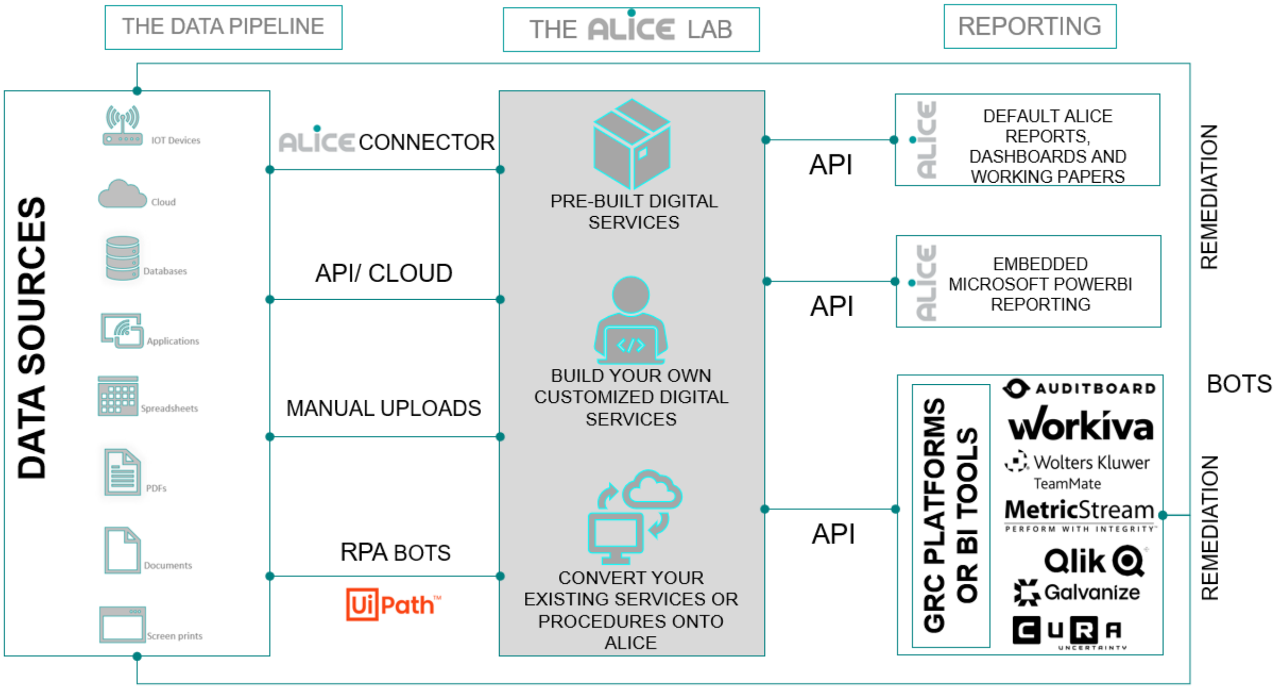
Meet ALICE

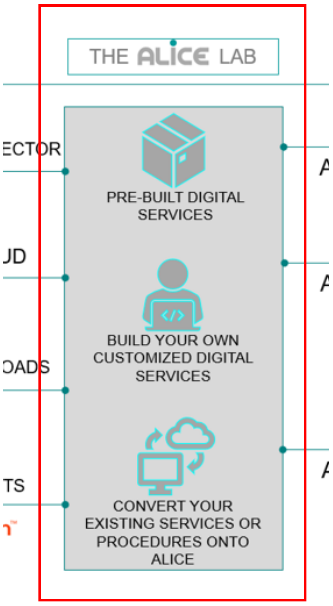
ALICE is a platform that enables those charged with governance to digitalize the management and monitoring capabilities of their business. She combines intelligent automation with cognitive services to create an ecosystem of digital services which provide continuous visibility of her monitoring outcomes and test results in a near real-time and remote manner globally and at scale. In short, ALICE's purpose is to deliver always-on audit, always on compliance and always-on peace-of-mind.

How does ALICE work?

ALICE can collect data from any source through her Data Pipeline. Digital services are developed in the ALICE Lab and applied to the data collected resulting in monitoring outcomes and/or test results. These outcomes and/or results are then reported in auto-populated and standardized working papers and default dashboards. The drill down functionality embedded within ALICE allows users to review findings to the minutest detail. These outcomes and/or results can also be interrogated by users in Microsoft's PowerBI which is embedded within the ALICE platform. Alternatively, the outcomes and/or results can be ingested and/or integrated into other governance or business intelligence tool(/s) of choice.

The ALICE platform is illustrated simply below.




THE ALICE LAB
ECTOR
JD
OADS
TS
PRE-BUILT DIGITAL SERVICES
BUILD YOUR OWN CUSTOMIZED DIGITAL SERVICES
CONVERT YOUR EXISTING SERVICES OR PROCEDURES ONTO ALICE

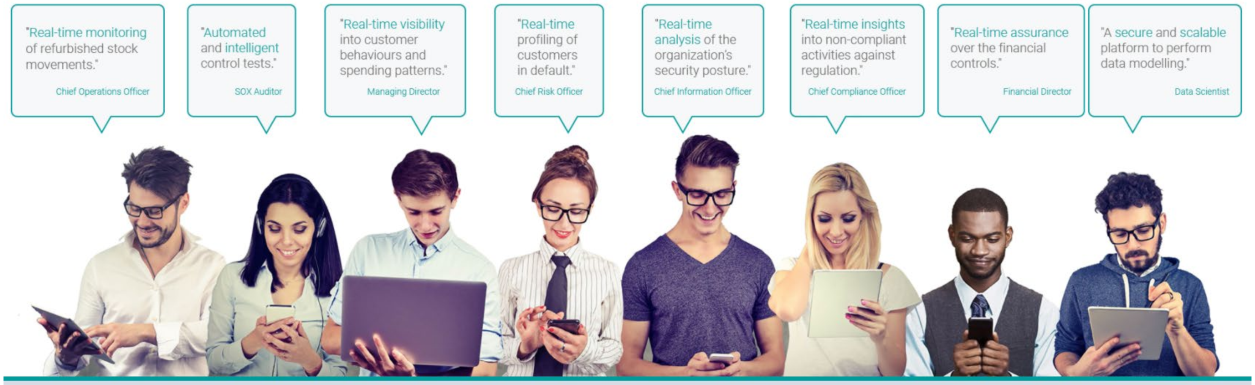
Pre-Built Digital Services - The ALICE platform comes standard with some pre-built digital services, namely digital IT audit procedures, that can be deployed and run in any environment. The purpose of these pre-built digital IT audit procedures is to demonstrate value quickly and in a cost-effective manner without any upfront investment in time and money in building customized digital audit procedures. Please see Annexure A for a list of the pre-built digital IT audit procedures.

Custom-Built Digital Services - The ALICE Lab allows for customized digital services to be built according to your business needs and audit or compliance methodologies. These customized digital services can relate to any business discipline (not only IT) and can be run according to a schedule per the business needs and or annual audit or compliance plans.

Converted Services or Procedures - The ALICE Lab also allows for management or auditors, hereinafter referred to as stakeholders, to bring their own services or procedures, for example, in the form of scripts, and digitalize them on the ALICE platform allowing them to be automatically run in a remote and near real-time manner on fully managed and scalable infrastructure.

Who can ALICE help?

No matter which stakeholder you are in the organization, ALICE can help.


"Real-time monitoring of refurbished stock movements."
Chief Operations Officer
"Automated and intelligent control tests."
SOX Auditor
"Real-time visibility into customer behaviours and spending patterns."
Managing Director
"Real-time profiling of customers in default."
Chief Risk Officer
"Real-time analysis of the organization's security posture."
Chief Information Officer
"Real-time insights into non-compliant activities against regulation."
Chief Compliance Officer
"Real-time assurance over the financial controls."
Financial Director
"A secure and scalable platform to perform data modelling."
Data Scientist

For the **Managing Director**, digital services may mean gaining visibility and insight across the different business disciplines in order to make informed business decisions and advise the organization's stakeholders accordingly.

For the **Chief Compliance Officer**, digital services may mean intelligently automating the assessment and reporting of compliance against, for example, legal and regulatory standards, occupational health and safety requirements or organizational policies and procedures.

For the **Sarbanes Oxley Auditor**, or any auditor for that matter, digital services may mean digitalizing audit procedures to provide more assurance with the same or less human effort. More assurance may translate to more scope and coverage provided in a more intelligent, real-time, continuous, automated and value-adding manner.

For the **Data Scientist**, digital services may mean harnessing the power of a platform to be able to scale and provision infrastructure to be able to model and analyze volumes of data without being concerned about versioning, privacy, auditability and security of the data. Sharing and re-use of digital services by the Data Science team may also encourage collaborative economy of brainpower, data assets, procedures and outcomes within the organization and potentially even beyond.

For the **Chief Risk Officer**, digital services may mean intelligently automating the assessment, profiling and mitigation of risks identified across the organization in a continuous and real-time manner. Digitalization of the risk monitoring process could range from reporting transactions above specified regulatory thresholds to assessing loss ratios and claim philosophies against industry norms.

For the **Chief Operations Officer**, digital services may mean digitalizing the mechanisms of overseeing the operational and administrative functions of the different business disciplines. These mechanisms may include dashboards exposing real-time and continuous information over business operations, workforce performance, control effectiveness and financial metrics.

For the **Chief Information Officer**, digital services many mean digitalizing the monitoring of the security hygiene and posture of the organization, ranging from recertification of users to patch management

For the **Financial Director**, digital services may mean gaining visibility and insight into the financial health of and effectiveness of the control functions across the organization. For the Financial Manager, digital services may mean intelligently automating reviews over, for example, journals, debtors aging, stock levels or reconciliations

Annexure A: List of Pre-Built Digital IT Audit Procedures

User Administration Digital Audit Procedures

1. User profile data accuracy (comparison of user lists from different systems to a human resource list);
2. Identification of duplicate usernames in a system;
3. Identification of multiple user profiles in a system;
4. Identification of generic user profiles (human vs non-human user profiles);
5. Identification of dormant user profiles;
6. Identification of inactive user profiles; and
7. Identification of terminated employees that still have access to systems.

Cybersecurity Digital Audit Procedures

Microsoft Baseline Network Configuration

8. Number of administrators are appropriately limited;
9. The local guest user profile on devices has been disabled;
10. Domain level auditing of security related events has been enabled;
11. Automatic logon has been disabled for all devices;
12. Windows systems do not use FAT or FAT32 file systems;
13. All local user profiles have passwords set to expire;
14. Anonymous user profiles have been restricted on the network; and
15. Network shares are appropriately limited.

Password Configuration

16. User profiles are locked out after five (or less) failed sign-on attempts;
17. Password history has been enabled to prohibit the re-use of the previous six (or more) passwords;
18. Password complexity is enforced;
19. Password complexity rules enforce the use of upper- and lower-case characters (e.g. a z, A Z);
20. Password complexity rules enforce the use of alpha, numeric and special characters (e.g. 0 9,!@#$%^&*()_+|);
21. A password length of at least eight characters or more is enforced;
22. The maximum password age is between 30 to 90 days;
23. The minimum password age is 48 hours or more;
24. All user profiles have passwords set to expire;
25. User profiles do not bypass password controls by having "Password Not Required" enabled on Active Directory; and
26. There are no active user profiles with passwords that have not been reset in over 90 days;

Patch Management

27. Application, operating and network level patches are up-to-date.