhile, staff morale plummeted. Shop floor workers felt alienated by the rapid changes, and regional managers complained of being turned into "button-pushers." Customers began posting stories online about poor service and surreal AI replies. By the time the board demanded an internal audit, it was clear the transformation had prioritised technological ambition over operational alignment and stakeholder engagement.

In the post-mortem, it became evident that no strategic portfolio review had been conducted. There was no Target Operating Model (TOM), no alignment between IT capabilities and business processes, and no stakeholder mapping. The CTO resigned. The CIO was called back in to lead a more inclusive, phased realignment effort—starting with defining what "AI-driven" should mean in a retail business context.

2.5 Story: VisioRetail CEO Shuffle

VisioRetail, a fast-expanding home and lifestyle retail chain in Southern Europe, was known for its daring digital bets. But beneath the shiny innovation, board-level tensions were simmering.

The previous CEO, Raul Andrade, had led the company through aggressive expansion, heavily investing in automation and predictive analytics. While this earned media praise, internal governance was weak. Raul maintained tight executive control and bypassed traditional reporting channels, relying instead on a small "strategy cell" reporting directly to him. The board, impressed by growth numbers, remained passive.

In Q2 2024, sales plummeted in several regions, and a whistleblower flagged undisclosed losses due to mismanaged stock and overpromised supplier contracts. As pressure mounted, the board forced Raul to resign and appointed an interim CEO, Sofia Matos, previously Head of Compliance. Her mandate: restore governance maturity and rebuild internal trust.

Sofia quickly discovered the absence of a functioning management system: KPIs were inconsistent across departments, risk registers were outdated, and accountability was blurred. There was no audit trail on critical IT contracts. While the CIO had been technically competent, he had no board-level access and had been routinely sidelined from strategic discussions. The HR director had resigned a year earlier, citing "values drift."

Sofia restructured the executive team and initiated a governance review based on the ISO 37301 framework. She invited staff into stakeholder sessions and brought in an external auditor to rebuild control functions. The board, now more aware of its oversight role, established a formal risk committee and mandated annual reviews of the management system.

As the company entered its next strategic cycle, Sofia raised an internal discussion: was VisioRetail's culture too enamoured with charismatic leadership? And could sustainable governance take root in an organisation built on speed and intuition?

2.6 Story: MetroWater Access Denied

MetroWater is a large public utility responsible for water distribution and wastewater management in a densely populated metropolitan region. As part of a national push for smart infrastructure, MetroWater launched an ambitious programme to digitise field operations, introduce predictive maintenance, and consolidate SCADA (Supervisory Control and Data Acquisition) systems into a unified cloud-enabled platform.

The CIO championed the effort, outsourcing both the systems integration and platform management to a multinational vendor. The contract was signed under pressure to comply with tight national funding deadlines, and key technical staff were excluded from final design reviews.

Soon after deployment, technicians began reporting erratic remote access to pump stations. Field operators could no longer override sensors on-site when cloud access failed. A routine firmware update caused a cascading failure that blocked control of three major stations for 12 hours. Water pressure dropped city-wide. Emergency protocols had to be triggered manually by staff unfamiliar with the digital failover procedures.

An internal review exposed systemic gaps: no operational continuity testing, unclear responsibilities for patch approval, and lack of alignment between MetroWater's risk management framework and the vendor's change control process. Documentation was fragmented across systems. The CIO insisted the vendor was responsible, while the vendor pointed to MetroWater's lack of role definitions and fallback plans.

Under scrutiny from the municipal oversight committee, MetroWater admitted there was no IT governance model linking critical infrastructure oversight with vendor service levels. There were also no metrics in place to track resilience or recovery capacity. A whistleblower claimed internal warnings had been ignored because "governance was treated as a compliance checkbox, not an operational necessity."

2.7 Story: MetroWater Leap Too Far

MetroWater, a large urban utility responsible for water and wastewater services, faced increasing political pressure to modernise its image and services. In response, the new CEO launched a high-profile strategic transformation programme titled *"MetroWater 4.0"*, aiming to position the organisation as a smart utility leader through automation, digital customer engagement, and AI-based consumption analytics.

The initiative was led by a freshly appointed Chief Strategy Officer, who came from the energy sector. The CIO and the Operations Director were only consulted at the implementation stage. No enterprise architecture modelling or Target Operating Model was developed. Business process owners were instructed to adopt pre-packaged "innovation accelerators" offered by the vendor without adaptation.

Internally, employees struggled to understand how their work fit the new tools. Billing support agents were suddenly asked to interpret machine-generated risk scores. Customer complaints surged when billing algorithms applied penalties based on faulty assumptions. Union representatives protested the speed of automation and accused leadership of "consultant-led chaos."

The board was unaware that the transformation lacked integrated KPIs or formal strategic portfolio governance. The CEO had delegated decision-making to the CSO, who focused on short-term deliverables over cross-departmental coordination. When the first quarterly review showed reputational damage and cost overruns, a governance crisis emerged.

An internal audit found the management system was not updated to reflect the transformation programme. Department heads reported "vision without structure." The CIO later noted that digital ambitions had outpaced both operational capacity and managerial clarity, with no coherent roadmap to ensure long-term alignment.

2.8 Story: BeaconLab Algorithmic Secret

BeaconLab is a private biotech start-up owned by John José and known for rapid development of diagnostic software using machine learning. In 2024, it launched an internal challenge to compress DNA sequence analysis into a mobile application that could deliver results in under 10 seconds. A team of junior data scientists announced that they had succeeded by creating a new custom algorithm optimised for GPU acceleration.

The app was celebrated internally and posted as a preprint on a public research server. However, a few weeks later, John José discovered that the algorithm violated a clause in a third-party academic code licence. The developers' team had copy-pasted parts of the original algorithm without proper attribution, believing that code snippets published in public forums were "community-owned."

BeaconLab apologised and voluntarily took the app offline. A disciplinary review led to temporary suspension of two developers. John José issued a statement reaffirming the company's commitment to scientific ethics.

Following the incident, BeaconLab adopted a mandatory open-source compliance checklist for developers and hired a legal advisor. The company resumed operations, and the preprint was withdrawn. Some of the affected researchers later joined a university spin-off.

2.9 Story: BeaconLab Growth Pains

BeaconLab, a rapidly scaling biotech company, earned global attention for its AI-based diagnostics and mobile DNA testing platform. Flush with investor funding, the leadership launched a growth initiative to accelerate time-to-market for new algorithmic services by shifting from research-based software governance to an industrial-grade cloud architecture.

The CTO partnered with a digital consultancy to implement a new cloud-native analytics pipeline but skipped formal architectural reviews to maintain momentum. Internal documentation was scattered, and developer teams were left to self-organise code management using public repositories. An internal DevOps team raised concerns about lack of secure API governance and licensing controls, but their feedback was not escalated.

A month before launch, BeaconLab received a legal notice from a university claiming their core sequence compression engine violated terms of a research licence. An audit confirmed that one of the algorithm components had been used without proper integration review or reuse authorisation. The CTO had assumed the open code fell under "fair experimental reuse," but no due diligence process was in place.

To contain reputational fallout, the product launch was delayed. The CEO initiated a strategic realignment, mandating governance for code reuse and open-source dependencies. A new Enterprise Architecture team was created to oversee component integration, and a board-level risk committee was formed to align research agility with commercial compliance requirements.

BeaconLab now applies a dual-track innovation framework: one focused on exploratory research, and another governed by structured production and risk management processes. Developers attend onboarding sessions on IP risk, and all product modules undergo alignment review between IT, legal, and business units.

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.