Shadow System

What Are Shadow Systems?

Shadow systems (sometimes called shadow IT or shadow databases) are unofficial information systems that are created and used by employees or departments outside the control of the organization's central IT department.

These systems are not part of the official, approved IT or BI infrastructure — meaning they "live in the shadows" of formal governance.

They're usually built because business users need to solve a problem, get a report, or access data faster than IT can provide.

Example to Imagine

Suppose a company's marketing team wants a weekly report showing how many customers clicked on recent ads.

- *The official BI system takes **2 weeks** to deliver new reports because IT has a backlog.*
- *So, one marketing analyst downloads the raw data from Google Ads and Salesforce into **Excel**, builds a pivot table, and shares the results via **email or Google Sheets**.*
- *Soon, everyone in the team starts relying on that spreadsheet for decisions.*

*That Excel workbook is now a **shadow system** — because:*

- *It's not managed by IT,*
- *It's not integrated into the company's data warehouse,*
- *It's being used to make business decisions.*

How to Identify Shadow Systems

You can't manage what you can't see. To identify them, look for:

1. Duplicate or inconsistent data sources
    - Multiple versions of the same data (e.g., sales numbers that don't match the official report)
2. Locally managed databases or files
    - Access or Excel files with sensitive data
3. Reports or dashboards not linked to official BI tools
4. Manual processes
    - Employees manually copying data from one system to another
5. Department-owned applications
    - Apps purchased with departmental budgets (without IT's approval)

How to Evaluate Shadow Systems

Criteria	Questions to Ask
Business Value	Does this system provide critical functionality or insights not covered by official BI?
Data Quality	Is the data accurate, timely, and consistent?
Security Risk	Is sensitive data stored securely? Who has access?
Sustainability	Who maintains it? What happens if that person leaves?
Integration Potential	Can it be integrated into official BI systems?

Essentially: some shadow systems are *useful innovations*, others are *risk bombs*.

How to Govern Shadow Systems

Governance doesn't mean killing them all — it means managing them wisely.

Steps:

1. Acknowledge and document them
    - Maintain a registry of known shadow systems
2. Assess and prioritize
    - Decide which ones to formalize, migrate, or retire
3. Create policies and guardrails
    - Define when and how departments can create local solutions
    - Require basic standards (security, backup, data source integrity)
4. Provide better BI support
    - Often shadow systems exist because official tools don't meet needs — improve usability and responsiveness
5. Encourage collaboration
    - Empower business users ("citizen developers") but ensure oversight through IT and data governance teams

Why Shadow Systems Are a Problem (and Also an Opportunity)

The Risks:

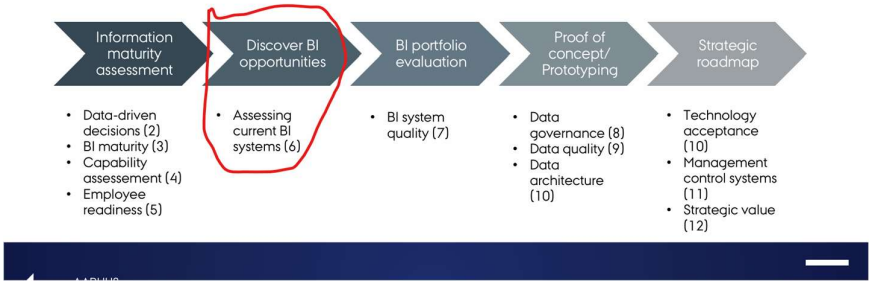
- Data inconsistency: Different versions of "the truth."
    - Example: Sales numbers in Marketing's spreadsheet don't match Finance's report.
- Security risks: Sensitive data stored on personal drives or shared via email.
- Lack of backups: If the creator leaves, the knowledge and system go with them.
- Poor scalability: Spreadsheets and Access databases can't handle large data volumes.
- Regulatory compliance issues: Data may be handled outside approved systems.

The Opportunities:

- They often fill gaps where official systems fall short.
- They can be sources of innovation — users experimenting with new ideas, dashboards, or analyses.
- Sometimes, IT can learn from shadow systems what kind of insights users really want.

AGILE INTEGRATIVE METHODOLOGY FOR STRATEGIC BUSINESS INTELLIGENCE

AIMS-BI



Proccess

- Assess current BI initiatives
- Understand any planned BI investments
- Discover BI opportunities

Data Collection

- Interviews with Business users
  - To learn about current data systems
  - To learn about future whishes

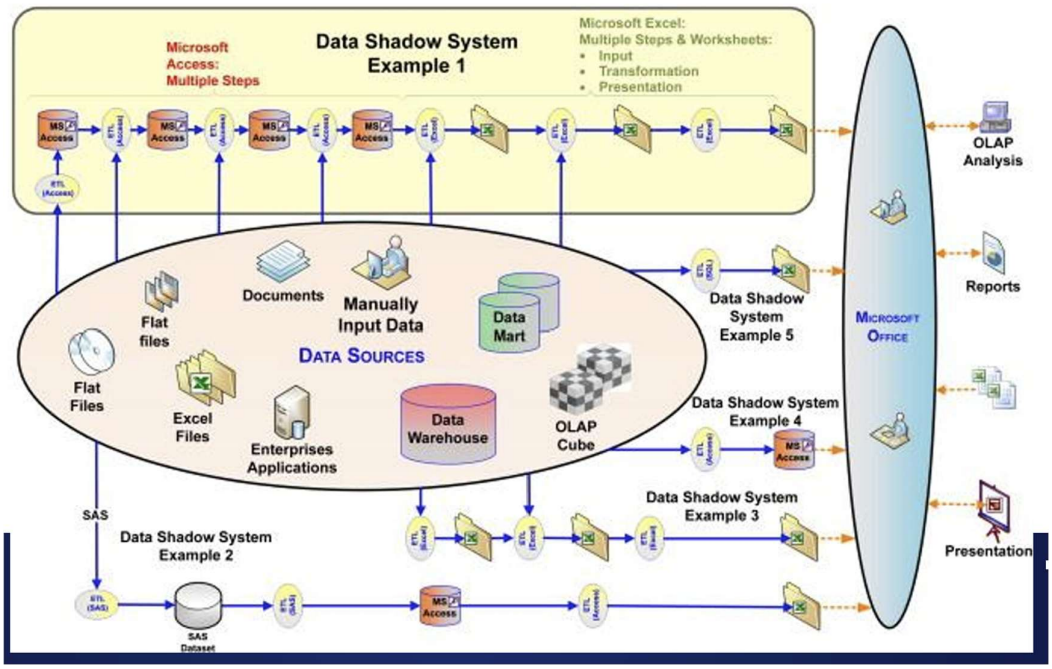
- the name of the initiative
- the type of BI involved (e.g. advanced vs descriptive analytics)
- the business process it supports
- the target users
- the business context
- the strategic objective the initiative aligns with
- the consumers of the information
- key business questions the initiative will answer
- the performance measures
- the constraints (i.e. what will affect the success of the initiative; e.g. poor data quality)
- the data sources needed to implement the initiative.

Shadow Systems

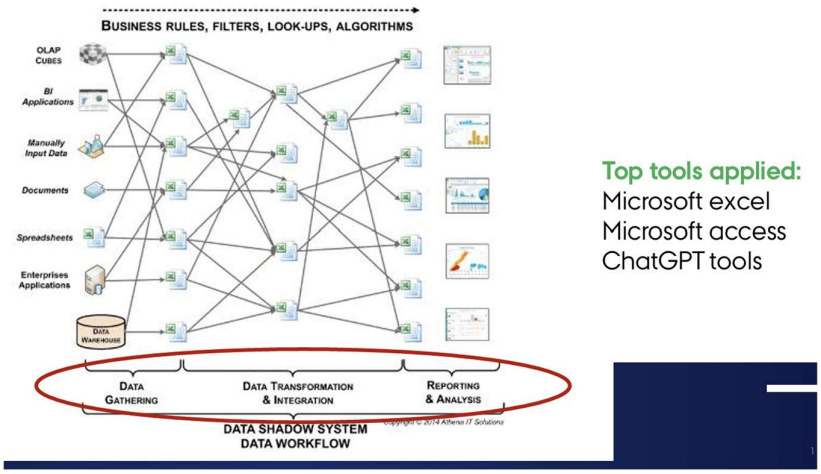
Data Shadow Systems

DATA SHADOW SYSTEMS

- Support Business Processes
  - Used for budgeting, forecasting, pipeline analysis, profitability analysis, etc.
- Include Data From Many Sources
  - Enterprise applications
  - Data warehouses
  - Data marts
  - External sources
  - BI applications
  - PDFs
- Use of BI and EDW
  - May use the BI and enterprise data warehouse (EDW) set up by IT
  - Or may be self-made systems created by business users
- Key Points
  - Data shadow systems are a fact of life in companies of all sizes
  - Business groups take matters into their own hands when:
    - They don't get the data they need
    - Business decisions are affected
    - Their requests are too low in the IT project queue
    - IT collaboration is ineffective
    - IT resources are not available
- What Happens
  - Business people gather data themselves
  - This enables their own reporting and analysis



Shadow Systems aka Spreadmarts



Examples of Shadow Systems / Spreadmarts

1. Excel Spreadsheets for Financial Reports
    - The Finance department downloads data from the company's ERP system into Excel every week.
    - They build their own budgeting and forecasting spreadsheets because the official BI reports take too long to update.
    - Each analyst keeps their own version — numbers don't always match across departments.
    - This is a classic "spreadmart" — a spreadsheet-based data mart used outside official BI systems.
2. Sales Team's Local Access Database
    - The Sales team creates an Access database to track customer leads and deals.
    - It combines data exported from CRM, Excel, and emails.
    - IT doesn't manage or back it up — only one person knows how it works.
    - This becomes a shadow system because it operates independently of the company's data warehouse.
3. Marketing's Power BI Dashboard from CSV Files
    - The Marketing team wants a campaign performance dashboard.
    - Since IT is busy, they export CSV data from social media and Google Ads and upload it into Power BI.
    - They update it manually every week.
    - This dashboard uses unofficial data — making it a shadow BI system.
4. HR's Google Sheet for Employee Data
    - HR needs quick headcount and turnover reports.
    - Instead of using the official HR system, they collect data in a shared Google Sheet.
    - Other managers edit it directly, causing data inconsistencies.
    - This Google Sheet acts as a shadow system.
    - Operations Team's "Homegrown" Tracking App
    - Operations builds a simple web app to track inventory and deliveries.
    - It's not connected to the enterprise data warehouse (EDW).
    - It works — but no one outside the team knows its structure or data rules.
    - Another shadow system, because it runs outside IT control.

SHADOW SYSTEM PROCESS FOR DATA

1. Sourcing (Records)
    - Collecting and updating data
    - Data comes from one or more different sources
      (for example: enterprise systems, spreadsheets, or external files)

    This is the step where shadow systems gather raw data.
2. Transformation (Integrating)
    - Integrating and processing data
    - Bringing together data from different places
    - Making it consistent and usable for analysis

    In this step, users combine and clean data manually or with simple tools.
3. Application (Analyzing)
    - Generating KPIs (benchmarks, targets, metrics)
    - Analyzing data and processing results to support business decisions

    This step turns data into insights, reports, or dashboards.

Result of the Three Phases

These three phases — Sourcing, Transformation, and Application — lead to an evaluation of risks versus value for the business.

- Shadow systems can provide high value (fast insights, flexibility)
- But they also bring high risk (data errors, inconsistency, lack of control)

Shapes of shadow systems

Shadow systems can take many forms or "shapes" inside a company. Here are the most common ones:

Spreadsheets

- Excel or Google Sheets used for storing, calculating, or reporting data outside the main BI system.

Workarounds

- Using systems for purposes they weren't designed for.
  Example: using the email system to store files instead of the central database.

BYOD / BYOA (Bring Your Own Device / App)

- Employees use personal or unauthorized devices or apps to access, store, or analyze company data.

Cloud-Based Solutions

- Using external cloud tools (e.g., Dropbox, Google Drive, or online analytics tools) that are not approved or managed by IT.

Unauthorized Software

- Installing or using programs not approved by central IT, often to perform analysis or reporting faster.

Software Installed Outside Central IT

- Business units install and manage their own local applications instead of using company-managed systems.

End-User Development

- Local business units or employees create their own additions or small systems — like Access databases, macros, or custom scripts — to extend existing systems.

In Short

- Shadow systems come in many shapes — from simple spreadsheets to unauthorized apps all built or used outside official IT control to meet immediate business needs.

How shadow IT (shadow systems) affect companies in real life.

High Prevalence of Shadow IT

- 41% of Danish companies report shadow IT within their organizations *(ITU)*.
- Employees often seek faster or more efficient tools than those officially approved by IT.

Security Concerns

- Over 60% of Danish companies cite security risks from shadow IT *(Trade.gov)*.
- Unauthorized tools are often used without proper security protocols, increasing vulnerability to cyberattacks.

Data Management Issues

- Around 45% of companies face data management challenges due to shadow IT *(Invest in Denmark)*.
- Unapproved tools lead to fragmented data storage, making data governance and compliance difficult.

Lack of Cybersecurity Training

- 50% of developers in Danish companies say they need more cybersecurity training *(ITU)*.
- This knowledge gap increases risks linked to shadow IT usage.

Regulatory Compliance Challenges

- 38% of companies struggle with regulatory compliance because shadow IT tools may not meet legal or industry standards *(Invest in Denmark)*.

Resource Constraints

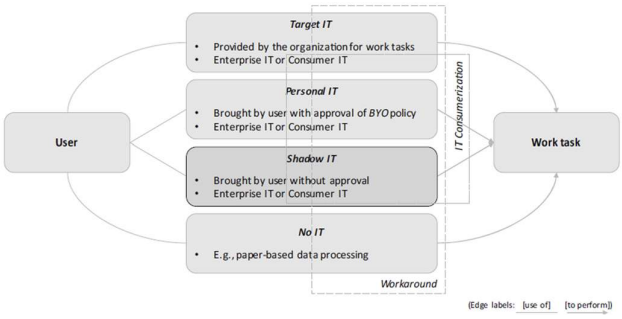
- 35% of companies believe they lack sufficient resources to effectively address shadow IT and cybersecurity issues *(Trade.gov)*.
- Cybersecurity management is resource-intensive and often underfunded.

Productivity Gains (Positive Aspect)

- 52% of companies say shadow IT has improved productivity *(Invest in Denmark)*.
- Employees use more efficient or user-friendly tools, which help them work faster despite the risks.

Different Types of Shadow IT

1. Target IT
    - Provided by the organization for official work tasks
    - Managed and approved by the IT department
    - Can be Enterprise IT or Custom IT
2. Personal IT
    - Brought by the user but with approval (as part of a BYO policy – Bring Your Own)
    - May include Enterprise IT or Consumer IT devices/apps
      (e.g., personal laptop approved for remote work)
3. Shadow IT
    - Brought or used by the user without IT approval
    - Can be Enterprise IT or Consumer IT tools
      (e.g., using personal cloud storage or unapproved software for work)
4. No IT
    - Non-digital methods used for information processing
      (e.g., paper-based data processing or manual record keeping)



The Shadow System Process

1. Pull data
    - From EDW (Enterprise Data Warehouse), data marts, business applications, or external sources
    - Import it into a spreadsheet or local database
2. Manipulate the data
    - Use data queries or Excel macros to clean or adjust the data
    - Perform several rounds of manual updates
3. Add more data
    - Pull in additional information that the business uses
    - Combine it with the existing dataset
4. Store results
    - Put the combined and processed results into a spreadsheet
5. Crunch numbers
    - Perform final calculations or analysis on the spreadsheet data
6. Create visuals
    - Build pivot tables, charts, or graphs to summarize results
7. Prepare reports
    - Format the final worksheet as a report
8. Present results
    - Share or present the analysis to management or stakeholders

Shadow System Weaknesses

Lack of Security

- Data is often stored in unprotected files or systems.
- High risk of data breaches or unauthorized access.

Limited Control

- IT has no visibility or authority over how data is used or managed.
- Difficult to enforce company policies or standards.

Inefficiency

- Manual processes take extra time and effort.
- Repeated data handling increases errors and delays.

Resource Use for Maintenance and Updates

- Requires constant manual updates.
- Consumes employee time that could be spent on higher-value tasks.

Low Integration and Supervision

- Shadow systems don't connect well with official IT systems.
- Lack of oversight causes inconsistent and incomplete data.

Lost Productivity of Business Analysts

- Analysts spend more time fixing or maintaining shadow systems instead of doing real data analysis or decision-making support.

Risk From Shadow System

1. Collection (Recording) – *SOR = System of Record)* *SOR* = ***collecting the right, safe data***.
   - Inconsistent data
   - Incorrect data entry
   - Errors when changing data sources
   - Lack of updates to master data
   - Example:
     Someone enters customer sales data into Excel by hand every week.
     If they forget to update or make a typo, the data becomes unreliable.
2. Transformation (Integration) – *SOI = System of Integration* *SOI= Combining data*
   - Missing data architecture and governance
   - Excessive reliance on macros for data processing
   - Example:
     A spreadsheet uses complex macros to merge sales data and forecast results.
     If one macro fails or data format changes, the whole file can produce wrong numbers.
3. Usage (Analyzing) – SOA = System of Analysis SOA = **using your data to make smart choices**.
   - Lack of scalability (systems can't handle growth or complexity)
   - Loss of productivity among business analysts
     - Time spent on system maintenance
     - Endless debates about finding "the right number" (data inconsistencies)
   - Example
     Two departments use their own versions of a report, showing different "total revenue" numbers — causing confusion about which one is accurate.

Benefits of Shadow Systems

Increased Productivity

- Employees can quickly get the data and reports they need.
- Less waiting for IT support or project approvals.

Cost Effective

- Cheaper to create and maintain than large IT systems.
- Uses existing tools like Excel or Access.

Increased Innovation

- Business users can experiment and find new solutions faster.
- Encourages creative problem-solving.

Increased Flexibility

- Easy to adjust when business needs change.
- Users can modify tools or data without IT delays.

Increased Agility

- Faster response to new opportunities or challenges.
- Helps teams act quickly in dynamic environments.

Optimal IT Solution

- Fills gaps where official IT systems don't provide needed functionality.
- Complements existing IT infrastructure.

Busniess Value from shadow systems

1. Collection (Recording)
    - Contains business knowledge — built by users who understand their data and processes.
    - Solves the lack of IT resources — created when IT can't deliver fast enough.
    - Generates useful data that helps business people make informed decisions.
    - Fills the gap where there's a lack of tools for analysis and visualization.
    - Designed for business users, not IT staff — increases efficiency and usability.
2. Transformation (Integration)
    - Generates actionable data for better decision-making.
    - Provides needed tools for combining, analyzing, and visualizing data.
3. Usage (Analyzing)
    - Supports the company's workflow — keeps business running smoothly.
    - Prevents operations from being delayed due to IT system limits.
    - Enhances efficiency by using business knowledge effectively.

In Simple Terms

- Shadow systems create business value by filling gaps left by IT —
  helping users collect, integrate, and analyze data faster to support daily decisions and operations.

Shadow Systems Die Hard

The phrase “Shadow Systems Die Hard” means that shadow systems are very difficult to remove or replace, even when a company introduces better, official IT systems.

They “die hard” because people keep using them, often for emotional, practical, or organizational reasons.

Why They’re Hard to Eliminate:

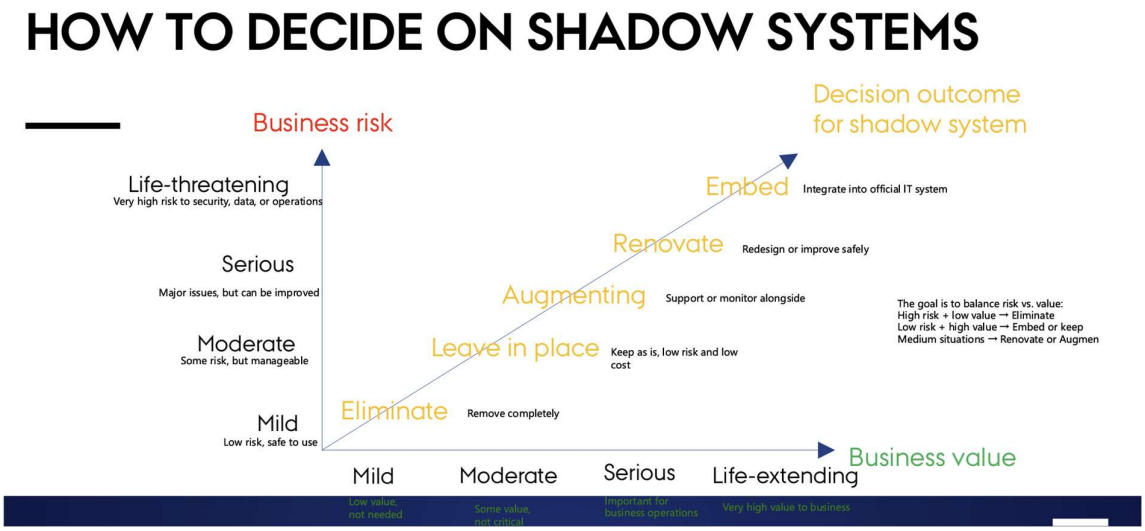
1. Change Reduces Effectiveness (at first)
    - When switching to a new system, productivity may drop temporarily.
    - People are comfortable with their existing shadow systems and don’t want to lose speed.
2. New Tools Require Learning
    - Employees have to spend time learning new software or processes.
    - It feels easier to stick with what they already know (Excel, Access, etc.).
3. Super Users Are Valuable
    - Some employees become “experts” in the shadow system.
    - It’s easier for management to rely on these experts than to build a new system from scratch.
4. Employee Identity and Motivation
    - People often take pride in their shadow systems because they built or customized them.
    - Shutting them down can hurt morale or make employees feel their work isn’t valued.
5. Question of Termination
    - Because of these reasons, companies must think carefully before removing all shadow systems at once.
    - Sometimes it’s better to phase them out gradually instead of abruptly shutting them down.

Determinate what to do with Shadow Systems

1. Identify the Shadow Systems
    - Find all shadow systems used in the organization.
    - Describe each one:
        - Type of system (e.g., spreadsheet, local database, cloud tool)
        - Drawbacks/Risks (e.g., errors, security issues)
        - Benefits/Value (e.g., faster reporting, flexibility)

2. Evaluate Risk Level
    - Assess the risk of each shadow system during:
        - Sourcing (data collection)
        - Transformation (data integration)
        - Analysis (data usage)
3. Evaluate Business Value
    - Measure how much value each shadow system provides:
        - Locally (for a specific team or department)
        - Organizationally (for the whole company)
4. Create an Overview and Recommendations
    - Summarize all shadow systems.
    - Include key findings, risks, value, and recommendations (e.g., keep, improve, or replace).
5. Management Ranking
    - Rank each shadow system based on its contribution to KPIs (key performance indicators).
6. Decide on Each Shadow System
    - Based on the above evaluations, decide whether to:
        - Keep it
        - Improve it
        - Integrate it into official IT
        - Or eliminate it

How to decide on Shadow Systems



Business Risk Estimation

We need to know where the BI system is at risk — in:

- SOR (Sourcing / Recording)
- SOI (Transformation / Integration)
- SOA (Analysis / Usage)

Important Notes

- No risk can be ignored
- The highest risk level determines overall system risk
- A risk is a risk — even small ones matter
- Risk at all levels = red flag

On a scale from 1-10

- 1-2: No risk
- 3-4: Modest risk
- 5-6: Risk
- 7-8: Sever risk
- 9-10: Life-threatning

🗂️ 1. Sourcing (SOR) – Data Collection

Goal: Collect accurate, consistent, and traceable data

Risk Level	Description	Example
1–2 (No Risk)	Data comes from official company databases or APIs; updated automatically.	Pulling data directly from ERP or CRM via secure BI connection.
3–4 (Modest)	Small delays or manual entries cause minor inconsistencies.	Weekly Excel updates of sales figures; occasional typos.
5–6 (Risk)	Some data missing or not approved by IT.	Local HR spreadsheet not synced with HR system.
7–8 (Severe)	Data sources unknown to others; not linked to central systems.	Department collects sales data manually; not shared with IT.
9–10 (Life-Threatening)	Data cannot be traced or verified; decisions based on wrong info.	Financial forecasts based on unverified Excel sheets.

2. Transformation (SOI) – Data Integration

Goal: Combine and process data with accuracy and governance

Risk Level	Description	Example
1–2 (No Risk)	Data is processed using standard ETL tools with full IT oversight.	Automated pipelines in Power BI or Tableau Server.
3–4 (Modest)	Some manual cleanup or Excel formulas used.	Manual lookup tables in Excel before reporting.
5–6 (Risk)	Unofficial scripts or macros used to merge data.	VBA macro combines data from two files; breaks easily.
7–8 (Severe)	No data cleansing or structure; integration often fails.	Different file formats merged manually; high error rate.
9–10 (Life-Threatening)	No governance, poor architecture; outputs unreliable.	Shadow Access database feeds critical reports with no validation.

3. Analysis (SOA) – Data Usage

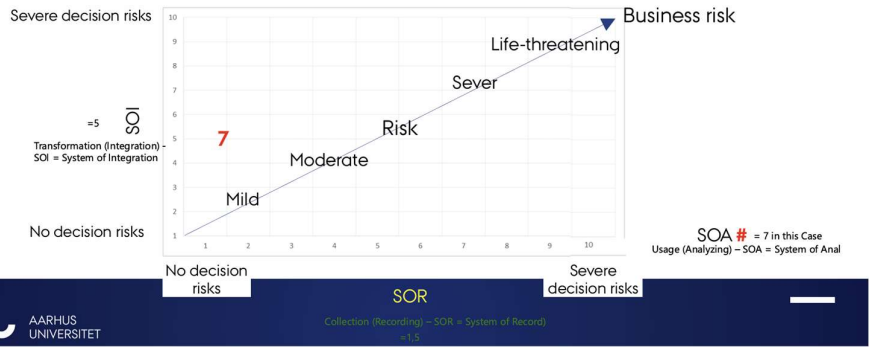
Goal: Enable accurate analysis, reporting, and decision-making

Risk Level	Description	Example
1–2 (No Risk)	Uses verified dashboards and IT-supported BI tools.	Reports generated in Power BI with approved access levels.
3–4 (Modest)	Occasional manual report creation; minor time waste.	Monthly KPI reports manually adjusted in Excel.
5–6 (Risk)	Analysts spend more time cleaning data than analyzing.	50% of time spent fixing broken Excel formulas.
7–8 (Severe)	High workload maintaining shadow systems; inconsistent results.	Department uses old Access database with frequent crashes.
9–10 (Life-Threatening)	System crashes or loses data; stops business work completely.	Unauthorized software fails during quarter-end reporting.

EXAMPEL: UNAUTHORIZED SOFTWARE

- Data records (SOR)
  - Pulls on EDW data in the company
- Transforming (integration) (SOI)
  - Security risk
  - Cost effective
  - Requires own data architecture
- Analyzing and use (SOA)
  - Crashes in software are not supported by IT (lost ability to work)
  - Flexibility

UNAUTHORIZED SOFTWARE

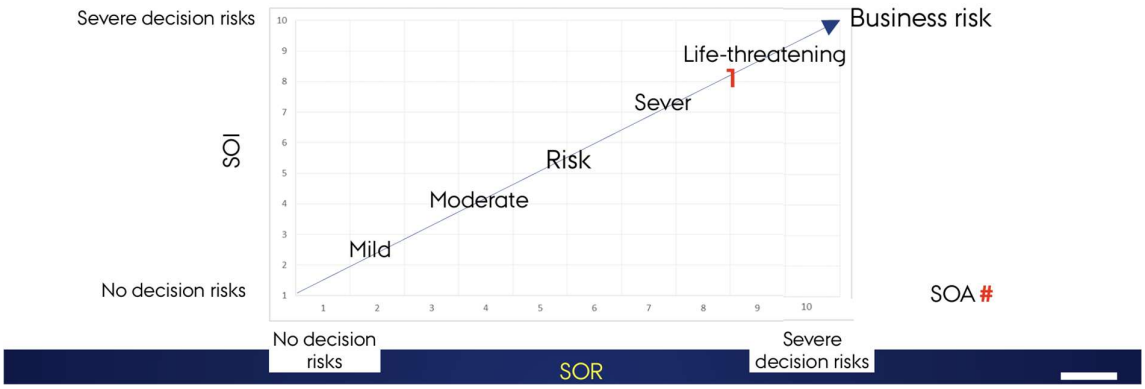


EXAMPEL – LOCAL DATA SOURCE

From raw data to BI dash board

- Data records (SOR)
  - Not linked to any public data points
  - Unknown to the rest of the organization
  - Data cannot be traced
- Transforming (integration) (SOI)
  - Data cannot be integrated
  - There is no cleansing and no franchinsing
- Analyzing and use (SOA)
  - Resources used on data management and not on job
  - High local use for business person

LOCAL DATA SOURCE



Evaluate Business Value

Business Value Levels

- Two Organizatinal Levels
  - Local level:
    - Low = individual value
    - Medium = Team or Group Value
    - High = Business Unit Value
  - Company level:
    - Low = Team value
    - Medium = Business unit value
    - High = enterprise value

🧩 1. LOCAL LEVEL

(Value within a department, team, or for individual users)

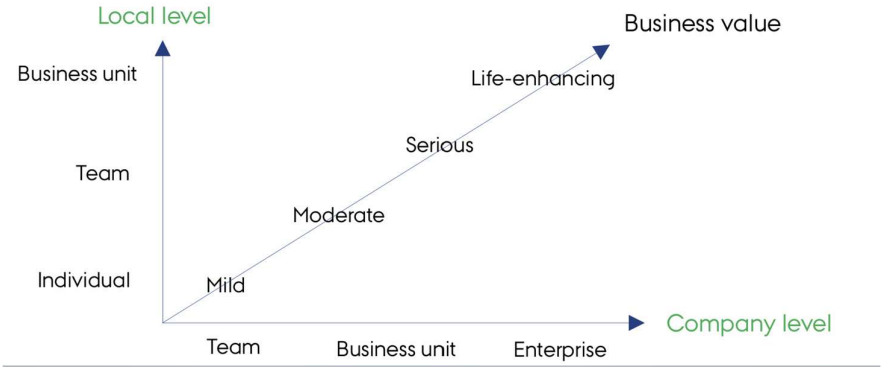
Value Level	Meaning	Examples
Low (Individual Value)	Used by one person for personal efficiency	• An employee keeps an Excel sheet to track their own sales leads. • A finance analyst uses a personal macro to speed up reporting. • A marketer tracks campaign results manually in Google Sheets.
Medium (Team or Group Value)	Used by a small team or group to coordinate work	• A small HR team uses a shared spreadsheet to track leave and attendance. • A project team builds its own dashboard to track progress. • A customer service group uses Trello or Airtable to monitor daily tickets.
High (Business Unit Value)	Used by an entire department or unit to manage core activities	• The finance department creates its own BI dashboard for budgeting and forecasting. • Sales department uses a local Access database to track client performance. • Marketing builds a shadow system for campaign analysis and KPIs.

🌍 2. COMPANY LEVEL

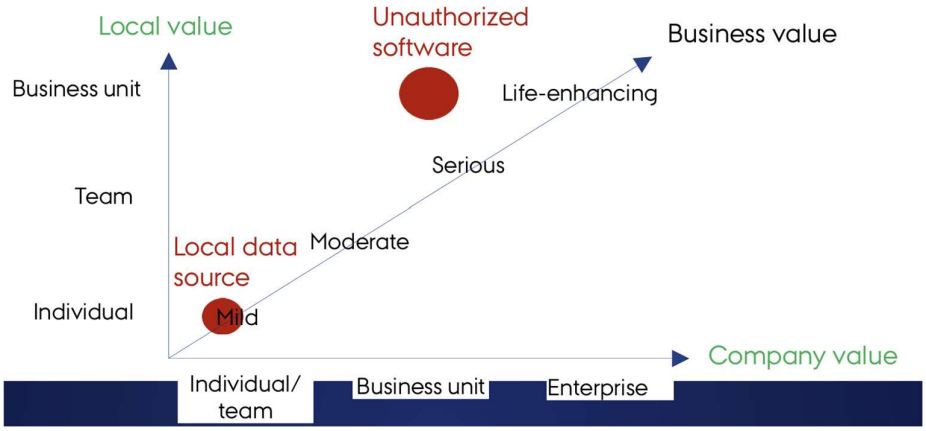
(Value that impacts the organization as a whole)

Value Level	Meaning	Examples
Low (Team Value)	Helps a small group, but not widely adopted across departments	• One logistics team uses a local app to track shipments. • A shadow reporting system exists in one store location.
Medium (Business Unit Value)	Used by a department or division that affects company results	• The finance division's spreadsheet model is used for company-wide budget planning. • The HR analytics dashboard is used to make hiring or training decisions across offices. • Regional sales reports built outside IT are used by upper management.
High (Enterprise Value)	The system supports or influences decisions across the entire company	• A global Excel model is used for forecasting company profits. • A Power BI dashboard created by one team becomes the standard reporting tool for executives. • A shadow data warehouse integrates multiple business areas and supports enterprise KPIs.

Tool to access Business Value of Shadow Systems



Example from above



Give Overview of shadow systems including recommendations(YOUR JOB)

This step is about collecting and presenting information — not making the final decision yet.
You create a clear picture of all shadow systems and what you recommend based on your findings.

What happens in this step:

- Summarize all shadow systems you identified.
- Describe their type, purpose, users, risks, and business value.
- Evaluate each one's pros and cons.
- Suggest recommendations (e.g., *keep, improve, integrate, or replace*).
- This overview helps management see the full landscape before making decisions.

Example:

Shadow System	Type	Risk	Value	Recommendation
Sales Excel Tracker	Spreadsheet	Moderate	High	Improve and integrate with BI
Local Access DB	Database	High	Low	Eliminate
Marketing Dashboard	Power BI	Low	High	Keep and support

✅ **Goal:** Present a structured **overview and recommendations** for decision-makers.

Management Ranking

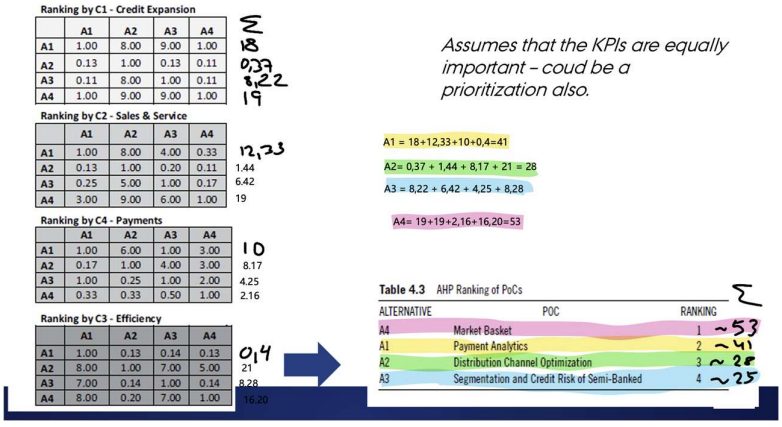
To decide **which shadow systems** should be **replaced, supported, or embraced first**, based on how important they are to the company's **strategic KPIs**.

1. Categorize Shadow Systems
    - Classify each system into one of the following groups:
        - Replace – High risk, low business value
        - Embrace/Support – Valuable and used widely
        - Improve – Moderate risk or value; needs governance
2. Rank by Strategic KPIs
    - Compare each shadow system's contribution to the company's key performance indicators (KPIs).
    - This helps prioritize which systems should be handled first (important ones linked to major KPIs).
3. Select KPIs for Evaluation
    - Management should choose 3–5 strategic KPIs (for example):
        - Profitability
        - Customer satisfaction
        - Operational efficiency
        - Data quality
        - Risk reduction
4. Use Analytic Hierarchical Processing (AHP)
    - Apply the AHP method to evaluate and rank systems.
    - AHP helps compare multiple systems objectively based on how strongly they impact each KPI.

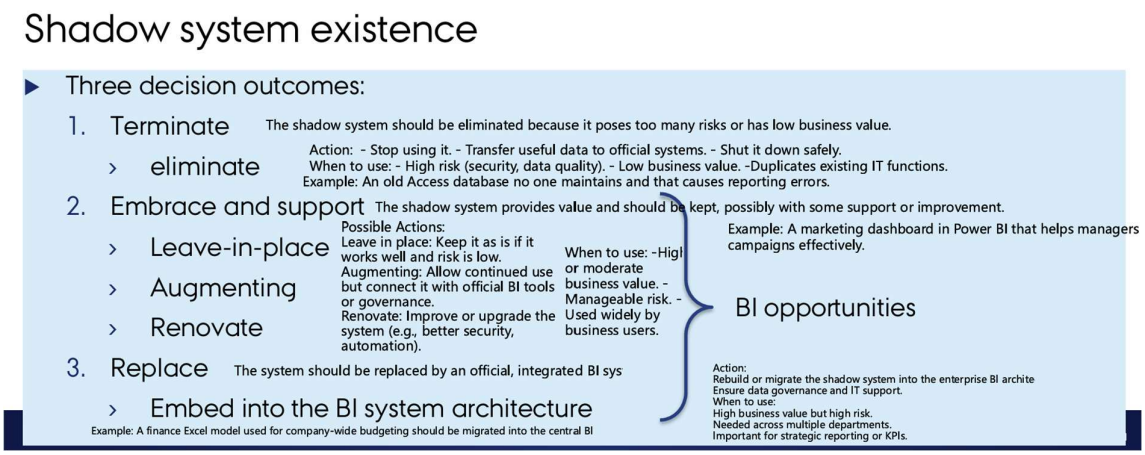
Table 4.1 Ranking Guide

COMPARED TO THE SECOND ALTERNATIVE, THE FIRST ALTERNATIVE IS:	NUMERICAL RATING
Extremely preferred	9
	8
Very strongly preferred	7
	6
Strongly preferred	5
	4
Moderately preferred	3
	2
Equally Preferred	1

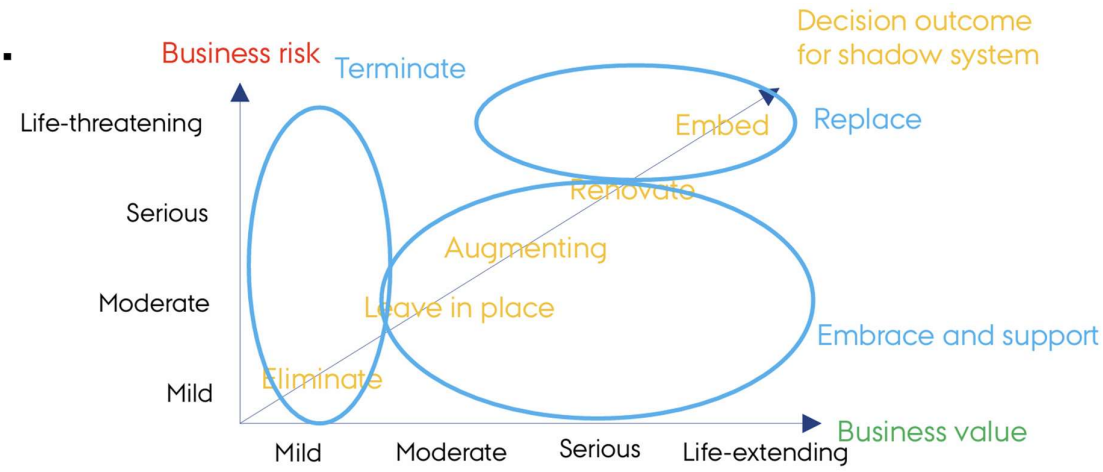
Example:



Management Decision



How to Decide on Shadow Systems



RENOVATING DATA SHADOW SYSTEMS

When a shadow system is valuable but risky, it can be renovated instead of eliminated. Renovation means improving and securing how the system works — especially how data is collected, integrated, and analyzed.

1. Secure Data Integration
   - Goal: Make sure all data coming into the system is accurate, consistent, and safe.
   - Actions:
     - Collect data from all relevant sources.
     - Integrate and validate it (check for errors or duplicates).
     - Apply business rules to standardize data (e.g., same format, same definitions).
     - Ensure compliance with company data policies.

Example:

A sales team's Excel system is connected securely to the enterprise data warehouse instead of manual uploads.

2. Secure Analytics
   - Goal: Ensure analysis and reporting are reliable, traceable, and secure.
   - Actions:
     - Analyze data to identify trends and patterns.
     - Create business plans and reports based on verified data.

- Use results to recommend decisions to management.
- Ensure only authorized users can access sensitive data.

Example:

A marketing shadow dashboard is renovated to pull verified data from approved BI sources and is now used safely for campaign planning.

Business Analysts' Role

- Collaborate with IT to ensure proper data integration.
- Use renovated systems to create insights, forecasts, and recommendations.
- Act as the link between data and decision-making.

Secure data integration:
Collect, integrate, and validate data and implement business rules

Business analysts

Secure analytics:
Analyze data, id trends, create plans, recommend decisions

Example 1

1. Identify the Shadow Systems

Case 1

1. Marketing Team Using Unauthorized Cloud Storage

Description: A marketing team uses a third-party cloud storage service to share large multimedia files internally and with external clients because the official IT-approved storage is too slow or ha insufficient capacity.

Why: Speed and convenience of file sharing and collaboration.

Risks: Data breaches, lack of control over sensitive information, potential non-compliance with da protection regulations.

Benefits: Faster and more efficient workflow, improved collaboration with external partners.

2. Sales Team Adopting CRM Software

Description: The sales department starts using an unapproved CRM system because the official one lacks certain features or is too complicated.

Why: Need for a more user-friendly interface and better functionality to track and manage customer interactions.

Risks: Data silos, inconsistent data management, security vulnerabilities, integration issues with other company systems.

Benefits: Increased sales productivity, better customer relationship management, enhanced user experience.

Case 2

3. HR Department Utilizing a Third-Party Recruitment Platform

Description: HR uses an external recruitment platform to streamline the hiring process because th company's internal system is outdated and inefficient.

Why: To access modern recruitment tools and features not available in the company's system.

Risks: Exposure of sensitive candidate information, potential data privacy issues, and lack of integration with existing HR systems.

Benefits: More efficient hiring process, access to a broader talent pool, improved candidate experience.

Case 3

Case 4

4. Finance Team Implementing Spreadsheet Macros

Description: The finance team develops complex Excel macros to automate financial repo because the ERP system's reporting tools are insufficient.

Why: To save time and reduce manual work in generating reports.

Risks: Error-prone macros, lack of version control, difficulty in troubleshooting, and depe specific employees.

Benefits: Faster report generation, reduced manual effort, increased efficiency in financia

Case 5

5. Customer Support Using Unauthorized Messaging Apps

Description: Customer support agents use unapproved messaging apps to communicate quickly with customers because the official communication tools are too slow or cumbersome.

Why: To provide faster and more responsive customer service.

Risks: Data leakage, non-compliance with communication policies, and potential breaches of customer privacy.

Benefits: Improved customer satisfaction, quicker resolution of issues, and more efficient communication.

Case 6

6. Research Team Setting Up Independent Servers

Description: A research team sets up their own servers and databases to handle large datasets and run analyses because the central IT infrastructure is inadequate for their needs.

Why: Need for specialized computing power and storage capacity for research projects.

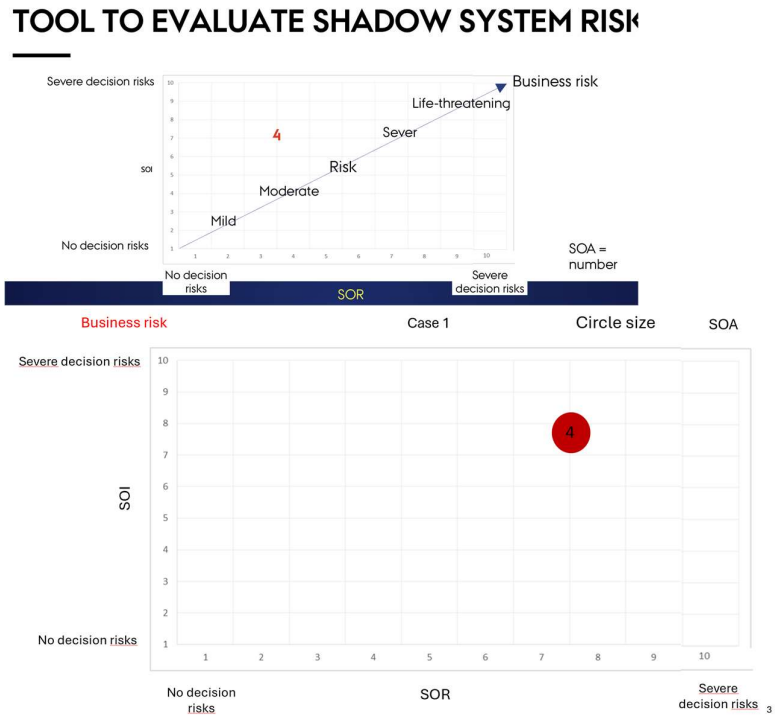
Risks: Security vulnerabilities, lack of backups, inconsistency with IT policies, and potential data loss.

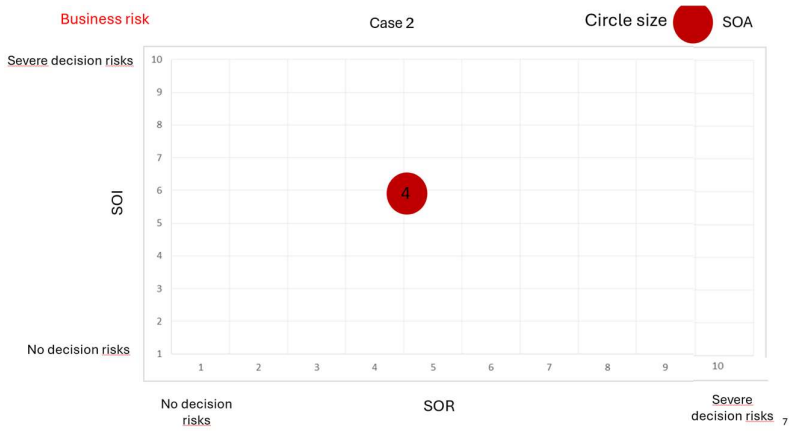
Benefits: Greater flexibility and control over research data, ability to customize the environment to specific needs, and faster project completion.

In each case, shadow IT arises due to a perceived or real inadequacy in the officially sanctioned IT solutions. While shadow IT can offer immediate and tangible benefits, it often introduces significant risks that can affect the organization's overall security, compliance, and operational efficiency.

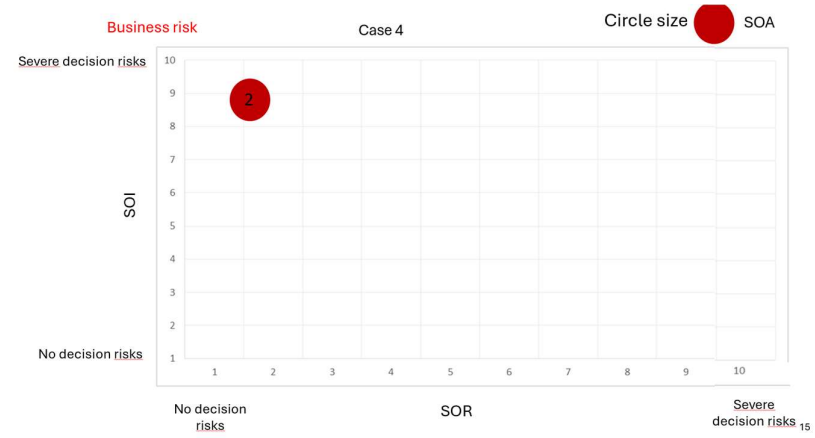
2. Evaluate Risk Level

Reminder:

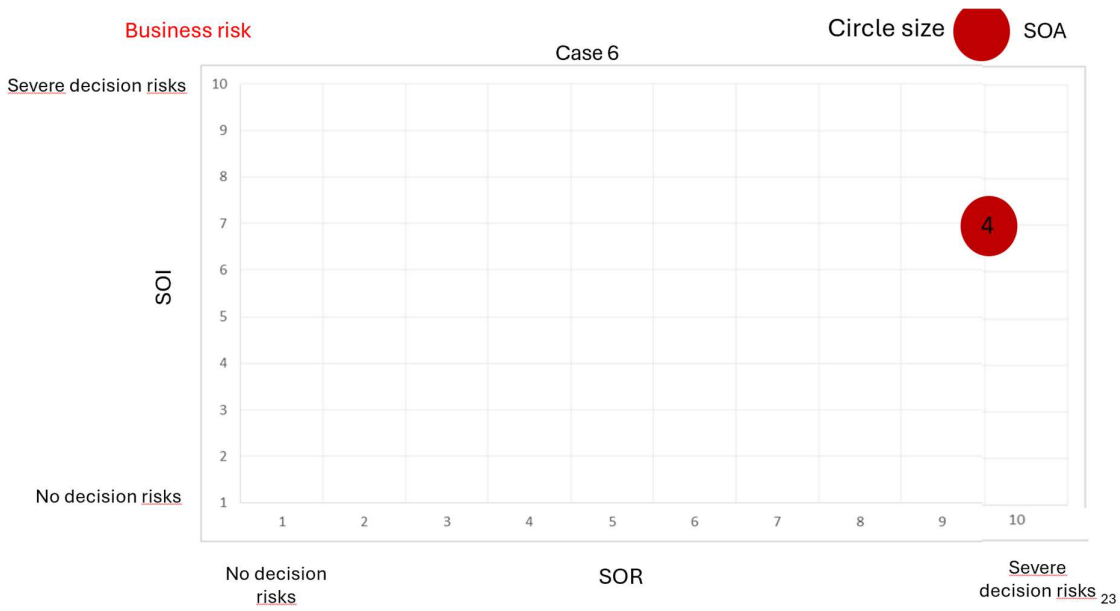



Business risk
Case 2
Circle size
SOA
Severe decision risks
SOI
No decision risks
4
No decision risks
SOR
Severe decision risks
7


Business risk
Case 3
Circle size
SOA
Severe decision risks
SOI
No decision risks
3
No decision risks
SOR
Severe decision risks
11


Business risk
Case 4
Circle size
SOA
Severe decision risks
SOI
No decision risks
2
No decision risks
SOR
Severe decision risks
15


Business risk
Case 5
Circle size
SOA
Severe decision risks
SOI
No decision risks
4
No decision risks
SOR
Severe decision risks
19



3. Evaluate Business Value

Reminder:

High = enterprise value

1. LOCAL LEVEL

(Value within a department, team, or for individual users)

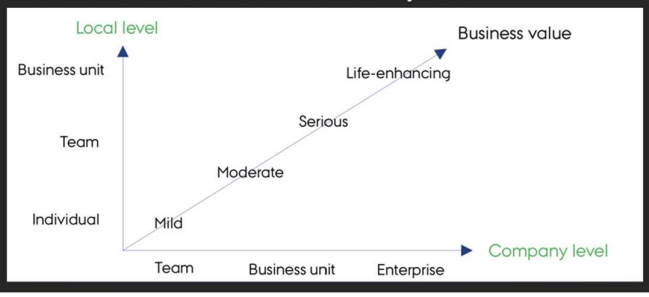
Value Level	Meaning	Examples
Low (Individual Value)	Used by one person for personal efficiency	• An employee keeps an Excel sheet to track their own sales leads. • A finance analyst uses a personal macro to speed up reporting. • A marketer tracks campaign results manually in Google Sheets.
Medium (Team or Group Value)	Used by a small team or group to coordinate work	• A small HR team uses a shared spreadsheet to track leave and attendance. • A project team builds its own dashboard to track progress. • A customer service group uses Trello or Airtable to monitor daily tickets.
High (Business Unit Value)	Used by an entire department or unit to manage core activities	• The finance department creates its own BI dashboard for budgeting and forecasting. • Sales department uses a local Access database to track client performance. • Marketing builds a shadow system for campaign analysis and KPIs.

2. COMPANY LEVEL

(Value that impacts the organization as a whole)

Value Level	Meaning	Examples
Low (Team Value)	Helps a small group, but not widely adopted across departments	• One logistics team uses a local app to track shipments. • A shadow reporting system exists in one store location.
Medium (Business Unit Value)	Used by a department or division that affects company results	• The finance division's spreadsheet model is used for company-wide budget planning. • The HR analytics dashboard is used to make hiring or training decisions across offices. • Regional sales reports built outside IT are used by upper management.
High (Enterprise Value)	The system supports or influences decisions across the entire company	• A global Excel model is used for forecasting company profits. • A Power BI dashboard created by one team becomes the standard reporting tool for executives. • A shadow data warehouse integrates multiple business areas and supports enterprise KPIs.

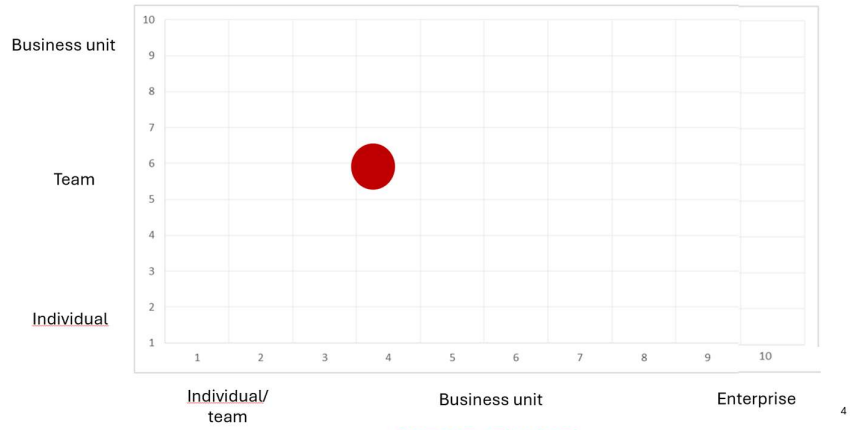
Tool to access Business Value of Shadow Systems



Business value

Local value level

Case 1



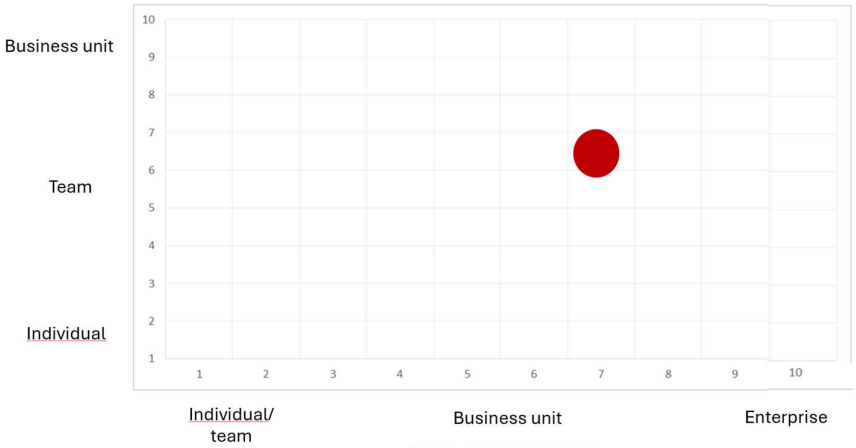
4

Company value level

Business value

Local value level

Case 2

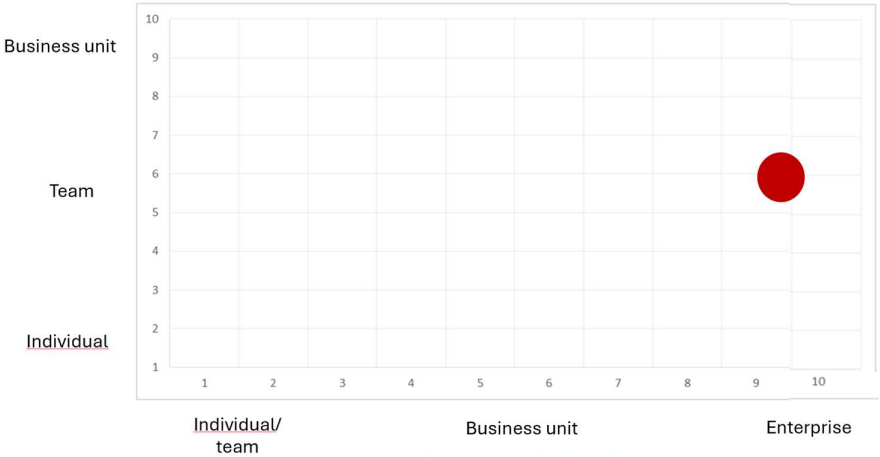


Company value level

Business value

Local value level

Case 3



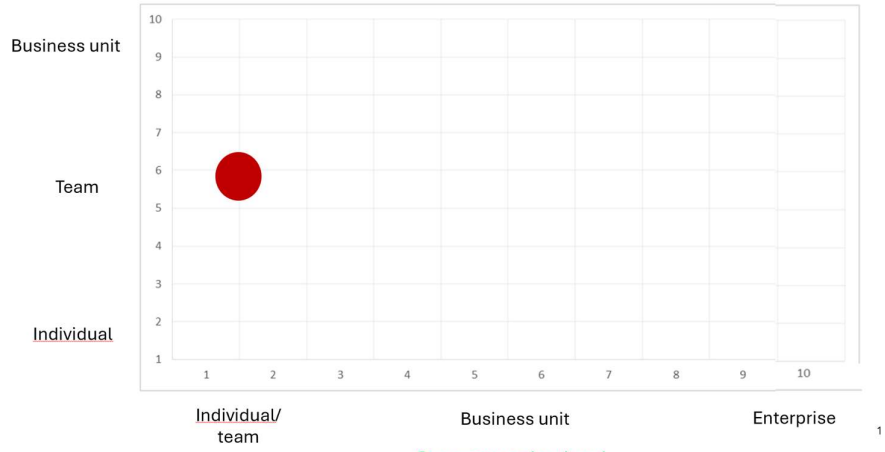
1

Company value level

Local value level

Business value

Case 4



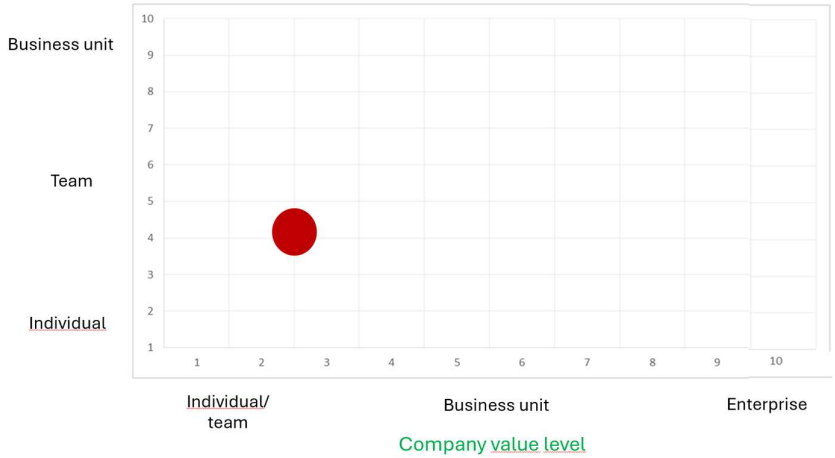
1

Company value level

Business value

Local value level

Case 5



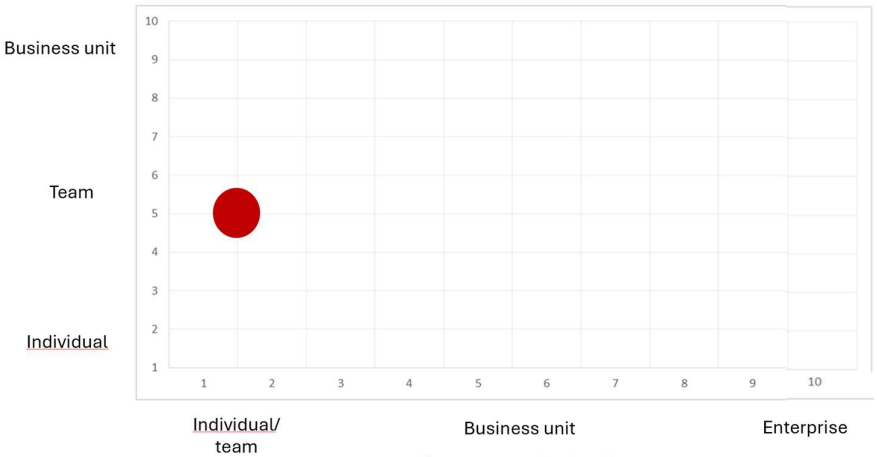
20

Company value level

Business value

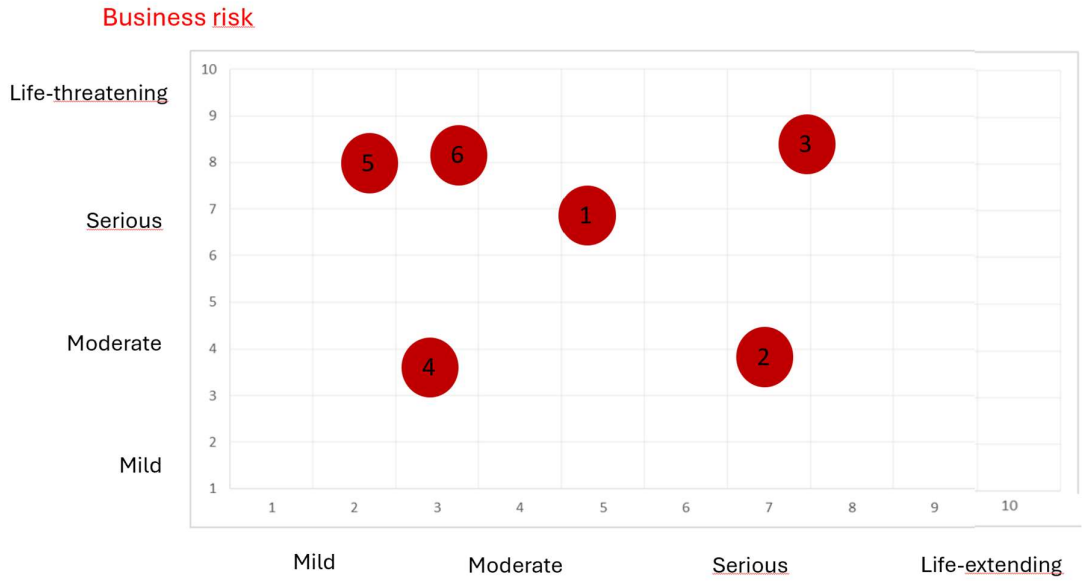
Local value level

Case 6



Company value level

4. Create an Overview and Recommendations



#	Shadow System	Key Findings	Business Risk	Business Value	Recommendation
1	Marketing team using unauthorized cloud storage	Easy file sharing, but stored data is outside company control; risk of data leaks or non-compliance.	**Serious to Life-threatening** ⚠ (security, privacy)	**Moderate** 💡 (useful for collaboration)	**Replace / Integrate** – Move to approved, secure cloud (e.g., SharePoint, OneDrive, or company server).
2	Sales team adopting CRM software without IT approval	Improves customer tracking and sales efficiency, but data is not synchronized with central BI systems.	**Moderate** ⚠	**High** 🔥 (supports key business processes)	**Renovate / Integrate** – Link CRM data with BI system, ensure IT security standards are met.
3	HR department using third-party recruitment platform	Efficient hiring, but sensitive candidate data may be stored externally; compliance risk (GDPR).	**Life-threatening** 🔴	**Serious** 🔥	**Replace** – Use official HRIS (Human Resources Information System) or approved recruitment tool.
4	Finance team implementing spreadsheet macros	Saves time for calculations and reporting, but prone to errors and difficult to audit.	**Moderate** ⚠	**Mild to Moderate** 💡	**Renovate** – Automate reports through official BI tools and reduce macro dependency.
5	Customer support using unauthorized messaging apps	Faster internal communication but unmonitored; risk of data leakage and no chat history tracking.	**Serious** ⚠	**Mild** 💡	**Eliminate** – Move to company-approved communication tools (e.g., Teams, Slack enterprise).
6	Research team setting up independent servers	Allows data processing freedom and experimentation, but lacks IT oversight, creating high security and maintenance risks.	**Serious to Life-threatening** 🔴	**High** 🔥	**Renovate / Integrate** – Bring servers under IT management; ensure data governance and backup.

General:

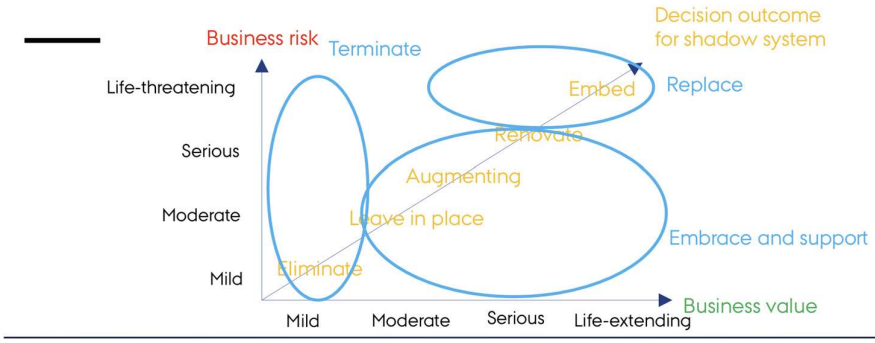
Business Risk	Business Value	Typical Key Findings	General Recommendation
Mild	**Mild**	Small, personal tool used by one person or team; minimal business impact; low risk of errors or leaks.	⚪ **Leave in place** – Low priority. Keep if useful; remove if unused.
Mild	**Moderate**	Simple tool supporting daily tasks efficiently; limited integration or oversight issues.	🟢 **Embrace & Support** – Keep and ensure backups, documentation, and basic data protection.
Mild	**Serious**	Reliable shadow system that supports multiple teams; well-maintained but informal.	🟢 **Support / Integrate Gradually** – Keep using it but align with BI standards and IT monitoring.
Mild	**Life-Extending**	High-impact, innovative system that drives success; low risk, strong user ownership.	🟢 **Embrace** – Consider formalizing or integrating into official IT environment.
Moderate	**Mild**	Somewhat outdated or redundant; provides limited benefit; manual processes.	🟡 **Phase Out** – Replace with official or automated BI solution if possible.
Moderate	**Moderate**	Useful but not standardized; inconsistent data quality; manual steps required.	🟡 **Monitor / Improve** – Clean data, reduce manual work, provide user training.
Moderate	**Serious**	Important for team operations; some security or consistency risks exist.	🟠 **Renovate** – Add automation, apply validation rules, involve IT for better control.
Moderate	**Life-Extending**	Critical tool with moderate governance weaknesses (e.g., Excel dashboards).	🟠 **Integrate / Support** – Work with IT to make it part of the BI system.
Serious	**Mild**	Old, insecure, or inaccurate tool with little real benefit.	🔴 **Eliminate** – Too risky for its small value; remove immediately.
Serious	**Moderate**	Provides value but exposes sensitive data or violates compliance policies.	🔴 **Replace** – Rebuild inside official BI or IT-supported tools.
Serious	**Serious**	Frequently used for decision-making but unstable or manual.	🟠 **Renovate / Embed** – Recreate within secure, governed BI environment.
Serious	**Life-Extending**	Mission-critical system with major risks (e.g., financial or compliance exposure).	🔴 **Urgent Replacement** – Integrate into enterprise BI or rebuild securely.
High	**Mild**	Error-prone, unsecured, minimal value to the organization.	🔴 **Terminate Immediately** – Not worth keeping.
High	**Moderate**	Locally useful but dangerous to data integrity or security.	🔴 **Replace** – Migrate data and functionality to official systems.
High	**Serious**	Valuable but ungoverned system used widely; lacks control or backups.	🟣 **Embed / Rebuild** – Integrate into official BI architecture with IT support.
High	**Life-Extending**	Critical to business operations but non-compliant or high-risk.	🔥 **Top Priority for Integration** – Immediate IT and management action needed.

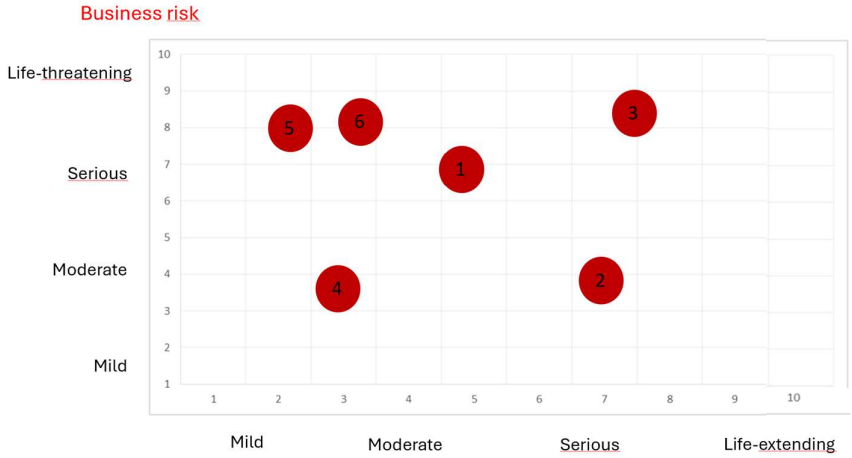
5. Management Ranking

- Rank each shadow system based on its contribution to KPIs (key performance indicators).

6. Decide on Each Shadow System

Reminder:





#	Shadow System	Decision	Why / Argumentation
1	**Marketing team using unauthorized cloud storage**	**Embrace and Support (Improve)**	The marketing team uses an unapproved cloud tool to **share campaign files quickly** and **collaborate efficiently**. While there is some **security risk**, the tool clearly provides **high flexibility and productivity gains**. Instead of eliminating it, IT should **formally assess and secure the tool** — for example, by implementing **access controls, encryption, and official approval**. Supporting the team through **training and integration** with the company's secure cloud (e.g., approved Google Drive or OneDrive) will balance **speed with compliance**.
2	**Sales team adopting unapproved CRM software**	**Integrate into official IT**	The CRM adds **strong business value** through better customer and sales management. However, without integration to the central BI and data warehouse, **data consistency and visibility** are at risk. The system should be **integrated and supported** by IT to keep its advantages while ensuring data governance and unified reporting.
3	**HR department using a third-party recruitment platform**	**Replace / Eliminate**	The system processes **sensitive personal data**, leading to **severe compliance and legal risks**. Although it improves recruitment speed, it lacks **IT approval and GDPR compliance**. The HR department should **migrate to an official, secure recruitment module** integrated with the company's HRIS and data protection standards.
4	**Finance team implementing spreadsheet macros**	**Improve**	The macros increase productivity by automating repetitive calculations but are **error-prone and hard to audit**. Instead of removing them, the process should be **modernized** using **official BI or reporting tools** (e.g., Power BI). Training staff in these tools will ensure accuracy and long-term sustainability.
5	**Customer support using unauthorized messaging apps**	**Eliminate**	The messaging apps create **data leakage and privacy risks**. Customer data could be shared outside controlled channels. Despite improving communication speed, the **lack of monitoring and traceability** is unacceptable. The team should move to **approved communication tools** (e.g., Teams or Slack Enterprise) with proper logging.
6	**Research team setting up independent servers**	**Integrate and Support**	The servers provide **high flexibility and innovation capacity**, but they also pose **security and maintenance risks**. Rather than shutting them down, they should be **brought under IT supervision** with managed access, backups, and monitoring. This preserves research autonomy while ensuring data protection and reliability.

General:

Eliminate

General Argumentation:

The shadow system poses high business risk (e.g., data security, compliance, or reliability) and delivers low or limited business value.

It operates outside IT governance, creating inconsistencies or data exposure.

Eliminating it will reduce risk and allow the organization to standardize operations using approved, secure tools.

Example reasoning:

- Data privacy violations or unencrypted information.
- High maintenance or duplication of existing IT systems.
- No integration with official data sources or workflows.

Integrate into Official IT (Embed)

General Argumentation:

The system has high business value and is widely used, but currently functions independently of official IT systems.

Integration ensures data consistency, security, and long-term sustainability while keeping the existing useful functionality.

IT should take over maintenance and align it with enterprise architecture and data governance.

Example reasoning:

- Supports critical processes (e.g., CRM or analytics).
- Contains valuable business knowledge worth preserving.
- Needs connection to BI/EDW systems for data accuracy.

Replace

General Argumentation:

The shadow system provides some value, but its technology, security, or scalability are no longer suitable for business needs.

Replacement with a modern, officially supported tool will deliver the same (or better) capabilities with lower risk and better integration.

The goal is to preserve the business function while upgrading the platform.

Example reasoning:

- Outdated software or unsupported systems.
- Frequent crashes or data loss.
- Better official alternatives are available.

Improve

General Argumentation:

The system works well and is valuable to business users but has inefficiencies, manual steps, or limited scalability.

Improvement through automation, training, or IT support can boost productivity and reduce risk without full replacement.

This option balances cost-effectiveness and performance.

Example reasoning:

- Spreadsheet macros or manual dashboards that need process optimization.
- Can be enhanced by IT-approved automation tools.

Embrace and Support (Integrate & Support)

General Argumentation:

The shadow system shows strong business value, user adoption, and innovation, with manageable risk.

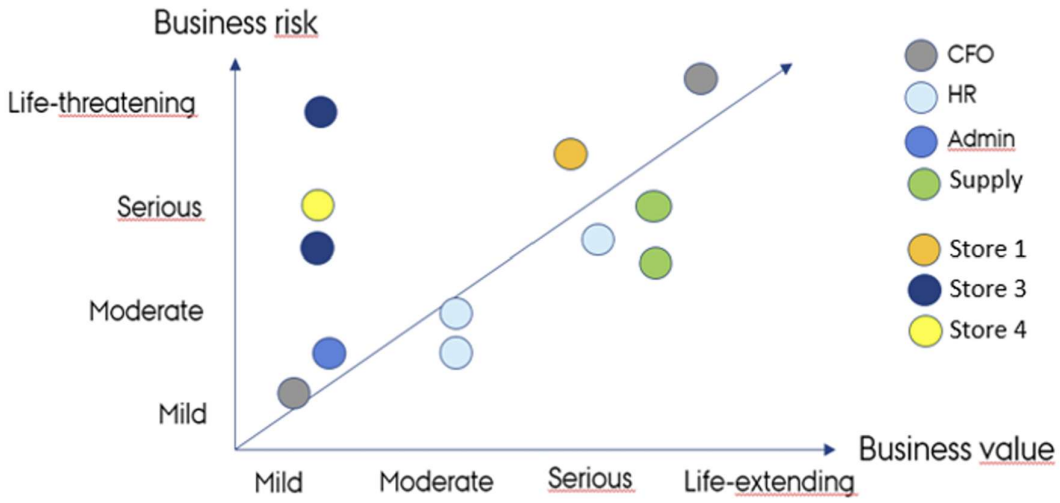
Rather than removing it, the organization should formally support, secure, and monitor it.

IT can provide guidelines, access control, and technical support to ensure compliance while maintaining flexibility and agility.

Example reasoning:

- The tool enables quick, innovative solutions that help business units operate efficiently.
- Risks can be mitigated through IT supervision, not elimination.

Example 2:



CFO Systems

Decision: Integrate into Official IT

Detailed Argumentation:

The CFO department's shadow systems show two extremes — one with very high business risk and high value, and another with low risk and low value.

Because financial data is highly sensitive and central to the organization's stability, any unregulated tool in this area poses serious threats to data integrity, compliance, and security.

Integrating these systems into the official IT environment will ensure centralized data control, auditability, and regulatory compliance (for example, GDPR or financial reporting standards).

At the same time, IT can help preserve the analytical flexibility the finance team needs, by embedding their preferred tools into a secure infrastructure.

In summary:

➡️ High impact on business → must be integrated.

➡️ Risk of non-compliance → cannot remain unmanaged.

➡️ Integration ensures both security and performance.

HR Systems

Decision: Embrace and Support

Detailed Argumentation:

The HR department's shadow systems are mostly placed around moderate risk and moderate to high business value.

This typically means HR is using third-party or self-developed tools for recruitment, employee data management, or training analytics.

These tools clearly increase efficiency and support HR operations, but because they handle sensitive personal information, they require consistent IT supervision and data protection policies.

Instead of removing them, HR systems should be regularly reviewed, documented, and approved by IT.

This approach maintains HR's agility and innovation, while ensuring compliance with data privacy regulations and preventing potential data leaks.

In summary:

➡️ Valuable tools for HR efficiency → keep them.

➡️ Moderate risk due to personal data → monitor and secure them.

➡️ IT support and employee training will reduce risks.

Admin Systems

Decision: Eliminate

Detailed Argumentation:

The administrative systems have low business value but moderate to serious risk.

These might include unauthorized tools for document storage, messaging, or tracking internal tasks, which duplicate functions already covered by official IT platforms like SharePoint or Teams.

Because they do not significantly improve efficiency but create unnecessary security vulnerabilities, maintaining them wastes both IT and administrative resources.

The best course of action is to phase out or eliminate these tools and guide users toward approved corporate solutions that are safer, better integrated, and easier to maintain.

In summary:

➡️ Low added value → not worth the risk.

➡️ Replace with official tools to ensure consistency and security.

Supply Systems

Decision: 🔁 Improve and Integrate

Detailed Argumentation:

The supply chain systems provide very high business value, but also show serious risk levels due to poor data integration, uncoordinated updates, or reliance on manual processes.

Since supply data is crucial for inventory management, production, and logistics, these systems cannot be eliminated — but they must be standardized and integrated into the company's main IT architecture.

Improving the system means:

- Establishing a clear data architecture and integration interface (APIs, automated ETL).
- Ensuring data consistency across all supply-related systems.
- Gradually integrating them under IT governance while preserving flexibility for business users.

In summary:

➡️ High strategic value → must stay.

➡️ Improve governance and data quality.

➡️ Long-term goal: full integration into the enterprise data environment.

Store 1 System

Decision: 🔁 Improve / Integrate

Detailed Argumentation:

The Store 1 shadow system shows serious risk but high business value, likely being a locally developed reporting or sales-tracking tool that helps the store operate efficiently.

While valuable for day-to-day decision-making, it exposes the organization to security, backup, and data synchronization risks.
It should not be removed — instead, it should be brought closer to the IT environment by improving data sharing protocols, setting up secure connections, and ensuring proper version control and documentation.
In summary:

➡️ Keep for operational use.

➡️ Gradually integrate to reduce security risk.

➡️ Maintain flexibility but ensure IT visibility.

Store 3 System

Decision: Eliminate
Detailed Argumentation:
The Store 3 system ranks very high on risk but provides little measurable business value.
It could be an unauthorized app or communication tool that duplicates functions already provided by corporate systems.
Because it contributes little to business goals while increasing the potential for data breaches, inefficiencies, and compliance issues, it should be completely phased out.
In summary:

➡️ High risk, low reward → eliminate immediately.

➡️ Replace with official, standardized solutions.

Store 4 System

Decision: Embrace and Support
Detailed Argumentation:
The Store 4 system holds moderate business value and serious risk, suggesting it is locally useful but not yet properly managed.
It helps store employees access data or perform analyses quickly, improving performance.
However, because it may lack proper backup, authentication, or security, IT needs to monitor and support it.
This system can be kept operational as long as it's brought under light governance, such as implementing secure logins, version control, and scheduled data validation.
In summary:

➡️ Provides real operational value.

➡️ Moderate risk → manageable with IT oversight.

➡️ Keep but formalize governance and security.

General Argumentation:

1. Eliminate

    Detailed Argumentation:

    This shadow system poses significant business risks while offering limited strategic or operational value.

    Its existence often leads to data fragmentation, non-compliance with security or privacy regulations, and inefficient duplication of officially supported systems.

    Because the system operates outside IT control, there's no guarantee of data integrity, backup, or access management, creating potential vulnerabilities.

    Given that its benefits do not outweigh the costs and risks, it should be gradually eliminated and its functions either migrated to approved tools or discontinued.

    This ensures consistency, reduces complexity, and strengthens overall governance and security posture.

    ✅ Typical Triggers for Elimination:

    - High risk, low or unclear business value.
    - Creates security or compliance vulnerabilities.
    - Duplicates existing official systems.
    - Maintained by one person (knowledge risk).
    - Hard to support or scale.

2. Improve

    Detailed Argumentation:

    This system provides clear operational benefits, such as improving workflow efficiency or decision-making speed, but it suffers from technical weaknesses or governance gaps.

    Typical problems include manual data handling, inconsistent data definitions, limited scalability, or lack of audit trails.

    Rather than replacing it, the organization can achieve greater impact by targeted improvements — for example, automating data updates, adding validation checks, improving documentation, or securing user access.

    This strategy retains the business value while reducing risk, ensuring the tool becomes more robust, compliant, and maintainable.

    Typical Triggers for Improvement:

    - Moderate business risk, moderate-to-high business value.
    - System is widely used but unstable or insecure.
    - Improvement is cheaper and faster than replacement.
    - Users rely on it but IT oversight is limited.

    Example Phrase:

    "The current tool effectively supports the sales team's forecasting, but lacks data validation and user access control. With moderate risk and high value, targeted improvements in automation and governance are recommended."

3. Integrate into Official IT

    Detailed Argumentation:

    The shadow system demonstrates high business value and has become essential to daily operations, but it exists outside the organization's IT governance framework.

    This introduces security, maintenance, and compliance risks, as IT has no oversight over its architecture, backups, or updates.

Given its criticality, the recommended approach is to integrate it into the official IT environment.

This includes transferring data to managed servers, assigning IT ownership, standardizing access policies, and ensuring compatibility with the company's BI and ERP systems.

Integration allows the organization to retain its innovative features and data insights while ensuring full compliance and long-term sustainability.

Typical Triggers for Integration:

- High value, high risk.
- System is critical to business performance.
- Needed enterprise-wide.
- Integration cost < potential damage of non-compliance.

4. Embrace and Support

Detailed Argumentation:

This system is a successful local innovation that adds measurable value to business operations.

It is generally low to moderate risk, as it may already align with company policies or involve non-sensitive data.

Instead of discouraging its use, management should recognize its positive impact, formally endorse it, and provide basic IT support (such as user training, security monitoring, or API connections to core systems).

This approach encourages bottom-up innovation, improves employee engagement, and ensures that these tools are used responsibly and securely within the broader IT ecosystem.

Typical Triggers for Embrace & Support:

- Moderate or manageable risk.
- Clear value at team or business-unit level.
- Encourages innovation and efficiency.
- Low cost to support and maintain.

5. Keep As-Is

Detailed Argumentation:

This system already operates within governance standards, delivers consistent value, and poses minimal business risk.

It is well-documented, maintained, and aligned with the organization's architecture and data policies.

Since it already meets performance and compliance expectations, no major interventions are needed.

Periodic monitoring, updates, and user feedback will ensure continued reliability and effectiveness.

This "keep" strategy allows the organization to focus resources on higher-risk areas without disrupting a stable and efficient process.

Typical Triggers for Keeping:

- Low risk, high stability, high alignment.
- No major compliance or performance concerns.
- System is standardized and well-managed.