WHITE PAPER

How to Manage IT Regulations with an EA Management Tool for Financial Institutions

LeanIX

WHITE PAPER

How to Manage IT Regulations with an EA Management Tool for Financial Institutions

CONTENT

LeanIX

Introduction

Financial institutions worldwide can benefit from aligning to government IT regulations via tools built for collaboration-based enterprise architecture (EA) programs. This is largely due to the ecosystems of integrated customer data that underscore today's modern banking services — the likes of which require superior pathways between compliance and IT architecture teams to protect.

LeanIX, a software-as-a-service platform used to map and optimize complex interdependencies in data and technology landscapes, is leveraged by many enterprises in the industry to standardize IT architectures according to precise regulatory frameworks while simultaneously pursuing more digitally-enabled services. Both in terms of managing risk and simplifying IT systems, the LeanIX EA Management tool streamlines information-gathering across siloed organizational units to initiate on-demand IT compliance reports and architectural models. These reports and models offer advantages to all stakeholders responsible for ensuring digital infrastructures adhere to finance regulations, and when paired with LeanIX's configurable data repository, can stimulate actionable forms of transparency to aid during and in advance of audit procedures.

This white paper will demonstrate how traditional and cloud-native financial institutions can use LeanIX to faster map regulatory requirements and assess IT landscapes. Further, it will showcase the collaborative functionality offered by LeanIX to help IT and business teams co-operatively build architectures geared equally towards data security and adaptability.

In this white paper, you will learn:

- **How an EA Management tool can help modernize IT infrastructures for financial institutions while creating efficient pathways for compliance and security teams.**
- **How to accelerate data security and IT compliance with enterprise-wide support.**
- **How to leverage automated reporting mechanisms to ensure the integrity, availability, and confidentiality of IT systems.**

Notable Finance and Banking Regulations that Impact IT

Nations and economic unions around the world impose varying degrees of control over how financial institutions must manage their IT infrastructures. As was the case even before the 2007-2008 global financial crisis, the chief priority among these regulatory bodies is ensuring that banking systems remain continually in service and capable of protecting consumer data — that is, without wholly restricting a holder's ability to develop competitive new offerings. In this current era of digital banking, IT and business managers from traditional and "FinTech" organizations alike must learn to adopt increasingly distributed and automated compliance strategies to perform reviews on decentralized customer journeys.

There are a number of notable regulations worldwide that are particularly reflective of the current obligations of today's compliance officers. Enterprise architects tasked with conforming fast-modernizing IT infrastructures in the finance industry will need to have some familiarity with these regulations in order to build a complete picture of their IT landscape.

Here is a glimpse of some of the more well-known regulations:

BAIT (Germany):
Germany's Supervisory Requirements for IT in Financial Institution (*Bankaufsichtliche Anforderungen an die IT*), or BAIT, came into force in 2017 to offer specific details on what operators of credit institutions must do to conform to IT security standards. Extending from IT strategy and governance to information risk management and outsourcing and external procurement, BAIT encompasses everything that Germany's bank managers must do to remain compliant.

GDPR:
The EU General Data Protection Regulation (GDPR) came into force in 2018 to reform data protection in Europe. The regulation forces all financial institutions that operate within the EU and process personal data to know exactly what, how, and where this information is stored. The GDPR has standardized data protection law across Europe in order to give individuals better control of their data, which, in the context of financial institutions, has meant pseudonymizing personal data and having concrete awareness of data flows across their various systems.

MaRisk (Germany):

Germany's MaRisk, or *Mindestanforderungen an das Risikomanagement*, is a detailed risk management framework for the county's banking institutions set out in the wider German Banking Act. Many elements of MaRisk emphasize the independence of dedicated risk control departments from a bank's overall organizational structure — right up to the management level.

PSD2 (EU member states):

The revised Payment Services Directive ("PSD2") entered into force in 2016 to update the first PSD rules concerning regulating European payment service providers. Its regulations are comprised of technical standards and rules relating to themes such as allowing third parties access to customer bank accounts via Application Programming Interfaces (APIs) to enable a more integrated ecosystem. Further, PSD2 has made it similarly possible for retailers to become Payment Initiation Service Providers (PISPs) and thereby directly take money from consumer accounts.

SOX (U.S.A.):

The United States' Sarbanes-Oxley Act of 2002 ("SOX") is a federal law that applies to all U.S. public companies. Of significant relevance for IT managers is the Act's requirement that CEOs and CFOs certify all financial statements within 90 days — a main driver for more real-time reports and automated information-gathering mechanisms. Further, on a topic adding another layer of complication is cloud-based migrations, a specific section in SOX discusses that public financial institutions must retain all paper and electronic details concerning sensitive financial records (e.g, instant messages, transactions, and email messages) for at least five years.

IT Strategy and Governance in Finance with LeanIX

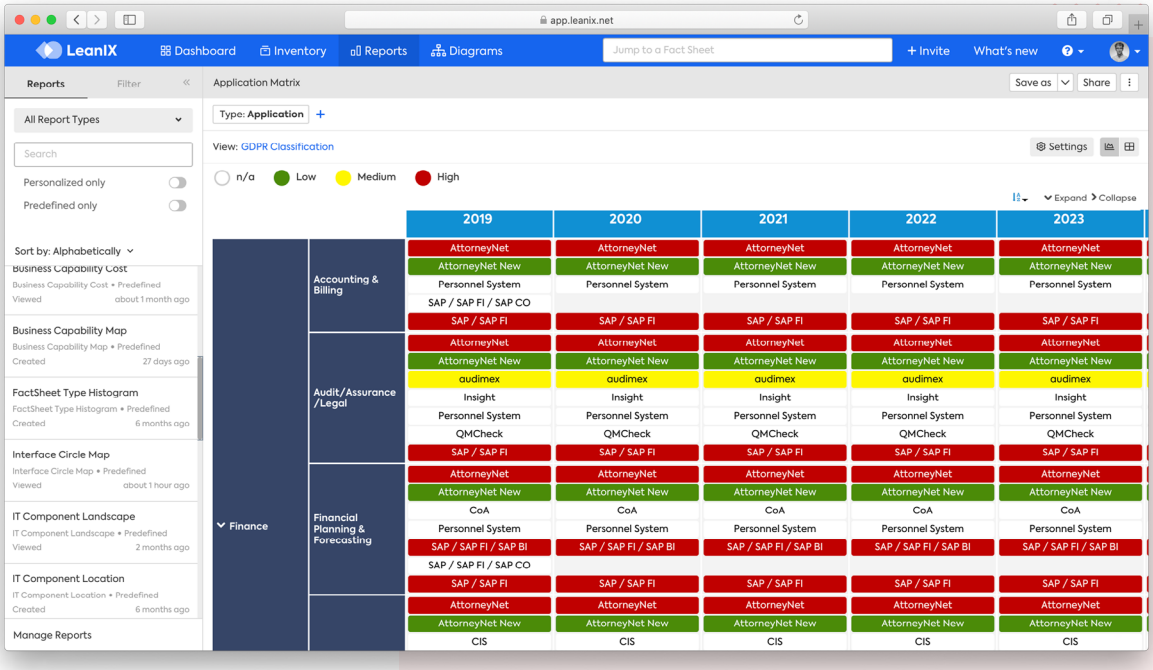
Senior IT and business leaders in the finance industry must possess clear lines of sight into the future arrangements of their IT systems. In so doing, all components within an IT infrastructure must be documented to define enterprise-wide technology standards and risk management protocols. This transparency is essential for performing executive-level assessments of IT landscapes and determining proportionate adjustments to compliance protocols based on operational considerations (e.g., company size, IT maturity level, etc.) and changing business objectives — which, in more cases than not, involve shifting current infrastructures to fit customer-centric business models.

The basis for such transparency in LeanIX rests in the tool's ability to provide overviews on technologies underlying business services — otherwise known as "business capabilities." The clarity of knowing exactly where and for what reason technology is used by a financial institution helps senior management prioritize risk assessments while also evaluating the long-term sustainability of any current or planned security protocol in relation to innovation agendas. For many bank and finance institutions running LeanIX workspaces, business capabilities are modeled after service landscapes set by Banking Industry Architecture Network (BIAN) framework standards.

In Figure 1, you can see the LeanIX Application Matrix report, a configurable report that connects business capabilities to their associated technologies. The LeanIX Application Matrix report can be viewed either by year or user group, and additional views such as "GDPR Classification" can be applied as overlays.

Figure 1

A LeanIX Application Matrix Report



Source: LeanIX GmbH

Capability-based insights into risk management and compliance reporting like that offered in the LeanIX Application Matrix report help senior IT and business leaders engage more fully in defining operational roles and responsibilities. In addition to business capabilities, many LeanIX reports can also be configured to display organizational processes — with all corresponding line managers and technology owners just a click away — to simplify reporting channels and better monitor security tests and compliance reviews. These reports can be distributed at ease among board members and to those heading risk committees.

Questions that can be answered with LeanIX

1. How should the application landscape per business capability develop strategically over time?
2. How is the IT strategy documented and communicated in your company?
3. Is the IT strategy concrete enough so compliance with it can be monitored?
4. Can executives access overviews of technology standards?

Information Risk and Security Management in Finance with LeanIX

In close co-operation with CIOs and CFOs and various other senior IT and business managers, the task of officiating IT policies and data regulations in financial institutions falls heavily on security and compliance officers. These employees are at the frontlines of aggregating data to determine whether a financial institution's organizational and technical resources adhere to agency regulations and local/federal laws. In today's complex market environments, this involves collecting data stored throughout distributed IT systems and composed via a multitude of interfaces and technologies — many of which incorporated, ad hoc, as a result of organic growth and mergers and acquisitions.

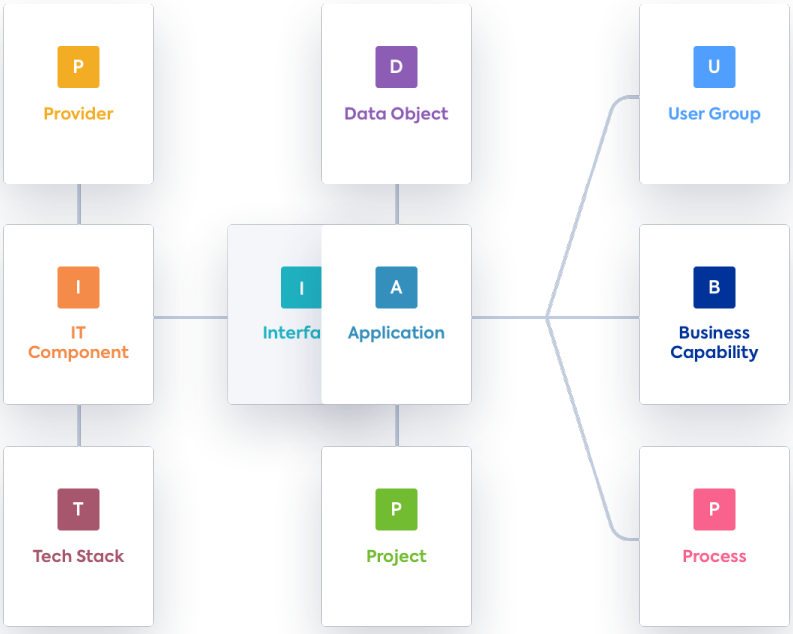
To accelerate uncovering and classifying data, LeanIX offers security and compliance officers the following collaboration-based functionality when aligning IT landscapes to external regulations or internal policies.

Subscription-based "Fact Sheets"

LeanIX disperses data collection to manage knowledge resources and IT landscapes while implementing fail-safe accountability measures. To do so, stakeholders are assigned varying degrees of ownership over the upkeep of "Fact Sheets" — the individual repositories used to document information regarding any individual architectural object. Even auditors and regulators themselves can be given read access to the systems to freely access the information needed, and their inputs can thereafter be directly communicated and stored in the LeanIX system.

Information contained within LeanIX Fact Sheets power LeanIX's out-of-the-box reports, and by subscribing to LeanIX Fact Sheets themselves or at the request of IT security and compliance officers, collaborators can be contacted via manual or automated mechanisms to provide data related to their services. Of note, there are ten LeanIX Fact Sheet templates, each of which corresponding to the ten core elements of the LeanIX data model.

Figure 2
The data model of the LeanIX Enterprise Architecture Suite

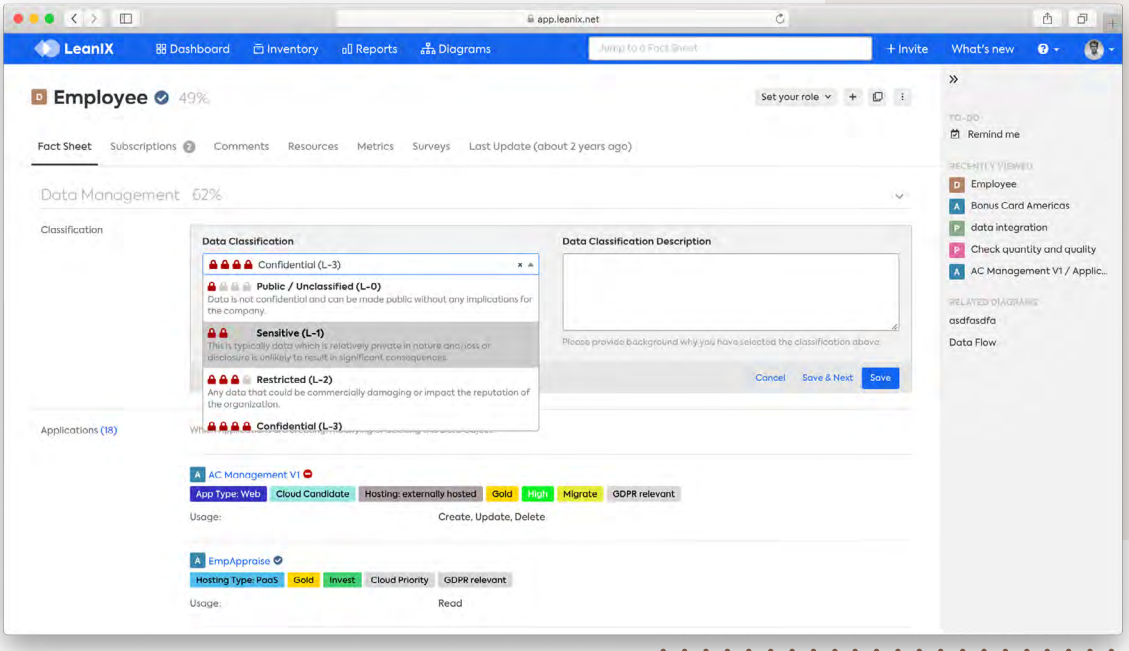


Source: LeanIX GmbH

Inside LeanIX Fact Sheets, IT security and compliance officers can access information relating to an IT entity's data management (e.g., "Data Objects", "Provided Interfaces", "Consumed Interfaces"), sourcing (e.g., "Technical Fit", "IT Components"), business support ("Business Criticality & Functional Fit", "Business Capabilities", "Processes", "User Groups"), and assortments of general information (e.g., "Name & Description", "Lifecycle"). If required, these fields and names can be altered to enterprise-specific naming conventions using LeanIX Self-Configuration.

Of particular importance to IT security and data compliance officers, LeanIX Fact Sheets for Data Objects are embedded with dedicated fields for grading data classification according to the following:

Figure 3
A LeanIX Data Object Fact Sheet



Source: LeanIX GmbH

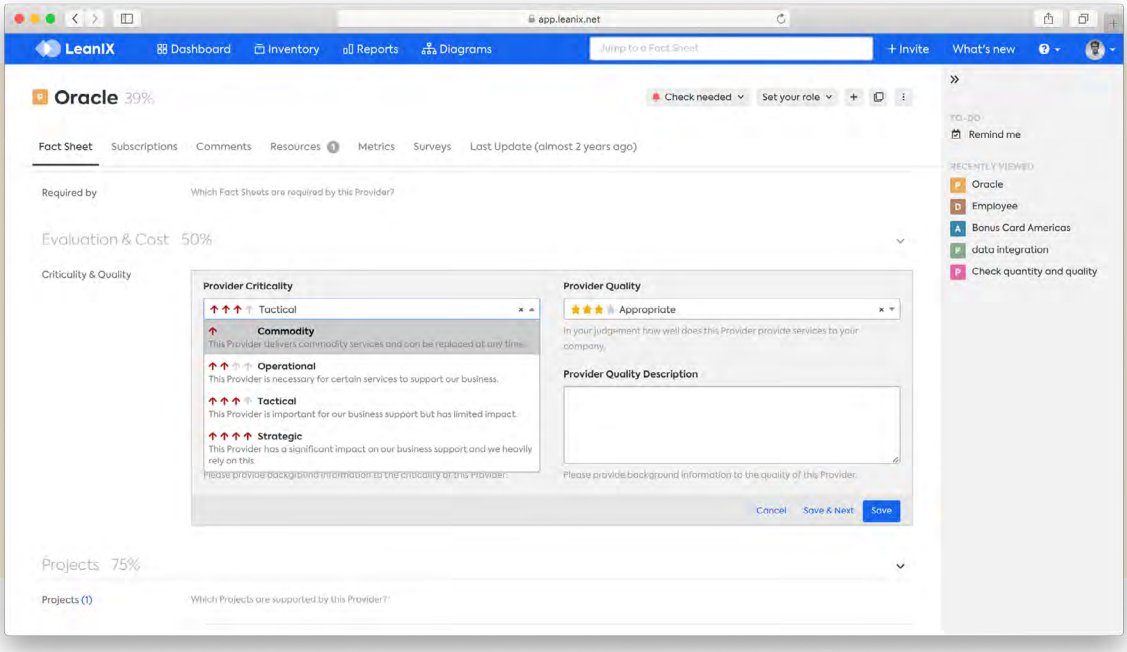
Data Classification

- **"Public / Unclassified (L-0)":** Data is not confidential and can be made public without any implications for the company.
- **"Sensitive (L-1)":** This is typically data which is relatively private in nature and loss or disclosure is unlikely to result in significant consequences.
- **"Restricted (L-2)":** Any data that could be commercially damaging or impact the reputation of the organization.
- **"Confidential (L-3)":** Any data that may adversely affect individuals or the business of the organization.

A similar evaluation rubric is embedded within LeanIX Fact Sheets for Providers, one designed to assess the criticality *and* quality of technology providers:

Figure 4

A LeanIX Provider Fact Sheet



Source: LeanIX GmbH

Provider Criticality

- **"Commodity":** This provider delivers commodity services and can be replaced at any time.
- **"Operational":** This provider is necessary for certain services to support our business.
- **"Tactical":** This provider is important for our business support but has limited impact.
- **"Strategic":** This provider has a significant impact on our business support and we heavily rely on this.

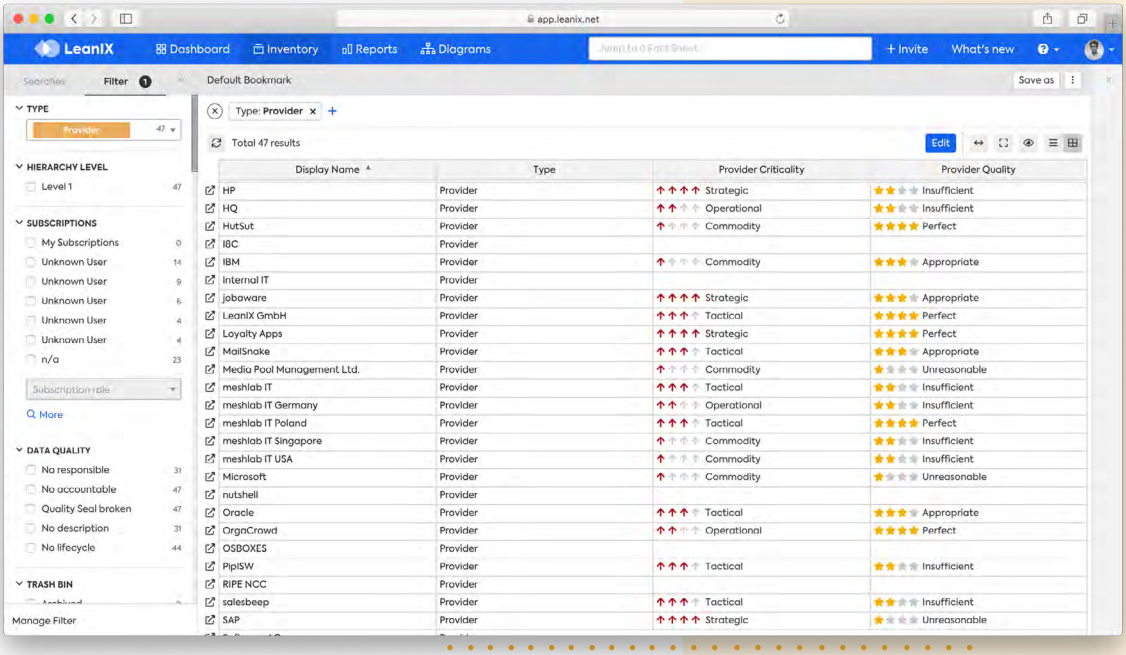
Provider Quality

- **"Unreasonable":** The service quality of this provider has a remarkably negative impact on our business.
- **"Insufficient":** The services of this provider have a negative impact on our business.
- **"Appropriate":** The service delivery is always as defined and business contirbution is positive.
- **"Perfect":** Service delivery is always of a very high quality and no disruptions have been experienced.

Among many options in LeanIX for obtaining quick and clean overviews of compliance-sensitive IT entities, the varying levels of provider criticality and data classification in an IT landscape can be seen as a table. Such tables can also be used to determine whether application and security managers are in place to oversee the day-to-day upkeep of IT entities.

Figure 5

A table view of a LeanIX inventory

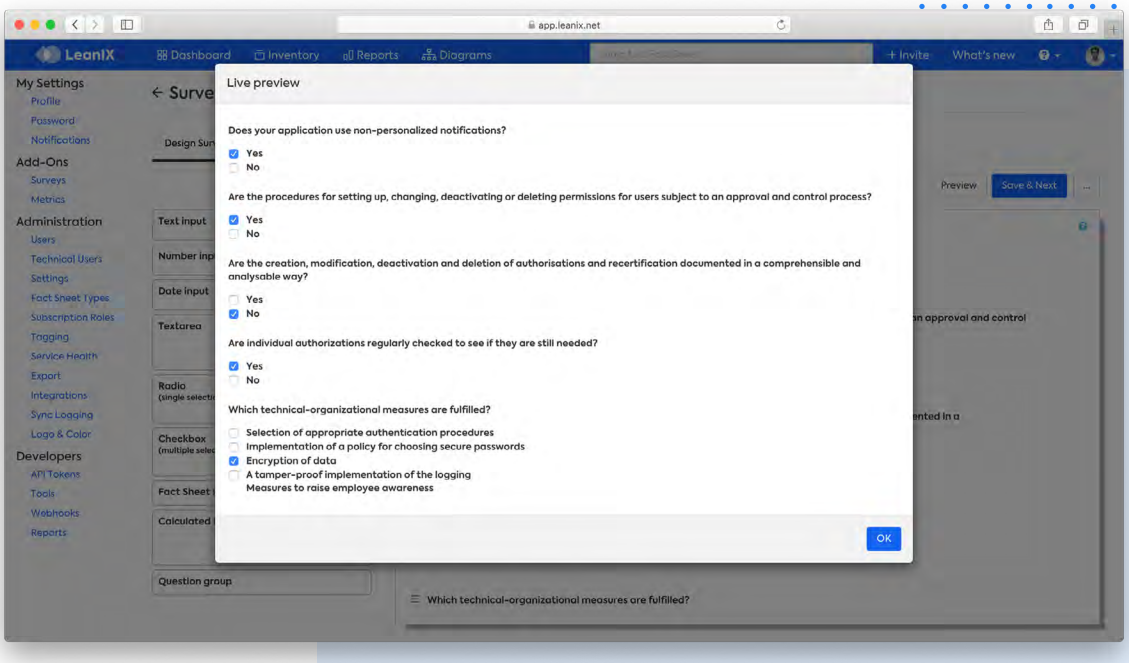


Source: LeanIX GmbH

LeanIX Surveys

To spur data contribution or field specific concerns on the integrity, availability, or confidentiality of IT systems, LeanIX Surveys can be sent to stakeholders inside or outside a financial institution's LeanIX network in easy-to-execute formats. LeanIX Surveys can be assembled using templates or made wholly from scratch based on whatever questions need answering, and the results can be set to arrive directly inside LeanIX Fact Sheet (with the data it replaces being put inside backlogs to provide audit trails). To benefit IT security and compliance officers, a "calculated field" function can be added to LeanIX Surveys to tally and compute numerical figures.

Figure 6
A LeanIX Survey



Source: LeanIX GmbH

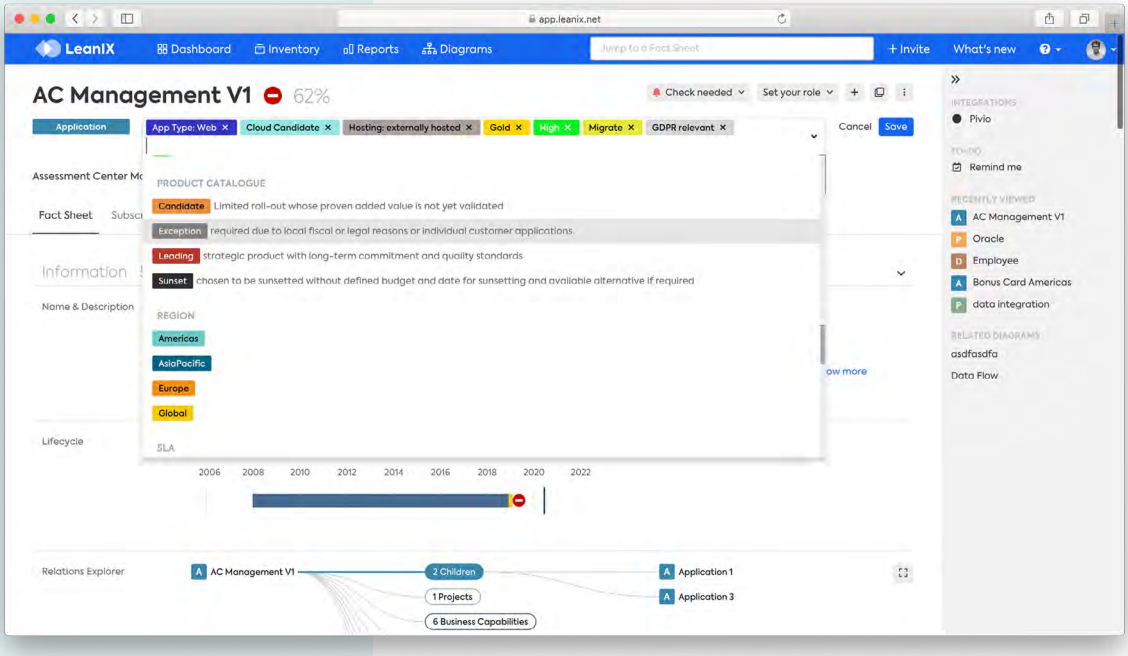
LeanIX Tags

In addition to the quality assurance fields embedded to LeanIX Fact Sheets, all IT entities stored within the LeanIX inventory can be labelled (or "tagged") with attributes chosen by IT security and compliance officers themselves. These tags can be filtered for when navigating through the LeanIX inventory or incorporated directly into LeanIX reports to generate more finely-grained analytics.

LeanIX tags offer financial institutions worldwide an opportunity to categorize IT assets and IT projects in relation to specific policies set forth by national regulatory bodies. A common use case for LeanIX tags is differentiating information assets during cloud-based migration strategies and determining whether appropriate policies — based perhaps on enterprise-specific best practices or industry standards — are in place.

Figure 7

Applying custom-made tags to LeanIX Fact Sheets



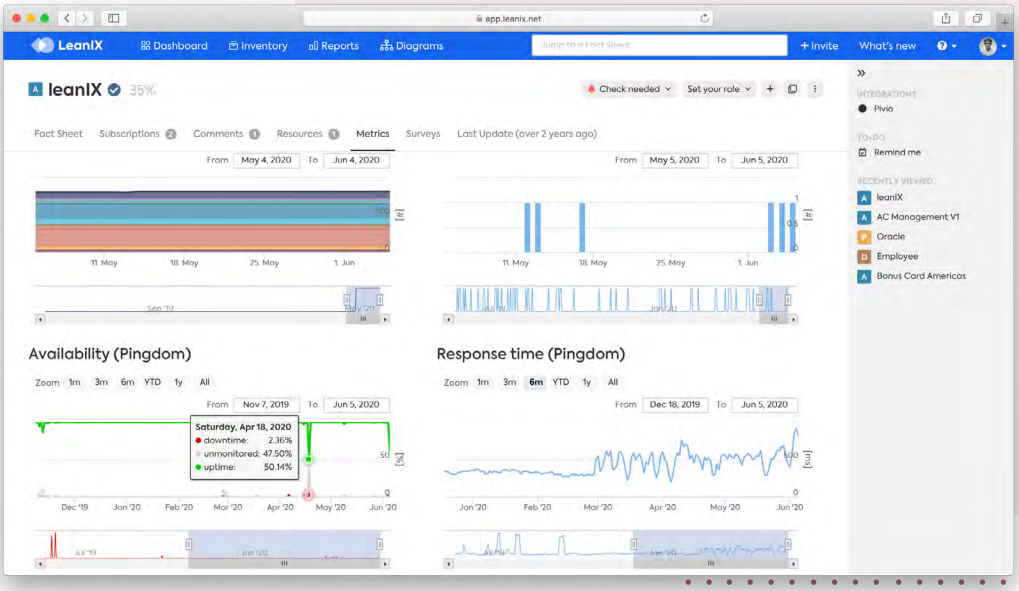
Source: LeanIX GmbH

LeanIX Metrics

Security and data officers can leverage real-time LeanIX Metrics when looking to classify IT entities within the context of larger compliance frameworks. Whether in terms of availability, response times, and interface transaction volumes, time-related data on an IT entity can be linked to LeanIX Fact Sheets or displayed in LeanIX reports via the LeanIX Metrics REST API.

Such streams of live data let security and compliance officers look beyond general information such as lifecycle data when drafting disaster recovery solutions by ensuring that applications are truly both compliant and dependable. LeanIX Metrics are not meant to replace the tools where data is sourced from but rather to aggregate information for LeanIX to observe it from within a wider business context.

Figure 8
LeanIX Metrics



Source: LeanIX GmbH

Questions that can be answered with LeanIX

1. How are technical standards selected? How often are they reviewed?
2. What criteria is used to evaluate technology — and are evaluations documented?
3. How are the standards communicated?
4. How is compliance monitored?
5. How do stakeholders receive an overview of which standards are used in the company?

IT Projects and Application Development with LeanIX

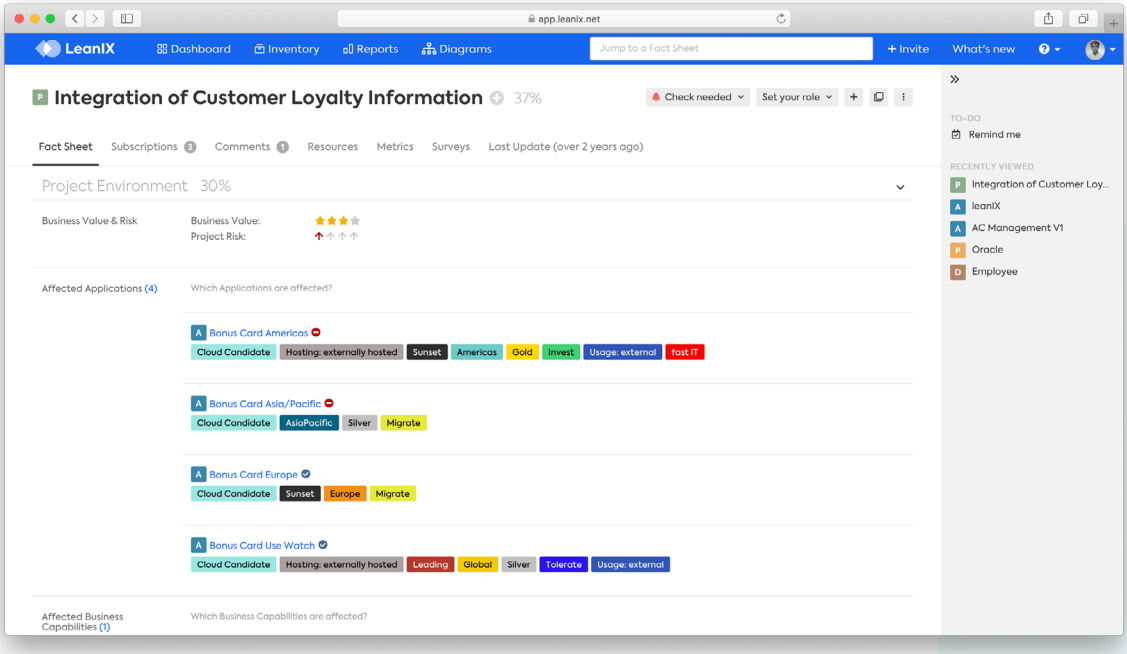
LeanIX provides enterprise architects in the finance sector with functionality to build holistic overviews of IT landscapes wherein systemic vulnerabilities can be monitored by stakeholders like security and data compliance officers. Its interactive solutions help architects and non-architects alike visualize fault lines between data connections and anticipate the adverse effects of IT projects and application on compliance efforts — all of which in ways more accessible, automated, and intuitive than Excel- or Visio-based methods.

Complete Documentation of IT Project Environments

In particular, not only can LeanIX Fact Sheets store both foundational and user-defined attributes of IT applications, but IT projects themselves can be documented alongside the very components that will be affected in an IT system as a result. These include: “Affected User Groups”; “Affected Processes”; “Affected IT Components”; “Affected Business Capabilities”; and “Affected Applications”. As well, using embedded tables similar to what’s available in LeanIX Fact Sheets for Providers and Data Objects, projects can be graded in terms of both “Business Value” and “Project Risk”, the results of which can be easily discovered in the LeanIX inventory and filtered for in addition to other qualities.

Figure 9

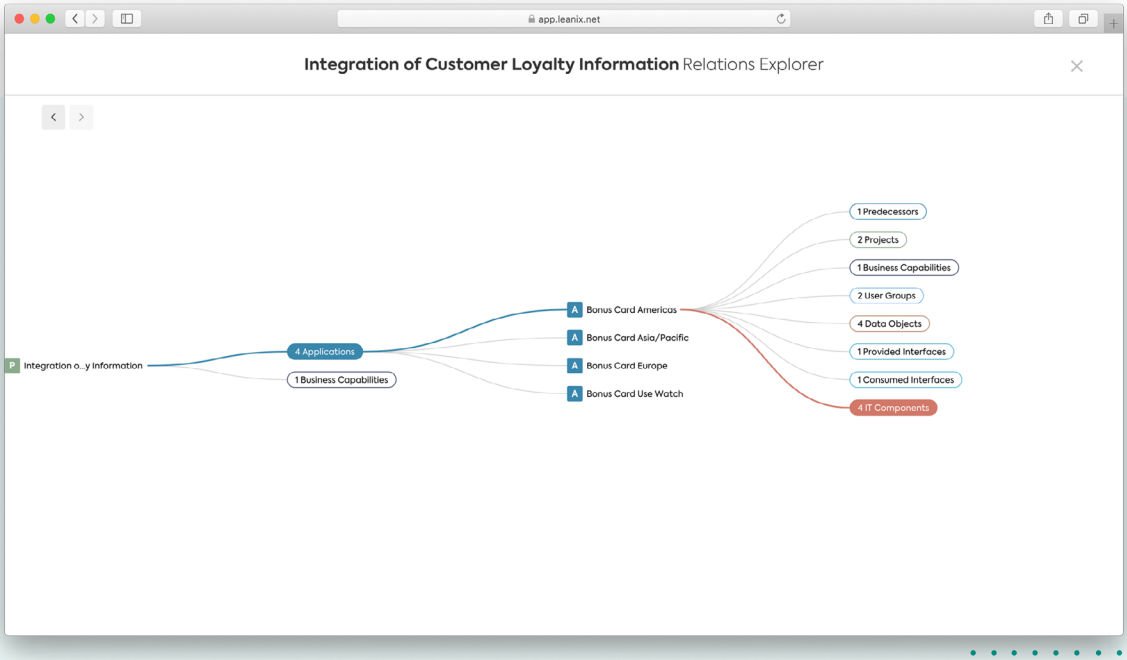
A LeanIX Project Fact Sheet



Source: LeanIX GmbH

The components in an IT system affected by any given IT project can also be examined from the LeanIX Relations Explorer, a fully-interactive and 360-degree way to observe dependencies across IT landscapes. The LeanIX Relations Explorer can be accessed directly from a LeanIX Fact Sheet.

Figure 10
The LeanIX Relations Explorer



Source: LeanIX GmbH

Of note, LeanIX Project Fact Sheets can be utilized to expedite recurring compliance reviews such as license management by simply connecting it to each of the applications under inspection.

Impact Analysis and Technology Roadmaps

Any attempt to modernize one service to meet heightened regulatory standards can inadvertently jeopardize the performance of another. Or, alternately, whenever customer data is channeled through a new application interface, security concerns pique and architectural analysis becomes required. In these cases, LeanIX offers a range of configurable reports such as technology/project roadmaps, heat maps, and application interface reports to assess IT landscapes with high-level or granular views.

Figure 11

A LeanIX IT Component Roadmap

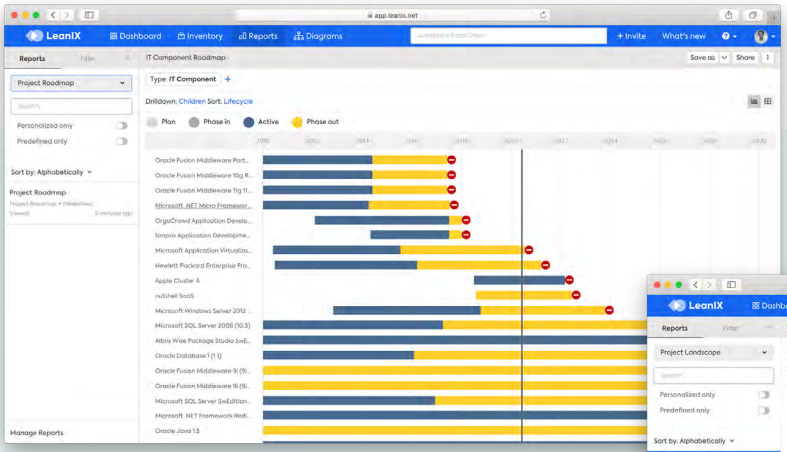


Figure 12

A LeanIX Project Roadmap

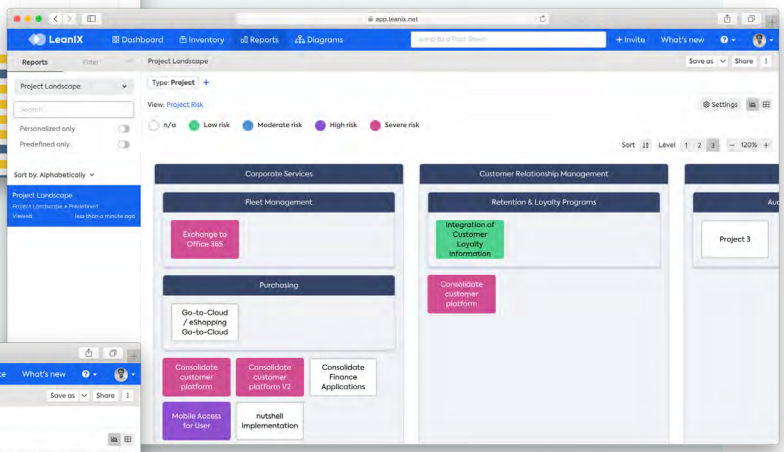
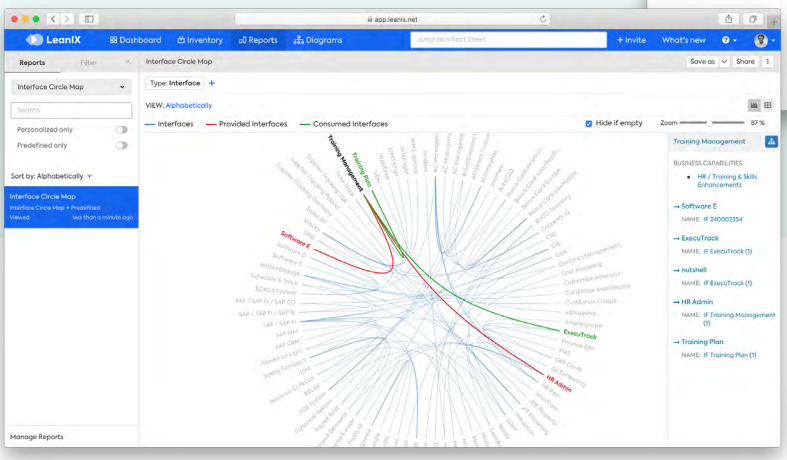


Figure 13

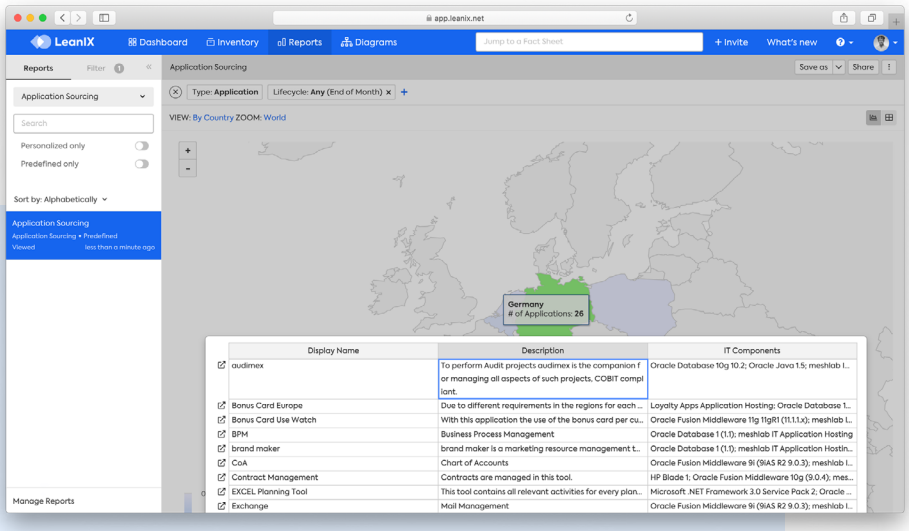
A LeanIX Interface Circle Map



Source for all figures: LeanIX GmbH

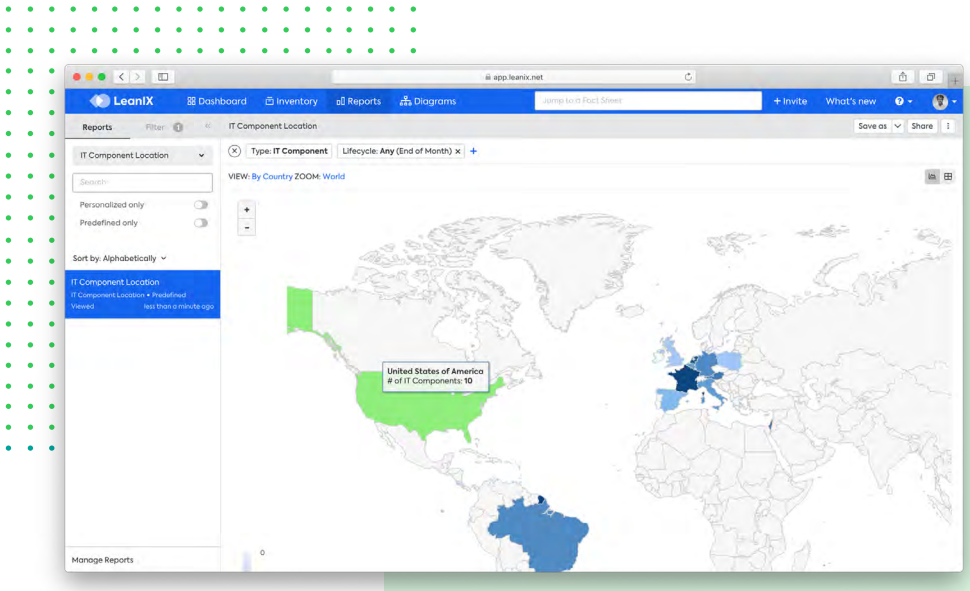
IT Component Outsourcing

Of increasing importance in the age of decentralized IT systems, compliance teams in financial and banking institutions must be able to adequately map third-party providers tied to critical functions. Among other requirements, the European Banking Authority (EBA), for example, mandates that finance groups with critical services outsourced to external groups periodically test business contingency plans in case these services become discontinued. To ensure this happens with any degree of repeatability, LeanIX provides out-of-the-box options such as the LeanIX Application Sourcing and LeanIX IT Component Location reports — both highly configurable and visual supplements when applying stress tests on third-party services.



Source: LeanIX GmbH

Figure 14
A LeanIX Application Sourcing report

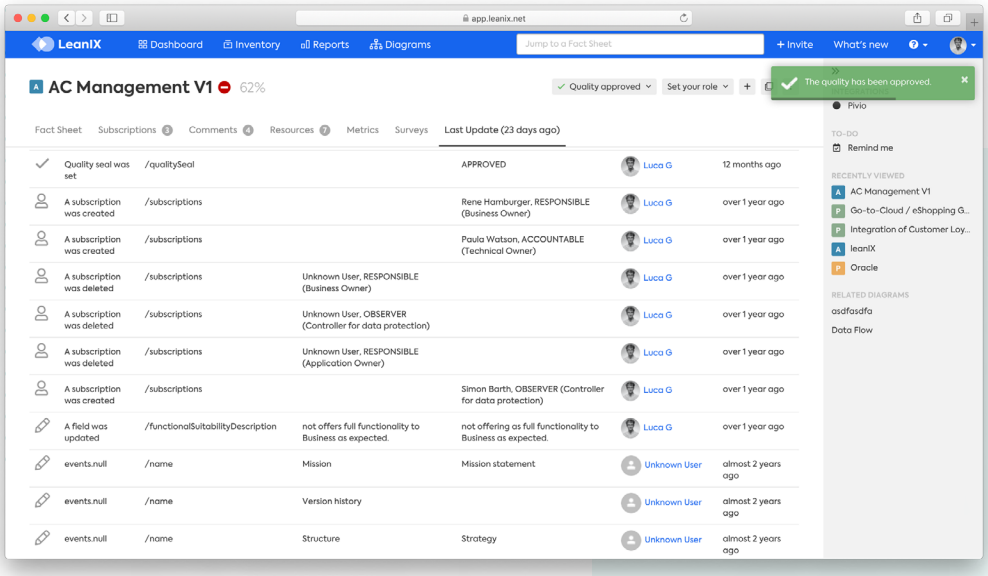


Source: LeanIX GmbH

Figure 15
A LeanIX IT Component Location report

Traceability

Changes made to any IT entity stored in LeanIX are immediately documented within LeanIX Fact Sheets. This traceability can be leveraged to help financial institutions assemble audit logs of IT activities and demonstrate active compliance efforts. Further, to reinforce the reliability of all data stored or modified within LeanIX Fact Sheets, LeanIX Quality Seals can be applied to issue scheduled maintenance checks for stakeholders. A broken LeanIX Quality Seal triggers a call to action for those subscribed and can work in conjunction with a LeanIX Fact Sheet's "Last Edit Date" (i.e., the data/time of the most recent update). The LeanIX Quality Seal will similarly break and release a notification if the wrong user changes a LeanIX Fact Sheet field.



Source: LeanIX GmbH

Figure 16
A history of changes to a LeanIX Fact Sheet

Questions that can be answered with LeanIX

1. Do you run all applications exclusively in your own data centers?
2. Do you use a CMDB to manage the components? If so, which ones?
3. Which IT applications use technologies that have already left the manufacturer lifecycle?
4. Which IT components need to be replaced soon?
5. Which applications are not technically fit for supporting API banking?
6. Which projects may need additional oversight to minimize risk?
7. Which IT component providers are considered strategic?

Summary

The generic requirements for IT management set out in frameworks such as COBIT are analogous to the regulations that many financial institutions must adhere to worldwide. As a result, the configurability of EA management tools such as LeanIX are perfectly suited to document the many categories of assets found in banks via both user-defined and tool-based templates. Moreover, LeanIX's ease-of-access equips financial institutions with the means to proliferate IT compliance efforts throughout organizational units and integrate its practice into the daily routines of users.