

Real-World Cases

Following is a list of real-world cases related to the concepts addressed in these notes. Each case includes a short description, references to relevant lecture note items, and a classification by cause, consequence, and result. These examples serve as learning tools to illustrate how decisions, failures, and successes influence the governance and evolution of digital systems in both public and private organisations.

<1> Maersk and the Quiet Catastrophe

Description: A.P. Møller–Maersk, the world's largest shipping and logistics company, suffered a massive operational shutdown in 2017 due to the NotPetya malware. Originating from a tax software update in Ukraine, the attack spread rapidly across global systems, disabling terminals, bookings, and communications. Maersk's recovery relied on salvaging a domain controller from a remote office that had been offline during the attack. The incident exposed deep architectural coupling, limited segmentation, and dependency on informal recovery practices.

Relevant Lecture Note Items:

- 3.5 Technical Debt and System Evolution
- 3.13 Operational Resilience and Incident Response
- 2.25 IT Supply Chain
- 2.15 The Ecosystem of Cybersecurity

Classification:

- **Cause:** Architectural fragility and lack of segmentation
- **Consequence:** Global service disruption across business units
- **Result:** Operational loss (~\$300M), reputational questions, improved cyber architecture

Sources:

- <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>
- <https://softwarelab.org/blog/notpetya/>
- <https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue>

<2> Colonial Pipeline and the Long Weekend (2021)

Description: In May 2021, Colonial Pipeline shut down fuel distribution after a ransomware attack on its IT systems, even though OT systems were not directly compromised. The lack of visibility into the breach's full impact, along with poor coordination between IT and OT, led to a service halt affecting the U.S. East Coast. The company paid a \$4.4 million ransom, partially recovered by authorities. The event demonstrated how digital risks can cascade into critical physical infrastructure.

Relevant Lecture Note Items:

- 3.13 Operational Resilience and Incident Response
- 2.6 Operational Technology and the IT/OT Interface
- 2.25 IT Supply Chain
- 2.15.2 National Authorities and Coordination
- 2.29.4 Strategic Relevance and Governance Maturity

Classification:

- **Cause:** Ransomware attack + poor IT/OT integration
- **Consequence:** Pre-emptive operational shutdown and fuel shortages
- **Result:** Economic disruption, federal policy reaction, cyber regulation update

Sources:

- <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>
- <https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html>
- <https://www.bbc.com/news/business-57050690>
- <https://ransomware.org/blog/one-year-later-lessons-from-colonial-pipeline/>

<3> ING agile transformation (2015)

Description: ING restructured its organisational model to adopt agile practices across banking functions, dismantling traditional hierarchies in favour of autonomous squads and tribes. While initially disruptive, it became a benchmark for digital transformation, despite early concerns from regulators.

Relevant Concepts:

- 1.1 Governance, Management, and Operations
- 4.1 Business and Strategy

Classification: Intended cause, Good consequence, Positive results

Sources:

- <https://www.mckinsey.com/industries/financial-services/our-insights/ings-agile-transformation>
- <https://www.ing.com/Newsroom/News/Squads-sprints-and-stand-ups.htm>

<4> OpenAI and the Boardroom Shockwave (2023)

Description: In November 2023, OpenAI's board suddenly fired CEO Sam Altman without consulting key stakeholders. The lack of transparency and stakeholder alignment provoked near-unanimous staff backlash, a public offer from Microsoft to hire the entire team, and the board's subsequent reversal. The event revealed governance fragility in hybrid non-profit/commercial structures and the strategic risk of board isolation from operational realities.

Relevant Lecture Note Items:

- 1.21 Board Dynamics and Governance Structures
- 1.25 CxO Roles in Governance and Strategic Engagement
- 4.26 CxO Dilemmas
- 4.3 Stakeholder Engagement and Strategic Communication

Classification:

- **Cause:** Governance misalignment and opaque board decision-making
- **Consequence:** Organisational crisis and mass resignation threats
- **Result:** Board restructuring, Altman reinstated, stakeholder trust questioned

Sources:

- https://en.wikipedia.org/wiki/Removal_of_Sam_Altman_from_OpenAI
- <https://medium.com/aicorporateedge/openais-boardroom-bombshell-unveiling-the-radical-shake-up-and-the-secret-players-behind-it-1e4a133fed5e>
- <https://boardshape.com/blog/when-boards-clash-with-visionaries-sam-altman-saga>

<5> NHS email storm (2016)

Description: An accidental mass email sent to NHS staff caused disruption across the UK health service. Despite initial confusion, the event prompted improved controls and digital hygiene measures.

Relevant Concepts:

- 1.2 Management and Maturity
- 2.1 Governance of IT

Classification: Unintended cause, Bad consequence, Positive results

Sources:

- <https://www.bbc.com/news/technology-37979456>
- <https://arstechnica.com/information-technology/2016/11/nhs-email-storm-distribution-list-blunder/>

<6> SEF migration debacle (2023)

Description: The poorly planned restructuring of Portugal's border agency SEF led to service failures, system outages, and a public backlash. Unclear role distribution and weak stakeholder coordination contributed to the disruption.

Relevant Concepts:

- 1.1 Governance, Management, and Operations
- 1.2 Management and Maturity

Classification: Intended cause, Bad consequence, Negative results

Sources (Portuguese):

- <https://cnnportugal.iol.pt/sef/problemas/problemas-informaticos-deixam-sef-lento-e-ate-parado-numero-de-processos-pendentes-nao-para-de-aumentar/20231003/65142e31d34e65afa2f5c77a>
- <https://observador.pt/2024/02/05/falta-de-acesso-as-bases-de-dados-do-sef-nao-compromete-investigacao-da-pj-diz-seguranca-interna/>
- https://www.rtp.pt/noticias/pais/falta-de-acesso-as-bases-de-dados-do-sef-nao-compromete-investigacao-da-pj-garante-seguranca-interna_a1548639

<7> Germany's E-ID project

Description: Germany's digital ID initiative faced low adoption and public criticism due to inter-agency misalignment, low trust, and limited usability, despite its ambitious goals.

Relevant Concepts:

- 1.2 Management and Maturity
- 2.1 Governance of IT

Classification: Intended cause, Bad consequence, Negative results

Sources:

- <https://www.signicat.com/blog/digital-identity-in-germany-market-status-trends-and-regulations-that-you-need-to-consider>
- https://link.springer.com/chapter/10.1007/978-3-031-45648-0_29

<8> France health data hub realignment (2018...)

Description: Facing backlash over storing health data on US cloud infrastructure, France restructured its Health Data Hub to use a European provider, rebuilding trust and compliance posture.

Relevant Concepts:

- 1.1 Governance, Management, and Operations
- 2.1 Governance of IT
- 4.3 Strategic Portfolio and Investment Governance

Classification: Intended cause, Good consequence, Positive results

Sources:

- <https://implicity.com/everything-you-need-to-know-about-health-data-hub/>
- <https://openfuture.eu/note/the-french-data-protection-authority-reluctantly-greenlights-the-health-data-hubs-hosting-by-microsoft>
- https://gdprhub.eu/index.php?title=CE - N%C2%BO_444937
- <https://www.euractiv.com/section/health-consumers/news/french-decision-to-have-microsoft-host-health-data-hub-still-attracts-criticism/>
- <https://azure.microsoft.com/es-es/blog/microsoft-azure-is-now-certified-to-host-sensitive-health-data-in-france/>
- <https://learn.microsoft.com/en-us/compliance/regulatory/offering-hds-france>

<9> Sonos App Overhaul Fallout (2024...)

Description: In 2024, Sonos released a major redesign of its mobile app that removed features, broke support for older devices, and degraded user experience. Loyal customers voiced frustration through negative reviews and social media backlash. Sonos was slow to respond, undermining trust. The case illustrates the risk of digital product changes without sufficient transition strategy or user engagement.

• Relevant Lecture Note Items:

- 4.3 Stakeholder Engagement and Strategic Communication
- 4.6 Enterprise Architecture and Alignment
- 4.5 Target Operating Model
- 3.5 Technical Debt and System Evolution

• Classification:

- **Cause:** Abrupt digital product redesign without stakeholder alignment
- **Consequence:** Feature loss, brand damage, and customer backlash
- **Result:** Negative publicity, user trust erosion, delayed roadmap revisions

• Sources:

- <https://www.theverge.com/2025/1/13/24342282/sonos-app-redesign-controversy-full-story>
- <https://edition.cnn.com/2025/02/08/tech/sonos-app-update-redemption-2025/index.html>
- <https://www.wsj.com/articles/sonos-marketing-chief-exits-as-fallout-from-app-calamity-continues-422ff362>

<10> Harley-Davidson boardroom eruption (2025)

Description: Governance weaknesses led to a leadership crisis during CEO succession at Harley-Davidson, exposing gaps in board oversight and strategic alignment, and resulting in reputational and strategic setbacks.

Relevant Concepts:

- 1.1 Governance, Management, and Operations
- 1.3 CxO Roles in Governance and Strategic Engagement

Classification: Intended cause, Bad consequence, Negative results

Sources:

- https://www.wsj.com/business/inside-the-boardroom-eruption-harley-davidson-future-ceo-search-proxy-battle-e740b646?mod=wknd_pos1
- <https://eu.jsonline.com/story/money/business/2025/04/17/harley-davidson-corporate-drama-the-players-impact-on-customers/83127406007/>

<11> Amazon Web Services (AWS) outages (2021)

Description: Several high-profile outages of Amazon Web Services disrupted global digital services, affecting major platforms across finance, media, logistics, and healthcare. These incidents raised awareness of over-reliance on single-cloud vendors and prompted widespread adoption of multi-cloud and hybrid strategies to improve resilience.

Relevant Concepts:

- 3.1 IT Services and Operations
- 3.2 Resilience and Incident Response
- 4.3 Strategic Portfolio and Investment Governance

Classification: Unintended cause, Bad consequence, Positive results

Sources:

- <https://devdosvid.blog/2024/06/03/unpacking-aws-outages-system-design-lessons-from-post-event-summaries/>
- <https://aws.amazon.com/message/12721/>
- <https://aws.amazon.com/premiumsupport/technology/pes/>
- <https://health.aws.amazon.com/health/status>

<12> Boeing and the 737 MAX crisis (2018...)

Description: Two fatal crashes involving Boeing 737 MAX aircraft revealed failures in software design, risk disclosure, and regulatory coordination. Investigations uncovered governance breakdowns, prioritisation of financial goals over safety, and suppression of internal warnings, leading to massive reputational damage and executive accountability reforms.

Relevant Concepts:

- 1.5 Governance, Risk and Compliance
- 1.10 Control: The Three Lines of Defence
- 1.25 CxO Roles in Governance and Strategic Engagement

Classification: Intended cause, Bad consequence, Negative results

Sources:

- https://en.wikipedia.org/wiki/Boeing_737_MAX_groundings
- <https://corpgov.law.harvard.edu/2024/06/06/boeing-737-max/>
- <https://apnews.com/article/boeing-plea-737-max-crashes-b34daa014406657e720bec4a990dccf6>
- <https://www.aviacionline.com/boeing-the-737-max-and-the-avoided-screw-crisis>
- <https://www.politico.eu/article/boeing-crisis-everybody-freaking-out-faa-easa-alaska-door-plug-737-max9/>

<13> Estonia's digital government ecosystem (2001...)

Description: Estonia developed a comprehensive digital government ecosystem with strong interoperability and user-centric services. Based on X-Road architecture and digital identity infrastructure, the country became a global reference for secure, integrated public services supported by proactive legal and governance frameworks.

Relevant Concepts:

- 4.1 Business and Strategy
- 4.2 Enterprise Architecture and Alignment
- 4.21 Identity Management

Classification: Intended cause, Good consequence, Positive results

Sources:

- <https://e-estonia.com/solutions/interoperability-services/x-road/>
- <https://complexdiscovery.com/estonias-digital-strategy-shines-in-the-2024-un-e-government-report/>
- <https://thedocs.worldbank.org/en/doc/165711456838073531-0050022016/original/WDR16BPEstonianeGovecosystemVassil.pdf>

<14> Facebook / Cambridge Analytica scandal (2018)

Description: Facebook allowed personal data of millions of users to be harvested without consent and exploited by Cambridge Analytica for political profiling. The case triggered global scrutiny of digital platform governance, data protection compliance, and algorithmic accountability.

Relevant Concepts:

- 2.11 Information Privacy
- 2.13 Consent Mechanisms
- 4.22 Governance of Algorithmic Systems

Classification: Unintended cause, Bad consequence, Negative results

Sources:

- https://en.wikipedia.org/wiki/Facebook%20Cambridge_Analytica_data_scandal
- <https://www.bbc.com/news/technology-54722362>

<15> GitLab backup deletion and live recovery (2017)

Description: A GitLab administrator accidentally deleted a production database, and all backup mechanisms failed — except a snapshot saved on a developer laptop. The recovery was livestreamed and transparently documented, earning praise for crisis communication and triggering long-term infrastructure improvements.

Relevant Concepts:

- 3.2 Resilience and Incident Response
- 3.10 Operational Culture and Organisational Maturity
- 3.12 Service Management Frameworks

Classification: Unintended cause, Bad consequence, Positive results

Sources:

- <https://about.gitlab.com/blog/2017/02/01/gitlab-dot-com-database-incident/>
- <https://lup.lub.lu.se/luur/download?func=downloadFile&recordId=8970730&fileId=8970734>

<16> Hawaii emergency alert: UI mistake, systemic failure (2018)

Description: A false missile alert was sent to Hawaii residents due to a poorly designed user interface and lack of process checks. The alert took 38 minutes to be retracted. The incident illustrated how human error, combined with UI flaws and inadequate governance, can cause mass panic.

Relevant Concepts:

- 3.2 IT Services and Operations
- 3.13 Operational Resilience and Incident Response
- 1.5 Governance, Risk and Compliance

Classification: Unintended cause, Bad consequence, Negative results

Sources:

- https://en.wikipedia.org/wiki/2018_Hawaii_false_missile_alert
- <https://www.nngroup.com/articles/error-prevention/>

<17> IKEA and the shift to unified digital platforms (2018...)

Description: IKEA consolidated fragmented systems into a unified global digital platform to support ecommerce and supply chain visibility. The transformation was grounded in strong enterprise architecture and gradual rollout. It enabled agility during the pandemic and positioned the company for omnichannel growth.

Relevant Concepts:

- 4.1 Business and Strategy
- 4.6 Enterprise Architecture and Alignment
- 4.8 Strategic Portfolio and Investment Governance

Classification: Intended cause, Good consequence, Positive results

Sources:

- <https://www.theagilityeffect.com/en/case/how-ikea-is-stepping-up-its-digital-transformation/>
- <https://www.thehrdigest.com/ikeas-digital-transformation-how-the-swedish-furniture-giant-is-adapting-to-the-new-retail-landscape/>

<18> Knight Capital: a \$440 million error in 45 minutes (2012)

Description: A faulty software deployment at Knight Capital caused unintended high-frequency trading activity, resulting in a \$440 million loss in under an hour. The case exposed the absence of change control, rollback procedures, and operational safeguards in mission-critical systems.

Relevant Concepts:

- 3.3 IT Operations
- 3.5 Resilience
- 3.12 Service Management Frameworks

Classification: Unintended cause, Bad consequence, Negative results

Sources:

- <https://www.henicodolfing.com/2019/06/project-failure-case-study-knight-capital.html> (great stuff this site!!!)
- <https://www.cio.com/article/286790/software-testing-lessons-learned-from-knight-capital-fiasco.html>

<19> Lidl and the SAP retail project failure

Description: Lidl invested heavily in a custom SAP-based retail management system to standardise operations across countries. After seven years and over €500 million, the project was cancelled due to poor architectural alignment, weak change management, and incompatibility with Lidl's existing decentralised processes.

Relevant Concepts:

- 4.6 Enterprise Architecture and Alignment
- 4.8 Strategic Portfolio and Investment Governance
- 4.25.4 Strategic Ambition Versus Organisational Capacity

Classification: Intended cause, Bad consequence, Negative results

Sources:

- <https://www.panorama-consulting.com/lidl-erp-failure/>
- <https://www.henicodolfing.com/2020/05/case-study-lidl-sap-debacle.html> (**great stuff this site!!!**)
- <https://www.humology.com/lidl-case-study>

<20> Log4Shell vulnerability (2021)

Description: A critical zero-day vulnerability in the widely used Log4j library allowed remote code execution, affecting systems worldwide. The incident revealed widespread dependency risks and prompted urgent patching efforts, stronger software bill-of-materials practices, and vendor accountability reforms.

Relevant Concepts:

- 2.16 Frameworks for Information Security and Risk Management
- 2.25 IT Supply-Chain
- 3.2 Resilience and Incident Response

Classification: Unintended cause, Bad consequence, Positive results

Sources:

- <https://en.wikipedia.org/wiki/Log4Shell>
- <https://www.nytimes.com/2021/12/20/technology/log4j-cybersecurity-vulnerability.html>

<21> OVH cloud data centre fire (2021)

Description: A fire in an OVHcloud data centre in Strasbourg caused service outages for thousands of European clients. The incident exposed weaknesses in disaster recovery and prompted new norms for data centre resilience, off-site backup practices, and transparency obligations in cloud infrastructure.

Relevant Concepts:

- 3.2 Resilience and Incident Response
- 3.10 Operational Culture and Organisational Maturity
- 2.1 Governance of IT

Classification: Unintended cause, Bad consequence, Positive results

Sources:

- https://www.theregister.com/2021/03/10/ovh_strasbourg_fire/
- <https://www.datacenterdynamics.com/en/analysis/ovhcloud-fire-france-data-center/>
- <https://www.datacenterdynamics.com/en/opinions/ovhclouds-data-center-fire-one-year-on-what-do-we-know/>

<22> SolarWinds supply chain attack (2020)

Description: Attackers compromised the software update system of SolarWinds, injecting malicious code that reached thousands of public and private sector clients. The case underscored the strategic risks of digital supply chains and the need for stronger detection, supplier vetting, and policy coordination.

Relevant Concepts:

- 2.25 IT Supply-Chain
- 2.17 Frameworks for InfoSec and Risk Management
- 2.29 International and National Governance of Cybersecurity

Classification: Unintended cause, Bad consequence, Positive results

Sources:

- <https://www.gao.gov/products/gao-22-104746>
- <https://www.csoonline.com/article/570191/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html>

<23> Spotify and the strategic use of cloud infrastructure

Description: Spotify transitioned from in-house data centres to Google Cloud, enabling rapid scaling, data analytics, and improved user experience. This strategic shift supported business agility but required careful management of vendor lock-in, data governance, and technical integration challenges.

Relevant Concepts:

- 4.1 Business and Strategy
- 4.2 Enterprise Architecture and Alignment
- 4.3 Strategic Portfolio and Investment Governance

Classification: Intended cause, Good consequence, Positive results

Sources:

- <https://cloud.google.com/customers/spotify>
- <https://engineering.spotify.com/2019/12/views-from-the-cloud-a-history-of-spotifys-journey-to-the-cloud-part-1-2/>
- <https://www.computerworld.com/article/1655983/how-spotify-migrated-everything-from-on-premise-to-google-cloud-platform.html>

<24> TSB Bank IT migration failure (UK)

Description: TSB's attempted migration to a new IT platform in 2018 led to major service outages, affecting millions of customers. The failure was linked to inadequate testing, overconfidence in vendor capabilities, and governance flaws. The case triggered fines, CEO resignation, and scrutiny of IT change management.

Relevant Concepts:

- 1.7 Governance, Management and Operations
- 3.3 Change Management
- 4.3 Strategic Portfolio and Investment Governance

Classification: Intended cause, Bad consequence, Negative results

Sources:

- <https://www.bankofengland.co.uk/news/2022/december/tsb-fined-for-operational-resilience-failings>
- <https://www.computerweekly.com/news/252528519/TSB-hit-with-huge-fine-after-IT-migration-disaster>
- <https://www.bbc.com/news/business-64036529>

<25> UK Post Office Horizon IT scandal

Description: The UK Post Office prosecuted hundreds of sub-postmasters based on faulty data from the Horizon IT system. The case exposed institutional failures in IT governance, accountability, and legal safeguards, leading to widespread public outcry, compensation claims, and a national inquiry.

Relevant Concepts:

- 2.1 Governance of IT
- 2.9 Information Security
- 4.22 Governance of Algorithmic Systems

Classification: Unintended cause, Bad consequence, Negative results

Sources:

- https://en.wikipedia.org/wiki/British_Post_Office_scandal
- <https://www.bbc.com/news/business-56718036>
- https://en.wikipedia.org/wiki/Mr_Bates_vs_The_Post_Office (the TV series)
- <https://www.postofficescandal.uk/> (the book)

<26> Uber and its toxic culture

Description: Uber's early leadership fostered a high-growth environment marked by toxic work culture, regulatory evasion, and poor internal controls. Whistleblower revelations led to reputational damage, executive turnover, and organisational reforms focusing on ethics, compliance, and governance.

Relevant Concepts:

- 1.19 Governance and Organisational Culture
- 1.25 CxO Roles in Governance and Strategic Engagement
- 4.1 Business and Strategy

Classification: Intended cause, Bad consequence, Negative results

Sources:

- <https://www.hrmagazine.co.uk/content/features/uber-s-toxic-corporate-culture-much-more-than-a-pr-problem>
- <https://observer.com/2017/06/fixing-a-toxic-culture-like-ubers-requires-more-than-just-a-new-ceo-business-ethics-sexism-harassment-leadership/>

<27> Volkswagen Dieselgate scandal

Description: Volkswagen installed software in diesel cars to cheat emissions tests, misleading regulators and customers. The scandal revealed a systemic failure of ethics, compliance, and internal control. It led to executive resignations, criminal charges, multibillion-dollar fines, and a global reputational crisis.

Relevant Concepts:

- 1.5 Governance, Risk and Compliance
- 1.18 Governance and Ethics
- 1.25 CxO Roles in Governance and Strategic Engagement

Classification: Intended cause, Bad consequence, Negative results

Sources:

- https://en.wikipedia.org/wiki/Volkswagen_emissions_scandal
- <https://www.bbc.com/news/business-34324772>

<28> Wirecard financial fraud

Description: Wirecard, a German fintech firm, admitted that €1.9 billion in assets were missing. The scandal exposed regulatory failures, weak audit oversight, and governance gaps. It led to the company's collapse, arrests of senior executives, and a reckoning for EU financial supervision.

Relevant Concepts:

- 1.5 Governance, Risk and Compliance
- 1.16 Management Assurance: Auditing
- 1.25 CxO Roles in Governance and Strategic Engagement

Classification: Intended cause, Bad consequence, Negative results

Sources:

- <https://www.ft.com/wirecard>
- https://en.wikipedia.org/wiki/Wirecard_scandal

<29> The Netherlands' Common Ground initiative (2024...)

Description: The Dutch government launched the Common Ground initiative to standardise municipal data handling and improve service interoperability. By separating data from applications and adopting modular architecture, it enhanced local autonomy and digital maturity across municipalities.

Relevant Concepts:

- 4.2 Enterprise Architecture and Alignment
- 4.1 Business and Strategy
- 4.3 Strategic Portfolio and Investment Governance

Classification: Intended cause, Good consequence, Positive results

Sources:

- <https://en.shift2.nl/visie-op-common-ground>
- <https://interoperable-europe.ec.europa.eu/collection/elise-european-location-interoperability-solutions-e-government/solution/eulf-blueprint/best-practice-79>
- <https://commonground.nl/> (in Dutch)

<30> Travelex ransomware and prolonged shutdown (2020)

Description: A ransomware attack forced Travelex to shut down global currency exchange operations for weeks. The incident exposed weak IT hygiene and lack of resilience. The company suffered reputational damage and financial losses, prompting stronger crisis management practices sector-wide.

Relevant Concepts:

- 3.2 Resilience and Incident Response
- 2.9 Information Security
- 2.17 Frameworks for InfoSec and Risk Management

Classification: Unintended cause, Bad consequence, Positive results

Sources:

- <https://www.bbc.com/news/business-51017852>
- <https://www.itgovernance.co.uk/blog/ransomware-victim-travelex-forced-into-administration>
- <https://www.onsecurity.io/blog/cyber-nightmares-what-went-wrong-with-travelex/>

<31> \$463M telemedicine fraud (2022)

Description: A large-scale fraud in the US involved telemedicine companies billing Medicare for unnecessary genetic tests. The case revealed oversight gaps in digital healthcare and regulatory frameworks. It undermined public trust and led to stricter controls on telehealth billing.

Relevant Concepts:

- 4.1 Business and Strategy
- 1.5 Governance, Risk and Compliance

Classification: Intended cause, Bad consequence, Negative results

Sources:

- <https://www.justice.gov/archives/opa/pr/lab-owner-convicted-463-million-genetic-testing-scheme-defraud-medicare>
- <https://healthexec.com/topics/healthcare-management/healthcare-policy/labsolutions-minal-patel-sentenced-medicare-fraud>
- <https://healthcarechief.com/genetic-testing-labs-in-463m-fraud-case/>

<32> Vastaamo and the Therapy Data Blackmail (2018)

Description: Between 2018 and 2019, Finnish psychotherapy provider Vastaamo suffered multiple data breaches due to serious failures in its IT and security governance. The attackers stole highly sensitive patient records, including therapy notes, and began blackmailing both the company and individual patients in 2020. It was later revealed that the breached database had been left exposed online for more than a year without password protection. Vastaamo's executive leadership failed to report the breach in a timely manner and neglected to implement even basic information security controls. The organisation ultimately went bankrupt, and its CEO faced criminal charges. The incident led to widespread public trauma, loss of trust in digital healthcare, and a national conversation on the governance of health data.

Relevant Lecture Notes Sections:

- 2.1 Governance of IT
- 2.2 Leadership Roles and Governance Posture
- 2.7 Stakeholder Management and Information Systems
- 2.8 Information Governance and Management
- 2.9 Information Security
- 2.11.2 Privacy by Design and Risk Orientation
- 2.12 General Data Protection Regulation
- 2.13.3 Consent Mechanisms
- 2.14 Personal Data
- 3.13 Operational Resilience and Incident Response

Classification:

- **Cause:** Inadequate IT governance and failure to apply basic information security practices.
- **Consequence:** Massive privacy violation, criminal extortion, psychological harm to patients.
- **Results:** Organisational collapse, legal prosecution, national policy scrutiny on health data governance.

Online Sources:

- https://en.wikipedia.org/wiki/Vastaamo_data_breach
- https://www.edpb.europa.eu/news/national-news/2022/administrative-fine-imposed-psychotherapy-centre-vastaamo-data-protection_en
- <https://www.bbc.com/news/articles/c97znd00q7mo>

<33> Portugal's Justice System Offline: The CITIUS Crash (2014)

Short: In September 2014, Portugal's Ministry of Justice deployed an updated version of CITIUS (the national platform used by judges and legal professionals for court case management) without adequate testing or fallback planning. The rollout coincided with the launch of a major judicial reorganisation that altered court structures and processes across the country. Within days, critical failures emerged: court staff could not access files, submit case updates, or process legal actions. The system remained unstable for weeks, causing thousands of delays and triggering nationwide protests from judges and court clerks. An internal investigation exposed poor coordination between the IT provider, the Directorate-General for Justice Policy, and frontline users. There had been no comprehensive system test, insufficient training, and no rollback strategy. Political fallout forced the resignation of the Justice Secretary, and the case became a symbol of digital misgovernance in public sector transformation.

Relevant Lecture Notes Sections:

- 2.1 Governance of IT
- 2.2 Leadership Roles and Governance Posture
- 2.5 Strategic Alignment
- 2.7 Stakeholder Management and Information Systems
- 2.9 Vendor and Contract Management
- 3.3 IT Operations
- 3.5 Resilience

- **3.10** Continuity and Recovery
- **4.6** Target Operating Model (TOM)
- **4.8** Strategic Portfolio and Investment Governance

Classification:

- **Cause:** Lack of IT governance, absence of integrated planning for simultaneous legal reform and system upgrade.
- **Consequence:** Nationwide system outage in the judiciary, operational paralysis, reputational damage to the Ministry of Justice.
- **Results:** Delays in court cases, national protest by justice workers, political accountability and resignation, overhaul of governance processes in digital justice programmes.

Online Sources (Portuguese):

- <https://www.publico.pt/2014/09/01/sociedade/noticia/site-citius-continua-indisponivel-no-arranque-do-mapa-judiciario-1668298>
- <https://tvi.iol.pt/noticias/sociedade/sindicato-funcionarios-judiciais-sobre-as-falhas-na-plataforma-informatica/citius-instituto-considera-abusivas-criticas>
- <https://expresso.pt/economia/2019-09-30-Auditoria-ao-colapso-do-Citius-classificada-como-confidencial-pela-IGF>
- <https://www.publico.pt/2018/03/30/sociedade/noticia/tres-anos-e-meio-apos-colapso-do-citius-nao-se-sabe-o-que-parou-os-tribunais-1808572>
- https://www.jornaldenegocios.pt/economia/justica/detalhe/igfej_diz_que_citius_esta_em_pleno_a_partir desta_segunda_feira

<34> The “Offshores Apagão”: A Failure in Financial Data Processing

Description: Between 2011 and 2014, the Portuguese Tax Authority (Autoridade Tributária e Aduaneira – AT) failed to process in a first moment all the declarations from financial institutions reporting offshore money transfers, amounting to around €10 billion. The underlying issue stemmed from a data import failure in the PowerCenter ETL system used by AT. The error was not flagged by any automated control until it was discovered in 2016 when a manual processing found inconsistencies in the data. Even if no data was lost, public outcry and media scrutiny followed, particularly after it emerged that the incident had been kept out of the political spotlight during an election year. Although criminal sabotage was ruled out, the case exposed failures in information management, internal controls, and accountability mechanisms.

Relevant Lecture Notes Sections:

- **2.1** Governance of IT
- **2.2** Leadership Roles and Governance Posture
- **2.5** Strategic Alignment
- **2.7** Stakeholder Management and Information Systems
- **2.8** Information Governance and Management
- **3.3** IT Operations
- **3.5** Resilience
- **3.10** Continuity and Recovery
- **3.13** Operational Resilience and Incident Response

Classification:

- **Cause:** *Systemic failure in information governance* — Lack of auditability, absence of alerts for unprocessed data, poor design of error handling in critical tax processing systems. No formal mechanisms ensured completeness or cross-verification of ETL imports.
- **Consequence:** *Institutional invisibility of €10 billion in offshore transfers* — Failure to detect undeclared transactions hindered compliance monitoring and undermined public trust in the justice and fiscal system.
- **Results:** *Political scandal, loss of institutional credibility, and reinforcement of demands for digital transparency and auditability in public sector systems* — The Ministry of Finance faced reputational damage, and Parliament initiated inquiries. Though the judiciary later closed the case without finding criminal intent, structural issues in public sector digital governance, management and operational assurance were questioned.

Online Sources (Portuguese):

- <https://www.publico.pt/2023/03/14/economia/noticia/ministerio-publico-arquiva-apagao-offshores-afasta-sabotagem-informatica-2042221>
- <https://pplware.sapo.pt/informacao/autoridade-tributaria-apagao-fez-desaparecer-10-mil-milhoes-de-euros/>
- <https://sicnoticias.pt/pais/2023-03-14-Arquivado-caso-do-apagao-que-deixou-fugir-10-mil-milhoes-ao-Fisco-5b753024>
- <https://jornaleconomico.sapo.pt/noticias/dez-mil-milhoes-para-offshores-ministerio-publico-arquiva-caso-do-apagao-na-autoridade-tributaria/>

<35> Amazon’s HR Tech Backlash (2021)

Description: Amazon faced significant employee dissatisfaction following the rollout of new internal HR technologies designed to manage performance evaluations, promotions, and employee support services. Instead of improving the employee experience, the new systems were often seen as opaque, rigid, and dehumanising. Reports highlighted that

automated workflows led to delays in resolving HR issues, errors in leave management, and communication breakdowns, damaging trust and morale. The case illustrates the risks of deploying internal digital systems without adequate governance of change management, stakeholder engagement, and employee-centric design.

Main Relevant Sections in the Lecture Notes:

- 1.5 Governance, Risk, and Compliance
- 1.19 Governance and Organisational Culture
- 2.5 Governance and Information Technology
- 2.7 Stakeholder Management and Information Systems
- 4.3 Stakeholder Engagement and Strategic Communication
- 4.5 Target Operating Model
- 4.8 Strategic Portfolio and Investment Governance

Classification:

- **Cause:** Poor stakeholder engagement; weak operational governance of internal digital initiatives.
- **Consequence:** Employee dissatisfaction; reputational damage; operational inefficiencies.
- **Results:** Ongoing adjustments to HR tech platforms; increased scrutiny on internal digital transformation governance.

Online Sources:

- <https://www.nytimes.com/2021/10/24/technology/amazon-employee-leave-errors.html>
- <https://www.shrm.org/topics-tools/news/technology/amazons-troubles-hold-lessons-hr-tech-employee-experience>
- <https://www.forbes.com/sites/jackkelly/2021/10/25/a-hard-hitting-investigative-report-into-amazon-shows-that-workers-needs-were-neglected-in-favor-of-getting-goods-delivered-quickly/>

<36> Delta's Digital Cascade Failure (2024)

Description: In July 2024, Delta Air Lines suffered a massive operational breakdown following a critical software failure triggered by a faulty update from cybersecurity vendor CrowdStrike. While many organisations recovered quickly, Delta's dependence on fragile internal systems (especially for crew-tracking and scheduling) amplified the disruption. Over 7,000 flights were cancelled, affecting more than 1.3 million passengers. Investigations revealed that Delta's internal resilience plans had not adequately addressed external vendor risks or critical system dependencies. Moreover, communication with stranded passengers was slow and confusing, eroding trust. The incident exposed systemic weaknesses in vendor governance, operational resilience, and stakeholder crisis management, prompting regulatory investigations, reputational fallout, and renewed calls for integrated risk oversight in critical infrastructure sectors like aviation.

Main Relevant Sections in the Lecture Notes:

- 1.5 Governance, Risk, and Compliance
- 1.7 Governance, Management, and Operations
- 2.5 Governance and Information Technology
- 2.23 Vendor and Contract Management
- 2.25 IT Supply-Chain
- 3.5 Resilience
- 3.13 Operational Resilience and Incident Response
- 4.3 Stakeholder Engagement and Strategic Communication
- 4.8 Strategic Portfolio and Investment Governance

Classification:

- **Cause:** Over-reliance on third-party software; insufficient operational resilience testing; weak vendor dependency governance.
- **Consequence:** Service paralysis; massive customer dissatisfaction; reputational harm; financial claims.
- **Results:** Federal investigations launched; Delta initiated strategic reviews of IT governance, vendor risk management, and resilience frameworks.

Links for Further Reading:

- https://en.wikipedia.org/wiki/2024_Delta_Air_Lines_disruption

<37> Via Verde: Seamless Mobility, Strategic Risks (1991...)

Description: Via Verde, launched in 1991 in Portugal, pioneered automatic electronic toll collection, allowing vehicles to pass through highway tolls without stopping. Over time, the system expanded to other services such as car parks, fuel stations, and drive-thru payments. Its success is attributed to strong stakeholder alignment (infrastructure operators, banks, government) and user-centric design. However, the strategic dependence on a single identity-token (the Via Verde transponder) raised concerns about privacy, service resilience, and vendor lock-in. The system's evolution illustrates both the benefits of digital integration and the governance challenges of managing multi-service platforms at national scale.

Main Relevant Sections in the Lecture Notes:

- 1.5 Governance, Risk, and Compliance
- 1.7 Governance, Management, and Operations
- 2.5 Governance and Information Technology

- 2.7 Stakeholder Management and Information Systems
- 2.8 Information Governance and Management
- 2.11 Information Privacy
- 4.1 Business and Strategy
- 4.5 Target Operating Model
- 4.8 Strategic Portfolio and Investment Governance

Classification:

- **Cause:** Strategic drive for frictionless mobility and national-scale digital integration.
- **Consequence:** Outstanding service convenience; growing dependency on a single platform; privacy and competition concerns.
- **Results:** Expansion into multiple service domains; reinforcement of governance structures; emerging public debates on data protection and future interoperability with European frameworks.

Links for Further Reading:

- <https://novaresearch.unl.pt/en/publications/a-collaborative-network-case-study-the-extended-via-verde-toll-pay>
- <https://recil.ulusofona.pt/server/api/core/bitstreams/54eb0b03-6272-49cb-b34a-430e14d284a3/content>
- https://en.wikipedia.org/wiki/Via_Verde
- <https://executivedigest.sapo.pt/cadernos-especiais/via-verde-mais-do-que-uma-marca-um-conceito/>

<38> Southwest's Meltdown: The Real Cost of Technical Debt (2022)

Description: In December 2022, Southwest Airlines faced a catastrophic operational collapse, cancelling thousands of flights and stranding millions of passengers. Investigations revealed that the disaster was rooted in years of accumulated **technical debt**, particularly the failure to modernise its crew-scheduling system, SkySolver. While other airlines recovered quickly after a major winter storm, Southwest's outdated system could not handle the scale of disruptions, forcing employees to manually reestablish crew assignments by phone. The incident highlighted systemic weaknesses in IT governance, operational resilience, and strategic risk management, demonstrating how deferred investment in core systems can magnify external shocks into full-blown organisational crises.

Main Relevant Sections in the Lecture Notes:

- 1.5 Governance, Risk, and Compliance
- 1.7 Governance, Management, and Operations
- 2.5 Governance and Information Technology
- 2.23 Vendor and Contract Management
- 2.25 IT Supply-Chain
- 3.5 Resilience
- 3.10 Operational Culture and Organisational Maturity
- 3.13 Operational Resilience and Incident Response
- 4.1 Business and Strategy
- 4.3 Stakeholder Engagement and Strategic Communication
- 4.8 Strategic Portfolio and Investment Governance

Classification:

- **Cause:** Accumulated technical debt; delayed IT modernisation; operational culture tolerating fragile legacy systems.
- **Consequence:** Widespread flight cancellations; reputational damage; financial losses; regulatory scrutiny.
- **Results:** Forced strategic review of IT and operational processes; accelerated (belated) investment in cloud migration and resilience initiatives; stronger industry focus on technical debt governance.

Links for Further Reading:

- <https://devops.com/southwest-technical-debt-richixbw/>
- <https://www.nytimes.com/2023/01/10/podcasts/the-daily/the-southwest-airlines-meltdown.html>
- <https://www.nytimes.com/2023/01/06/business/southwest-airlines-meltdown-costs-reimbursement.html>
- <https://www.nytimes.com/2022/12/29/opinion/southwest-airlines.html?searchResultPosition=4> (by Paul Krugman!!!)
- Popular Science Report