Where Execution Breaks Down

Digital transformation initiatives frequently falter not simply due to subpar tools or resistance to change amongst teams. More often, the root causes lie in a disconnection between how work is intended to be executed (the Process Domain) and how digital systems enforce that execution (the Digital Domain). This often leads organizations to a frustrating revelation: while they document processes intending to drive efficiency and innovation, the actual execution leads to misalignment and operational breakdowns.

In this exploration of execution challenges, we will delve into insights drawn from the lecture "Where Execution Breaks Down" and the underlying principles outlined in the whitepaper "Digital Transformation: Strategies for Execution." Our focus is on how organizations can better navigate the complex boundary between the Process Domain and the Digital Domain to ensure that execution aligns with strategic intentions.

The Boundary Where Execution Fails

When execution breaks down, the consequence can manifest as operational friction. Symptoms include tasks being duplicated across systems, delays in data availability, stalled approvals due to unclear authority, and the use of informal channels like emails and spreadsheets to handle exceptions. These patterns can mislead leaders into thinking they are facing technology issues, but often, they signal deeper problems with how processes and technologies interact at a fundamental level.

Execution relies heavily on how processes—the intended ways of doing work—are mapped to the technologies that support them. If a disparity exists, the organization may find itself executing according to what the technology dictates, not what the process requires. This boundary must be managed carefully; otherwise, organizations risk ceding control to technology, which might inadvertently degrade established processes.

Whether through gaps in workflow states, mismatched decision rights, or insufficient evidence capture, understanding and managing these misalignments is crucial. For instance, consider a scenario where a process requires certain approvals before moving forward, but the technology allows actions to be taken without those approvals being verified. In such cases, the organizational intent is undermined, leading to a cascading effect of risks and inefficiencies.

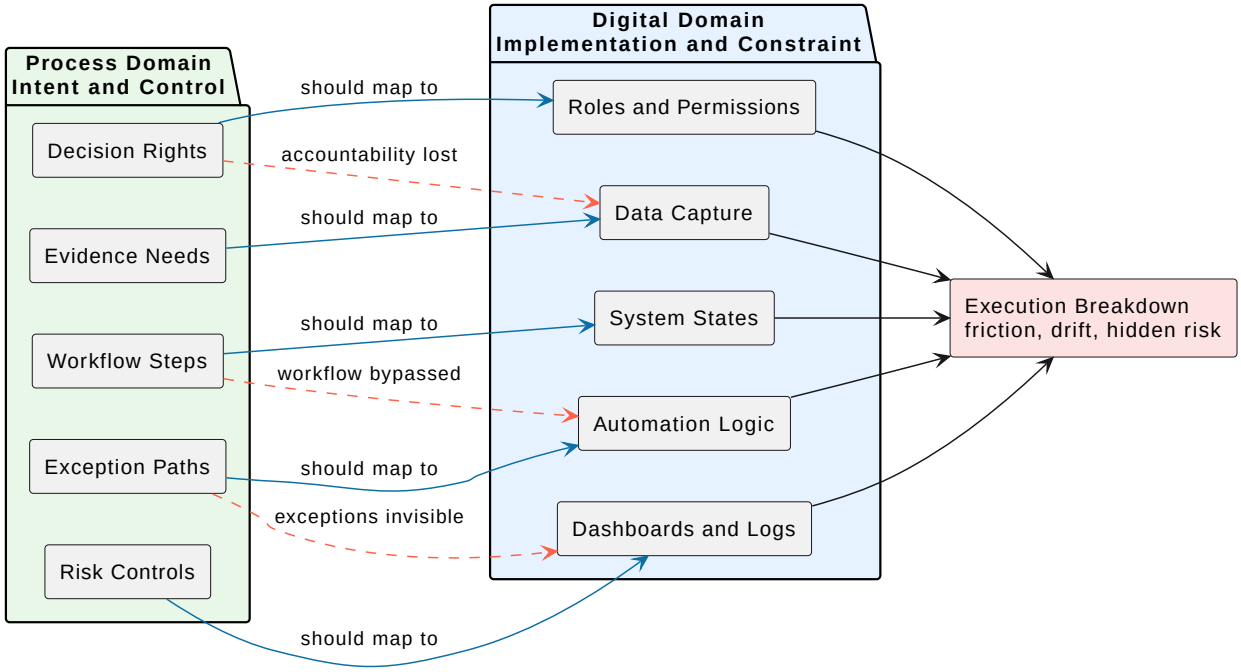

Figure 1. Process/Digital Mapping Failure

Understanding Execution Breakdowns

Fundamentally, execution failures occur when there's misalignment between the design of the Process Domain and the functionality of the Digital Domain. Here's how this misalignment typically manifests:

1. **Workflow Mismatch**: When documented processes and their corresponding digital workflows diverge, it often leads to confusion. Teams must either work around the technology or abide by rules that do not reflect reality, ultimately resulting in frustration and inefficiency.
2. **Decision and Evidence Mismatch**: The distinction between who makes decisions and who executes them can blur. If a process specifies decision-making authorities but the digital system only controls execution permissions, accountability diminishes, and operational effectiveness suffers.
3. **Data and Exception Mismatch**: Successful automation hinges on accurate and reliable data. When data is stale, duplicated, or not governed, it falls short of its potential—especially within analytics or automated decision-making frameworks.
4. **Governance Shortfalls**: Effective governance defines how processes should operate and clarifies roles, evidence requirements, and the controls necessary to maintain process integrity. A lack of governance can result in random technology configurations that compromise the intended workflow.
5. **Feedback Gaps**: Without proper metrics in place to monitor process health, organizations

miss early warning signs of breakdowns. Poor visibility into execution performance can lead to sustained inefficiencies and eventual failures in meeting commitments.

Understanding these distinctions allows organizations to recognize where execution issues often arise and prompts a reevaluation of both the Process and Digital Domains.

The Role of Governance in Workforce Mappings

Governance serves as an essential mechanism for aligning the Digital Domain with the Process Domain. By making mappings between these domains explicit, governance provides clarity about roles, responsibilities, and the protocols that must be followed throughout the workflow.

To achieve effective governance, organizations can ask the following critical questions:

- What steps within a process are automated versus manual?
- Who owns each stage of the workflow?
- What evidence must be captured as work is executed?
- How are exceptions managed when they occur?
- What policies govern the process, and how do the systems enforce them?

With governance in place, organizations can create comprehensive mappings that link process intents with technology implementations. This way, decision-making abilities, accountability, and evidence collection remain intact throughout digital transformations, ensuring that operational challenges are mitigated.

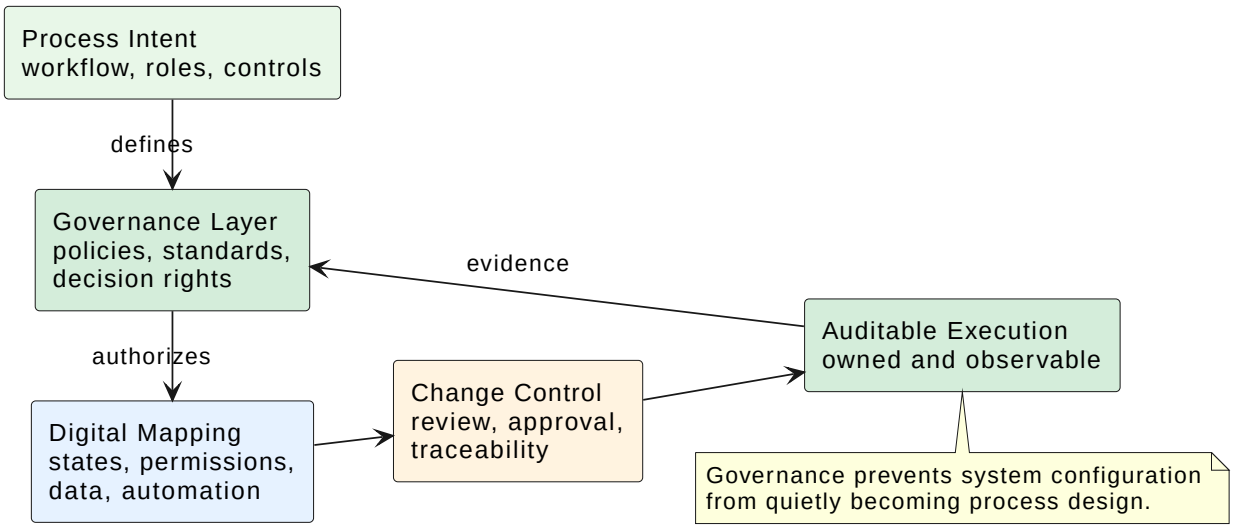

Figure 2. Governance Mapping Control

Risk Management: Proactively Identifying Failures

Risk Management plays a pivotal role by examining where process-to-technology mappings might fail and helping organizations establish controls to maintain that mapping's integrity. In doing so, it shifts the approach from merely reacting to failures to proactively designing against them.

Key considerations within risk management include:

- Understanding the limitations of automation—what happens if a data field is inaccurate or absent?
- Identifying areas where manual workarounds could bypass established controls, introducing unnoticed risks.
- Examining how exceptions are handled and whether they remain visible to governance oversight.

By embedding risk management within the early design of digital transformations, organizations can create a more resilient operational structure capable of withstanding unforeseen challenges.

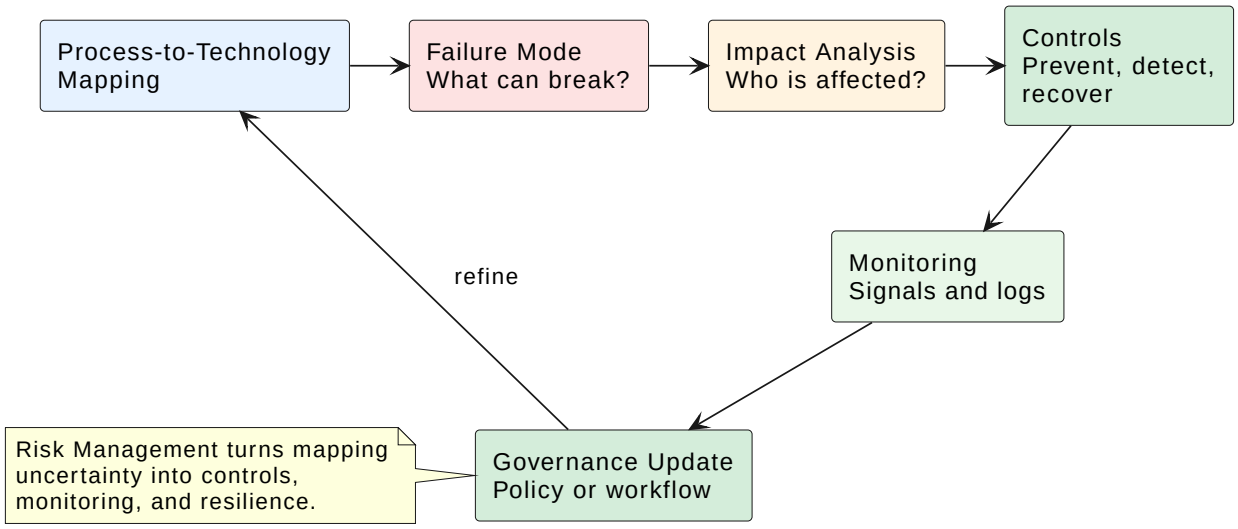

Figure 3. Risk Testing Loop

Identifying Opportunities for Improvement

For transformation efforts to succeed, organizations must regularly inspect their processes and the corresponding technology systems. This inspection involves ensuring that all mappings between the two domains align and that any drift is promptly addressed.

Here are some effective practices organizations can adopt:

- Ensure that system states correspond accurately to process states, allowing roles and responsibilities to be effectively managed.
- Include feedback mechanisms that reveal how well the organization is executing and where improvements are necessary.
- Foster a culture of transparency around data dependencies, controls, and exception handling.

By diligently managing the relationship between the Process Domain and the Digital Domain, organizations position themselves to decode the complexities of digital transformation while ensuring that their execution aligns with strategic objectives.

Conclusion: The Path Forward in Digital Transformation

In summary, addressing execution challenges requires comprehensive oversight of the

relationship between processes and technologies. Governance must clarify, control, and audit these mappings, while risk management should continuously identify failures before they escalate.

As leaders and practitioners navigate these challenges, it becomes essential to remember that technology should enhance and adhere to the established process architecture rather than define it. Doing so cultivates resilience in execution and increases the likelihood of successful digital transformation.

Learn More

- Full lecture episode: https://embracingdigital.org/en/lectures/dta-18/index.html
- Series blog summary: https://embracingdigital.org/en/lectures