

# ENSURING REGULATORY COMPLIANCE WITH IT ASSET AND SERVICE MANAGEMENT

Practical insights for achieving compliance while maximizing the value of data assets.

March 28<sup>th</sup> 2024

Joel Eijssen - Senior Asset & Service Management Solution Consultant

## Pleased to meet you...



Joel Eijssen

SERVICE & ASSET MANAGEMENT SOLUTION CONSULTANT

opentext™

North Europe region

# opentext™

Opentext™ is one of the world's largest software companies, with +25 000 employees. We develop and deliver innovative software combining cutting-edge technologies like AI, analytics, and automation to streamline business processes, enhance collaboration and improve decision-making solutions for enterprise content management.

150M

End Users of  
our software

25,000

Employees

180

Countries

98

of Top 100  
Global  
companies are  
customers

30+

Years of  
experience in  
Asset & Service  
Management





**Greg Wells**

*Sr. Account Executive*



**Joel Eijssen**

*Lead Solution Consultant*



**Anders Heimdahl**

*Sales*



**Terje Mognes**

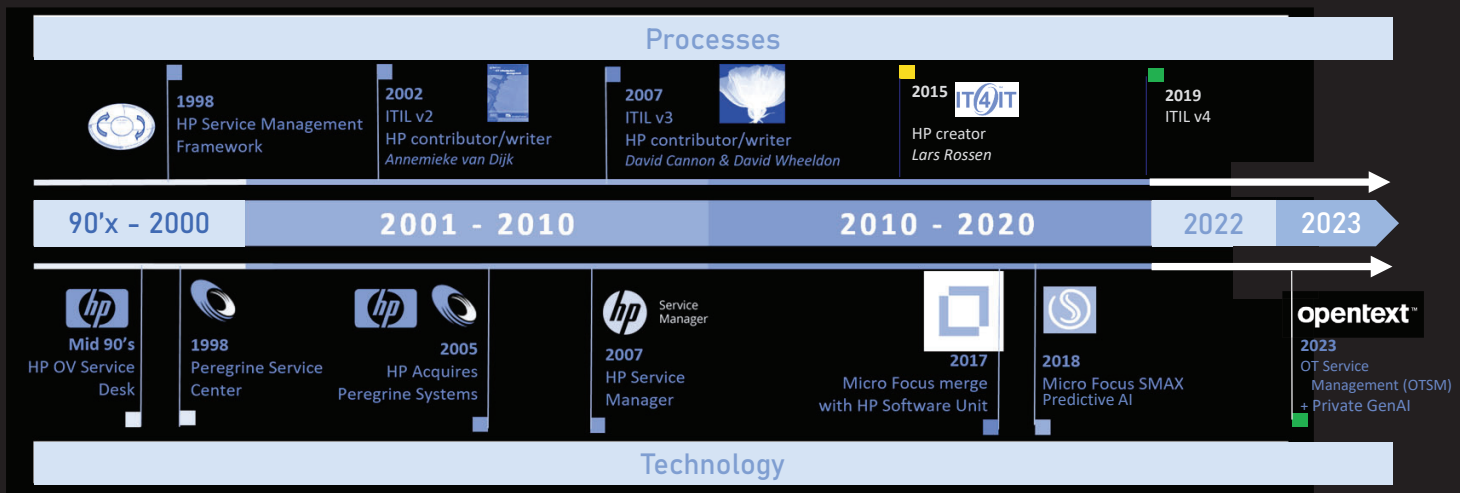
*Senior Sales Engineer*



OpenText

## 30+ Years Experience in IT Service & Asset Management

Service & Asset Management is in the opentext™ DNA





# Organizational and IT challenges



01

**Increasing regulatory and internal compliance requirements (e.g., NIS2, CRA, DORA)**



02

**Lack of visibility and control over IT assets**



03

**Security risks stemming from unmanaged or unknown assets.**



04

**Cost inefficiencies in IT Asset (Hard- & Software) and cloud resource management.**



openText

## Understanding EU Regulatory Compliance Requirements

Understanding a new era of European Union digital regulations

### NIS2



**What is it:** The Network and Information Security Directive (NIS2) replaces the original NIS. It aims to improve cyber security & resilience within the EU.

**When will it apply:** Each organization within scope of NIS2 must adhere to its requirements by Q4 2024.

**Who is in scope:** All operators of critical infrastructure and essential services in the EU. NIS2 has 15 sectors of business & industry in scope.

#### NIS2 details:

- Given its focus on critical infrastructure and essential services, many public organizations are in scope of NIS2.
- There are four main areas impacted by NIS2: Risk Management, Corporate Accountability, Reporting and Business Continuity & Crisis Management.
- There are other areas with impact and requirements, such as policies & procedures, and technical measures such as Multi-Factor Authentication (MFA), encryption, asset inventory, etc.
- NIS2 fines can reach €10 million or 2% of total worldwide turnover.

### DORA

**What is it:** The Digital Operational Resilience Act (DORA) strengthens IT security of financial organizations.

**When will it apply:** Each organization within scope of DORA must adhere to its requirements by January 17, 2025.

**Who is in scope:** Financial entities in the EU such as banks, insurance companies, investment companies, and their third-party (IT) service providers.

#### DORA details:

- Defines a strong minimum set of security requirements which apply to all financial organizations across the EU, and thus creating a widely adopted standard.
- (IT) Third parties that provide services to financial organizations must also adhere to stricter security requirements, which increases the effective reach of DORA.
- Higher testing requirements for effective measurement of IT & business resilience.
- DORA fines for financial organizations can reach 2% of total worldwide turnover. Critical third parties could be fined up to €5 million. Individuals can face fines up to €1 million.

### CRA

**What is it:** The Cyber Resilience Act (CRA) applies security requirements for hardware and software products with a digital element.

**When will it apply:** Products within scope of CRA must adhere to its requirements by ~2027.

**Who is in scope:** All producers and manufacturers of digital software and hardware products that are based in the EU or sell into the EU.

#### CRA details:

- Producers and manufacturers of digital goods must ensure security within the entire lifecycle of their product.
- More emphasis on secure by design and secure by default products and being able to prove this is the case.
- Examples of product types in scope: mobile devices, routers & switches, mobile apps, desktop applications, IoT devices, laptops and digital toys.
- CRA fines can reach €15 million or 2.5% of total worldwide turnover.

### AI Act

**What is it:** The Artificial Intelligence (AI) Act applies risk-based rules & requirements to AI systems and their usage.

**When will it apply:** AI systems must adhere to the requirements by around August 2, 2026, depending on the classification.

**Who is in scope:** All providers and operators of AI systems in the EU or providing services (using AI) within the EU.

#### AI Act details:

- It uses a risk-based approach. AI systems, and their usage is classified according to one of four levels: Unacceptable Risk, High Risk, Limited Risk and Minimal Risk. The requirements applied depend on the risk classification.
- Unacceptable Risk AI systems are prohibited.
- High Risk AI systems are subject to the most regulation (i.e., require a quality management system, impact assessments, logging & monitoring, central registration, etc.).
- AI act fines can reach €35 million or 7% of total worldwide turnover. The maximum fines are related to the risk classification.









# EU NIS2 Directive


The **Network and Information Systems 2 (NIS2) Directive** will improve the level of cyber security and resilience of critical organizations within the European Union.

NIS2 compared with the prior NIS version (initially released in 2016) requires that more organizations are in scope of the directive and must therefore adhere to its requirements. Further, NIS2 consolidates and standardizes the directive where NIS was fragmented between members states of the EU.

The four major NIS2 themes are:

-  **Board ownership & responsibility for risk:** The board is responsible for (security) compliance and risk management. They must also have relevant training in order to effectively perform these duties. The board can be held personally liable if not performing these duties.
-  **Minimum security requirements & processes:** Organizations in scope must implement minimum security controls. Examples include basic cyber hygiene, network security, vulnerability handling & disclosure, security training and the use of encryption.
-  **Managing supply chain risk:** The supply chain must be managed securely. The supply chain risks must be understood and documented, along with identification of supplier vulnerabilities, cyber security processes & practices, and secure development.
-  **Incident handling & reporting:** Significant incidents must be reported to the relevant Computer Security Information Response Team (CSIRT). This must occur within 72 hours (and early warning within 24 hours). Customers must also be informed if impacted.

Fines in case of non-compliance:

-  NIS2 fines can reach €10 million or 2% of total worldwide turnover. Further, enforcement can be preceded or included with warnings, mandatory instructions. Personal fines & liabilities can also be enforced in case of (major) board shortcomings.

What it means for member states and organizations:

- **Member states** will need to draft legislation to incorporate the directive into law, set timelines for implementation and provide oversight and enforcement capabilities.
- **Public & private organizations and companies in critical sectors** will need to adhere to the NIS2 requirements.

## High Criticality Sectors

ICT  
Services  
Management  
(B2B)  
  
Space  
  
Transport  
  
Digital  
Infrastructure  
  
Public  
Administration  
  
Financial  
Markets  
Infrastructure  
  
Drinking Water  
  
Banking  
  
Health  
  
Waste Water  
  
Energy

## Other Critical Sectors

Manufacture,  
Production and  
Distribution of  
Chemicals  
  
Manufacturing  
  
Research  
  
Postal and  
Courier Services  
  
Waste  
Management  
  
Production,  
Processing and  
Distribution of  
Food  
  
Digital Providers

Both High Criticality Sectors, and Other Critical Sectors must adhere to the NIS2 (security) requirements. High Criticality Sectors are subject to immediate supervisory oversight, whereas Other Critical Sectors are subject to supervision in case there is some evidence of non-compliance or gaps.

Note that there are some other minimum scoping rules that determine whether an organization is in scope of NIS2. For example, large sized organizations (minimum of 250 employees or 50 million revenue), and medium sized organizations (minimum of 50 employees or 10 million revenue) in the critical sectors are in scope. Smaller organizations may be out of scope (depending on some other factors).



# Regulatory Compliance – NIS2



## Relevant directive principles

- **Governance (NIS2 Directive - Article 20)**  
A readiness and encouragement to train employees enabling them to identify risk and assess cybersecurity risk practices and their impact.
  - The suggested tooling will support you in providing their internal organization with the right foundation to base their training exercises upon.
- **Cybersecurity risk-management measures (NIS2 Directive - Article 21)**  
The directive depicts a specific set of measures to be undertaken by impacted organizations.
  - The suggested tooling will support you in implementing and managing these measures, among others by;
    - Comprehensive Asset Visibility
    - Change Impact analysis' capabilities
    - Effective incident handling
    - Business Continuity support
- **Reporting Obligations (NIS2 Directive - Article 23)**  
The directive depicts a specific obligations and instructions around the reporting of incidents.
  - The suggested tooling will support you in doing so by providing:
    - Standardized & customizable reporting capabilities
    - Integrations capabilities for automated communication of incident reports
    - A holistic view of the CI's, assets and services affected by an incidents and drill down capabilities to enable fast resolution and diagnosis

## Potential Penalties & Fines

- Fines in case of infringement on articles 21, 23 and 34:**
- At least:
    - EUR 10.000.000,-, or;
    - 2% of total worldwide annual turnover in preceding year
- Potential penalties on national adopted measures (member states):**
- Will vary per member state.

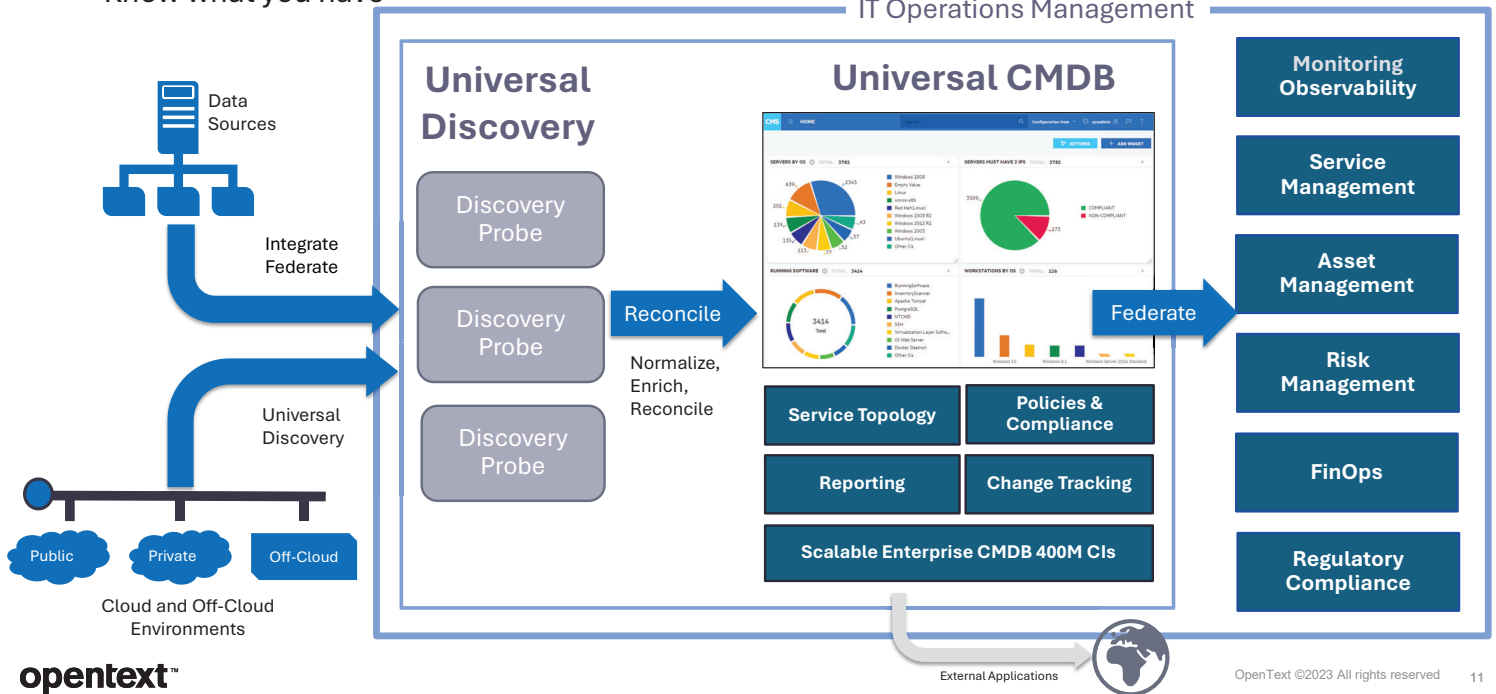
opentext™



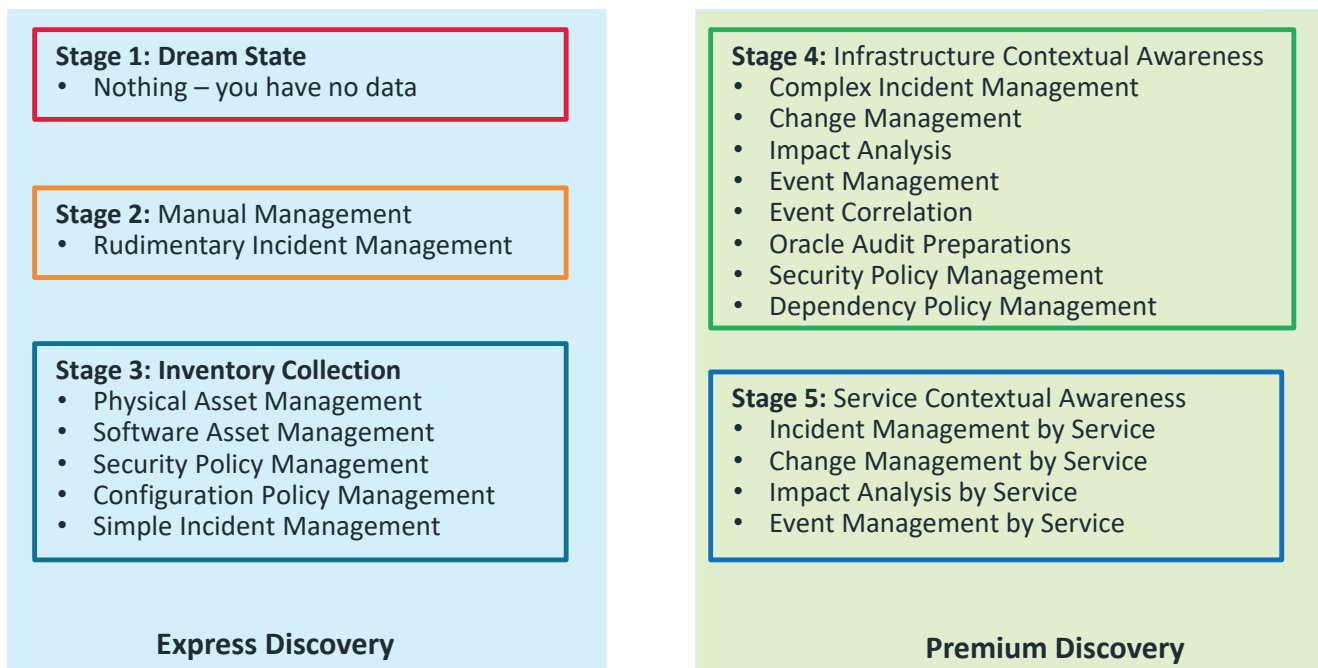
opentext™

# Discovery & CMDB

Know what you have

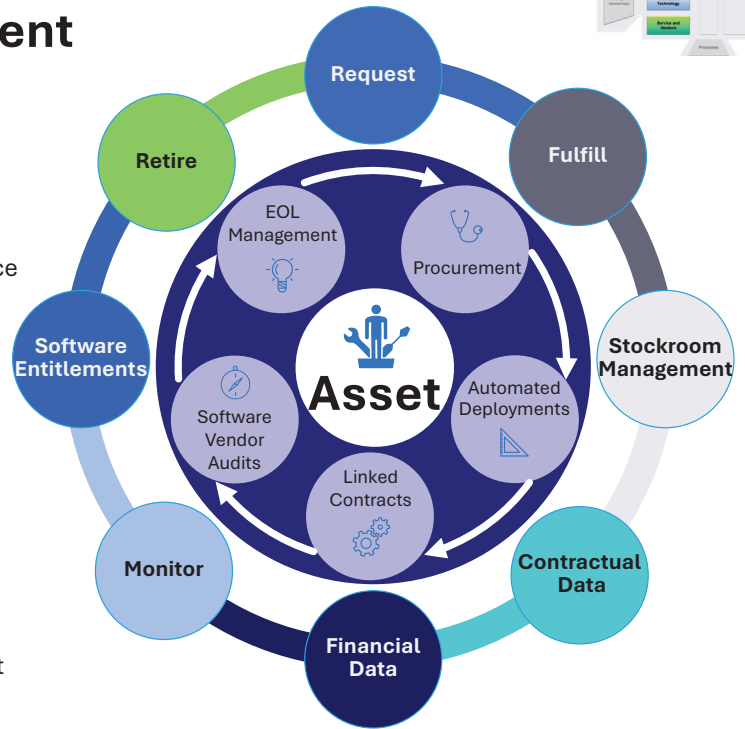
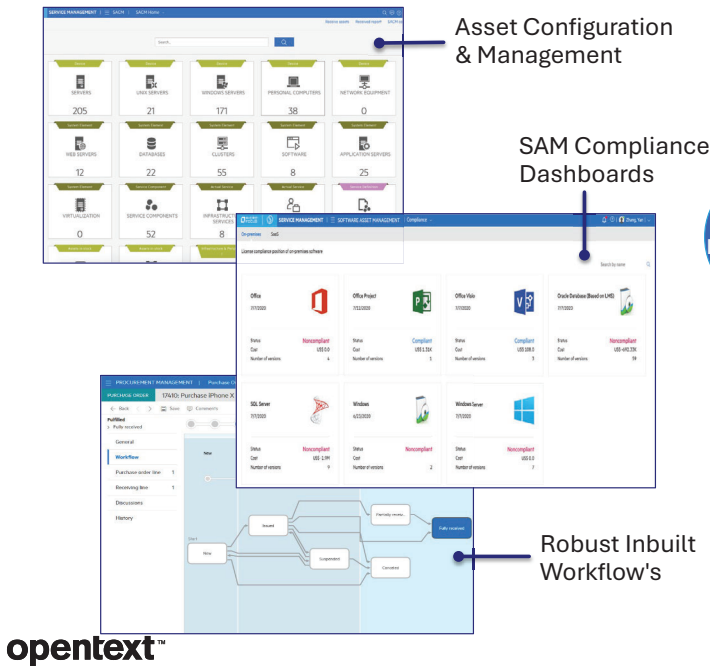


## Where are you?





# Asset Lifecycle management



OpenText ©2023 All rights reserved 13

# Agent Productivity & Process Owner KPI Optimization

## Intelligent Suggestions

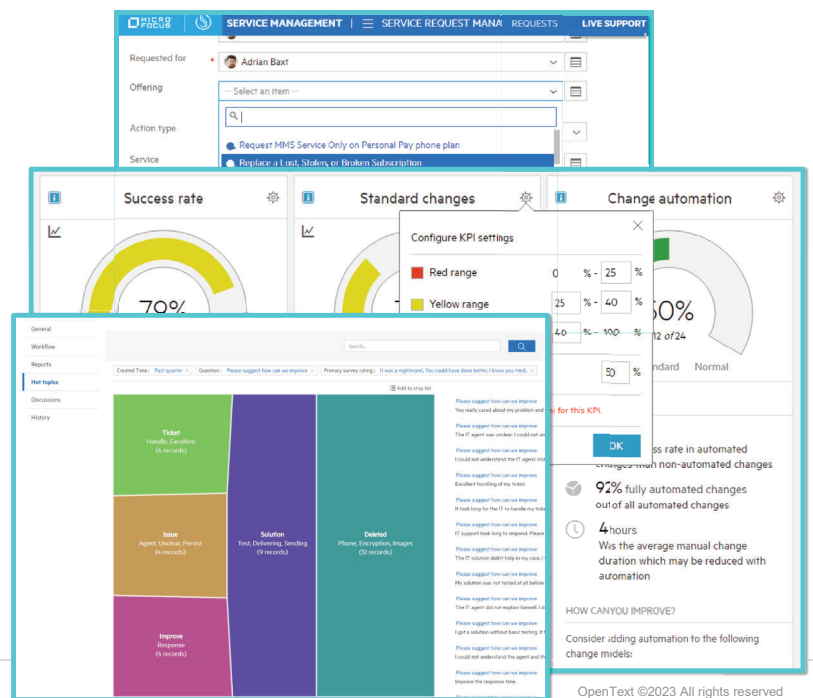
- Machine learning suggestions for ease of use and zero touch fulfillment

## Change Analytics

- Suggest concrete actions to improve process KPIs in defined library

## Hot Topic Analytics

- Pattern Clustering to identify recurring trends



OpenText ©2023 All rights reserved 14

# Full native SACM and Event widget in the Incident Process



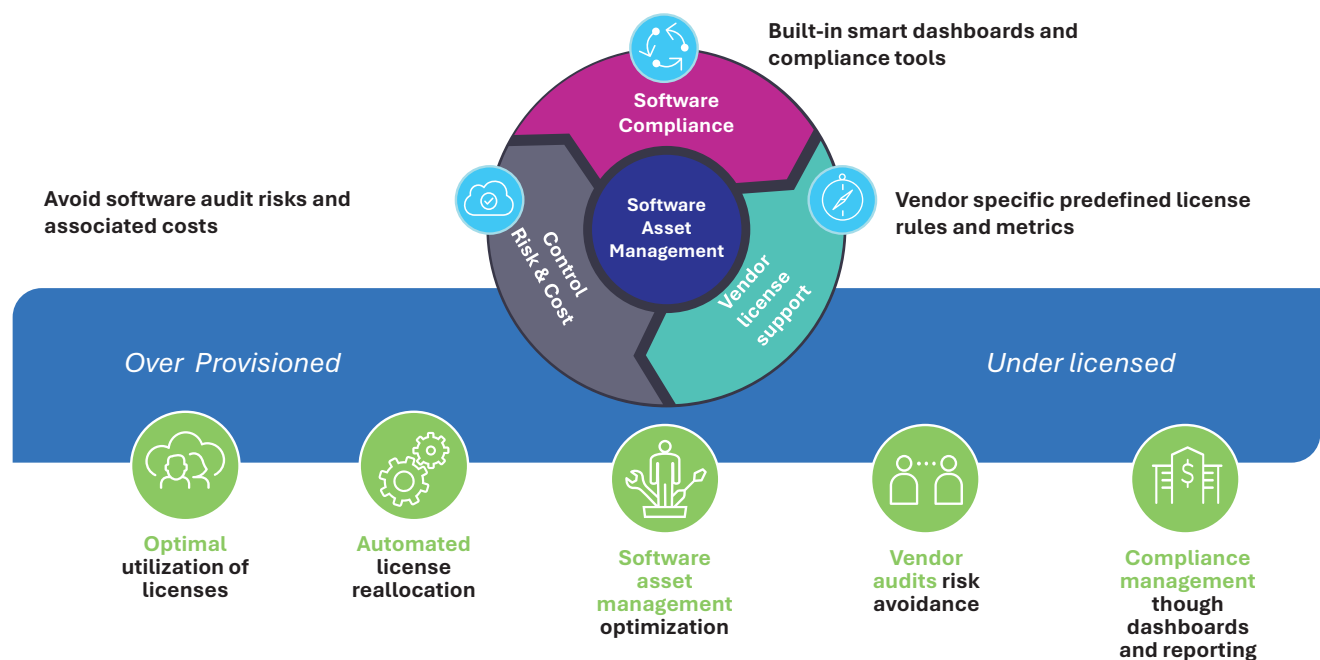
**Benefits**

- Up-to-date services and inventory
- Bi-directional data flow
- One service model & CI topology
- CI Topology and Impact widgets
- End to End lifecycle
- Auditing including federated attributes
- Enriched CI information
- Codeless configurability
- Event overview with Device and Incident

opentext™

OpenText ©2023 All rights reserved 15

# Software Asset Management



opentext™

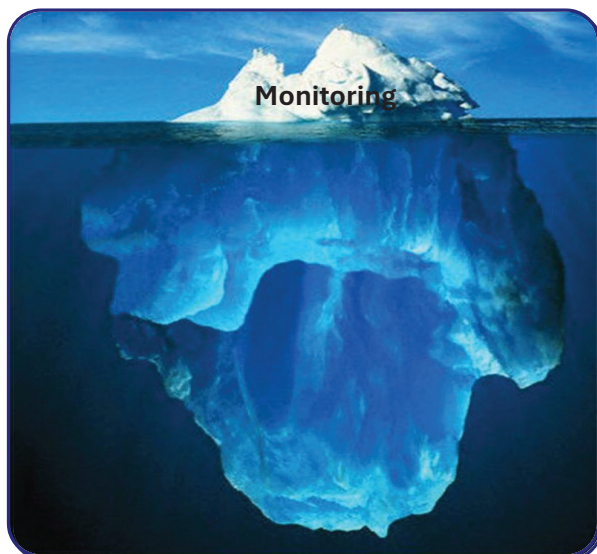
OpenText ©2023 All rights reserved 16





# Observability

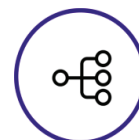
Go past monitoring - Observability as a Strategic Imperative



Metrics



Logs



Traces



# Observability

Go past monitoring - Observability as a Strategic Imperative



## Infrastructure Observability

- **Real-time monitoring & anomaly detection**  
Early detection and mitigation of cybersecurity incidents.
- **Automated compliance management**  
Enforces policies for CVE-based vulnerabilities with regular updates and automatic remediation workflows.
- **Comprehensive reporting**  
Facilitates transparent reporting of security incidents to regulators within mandated timelines.

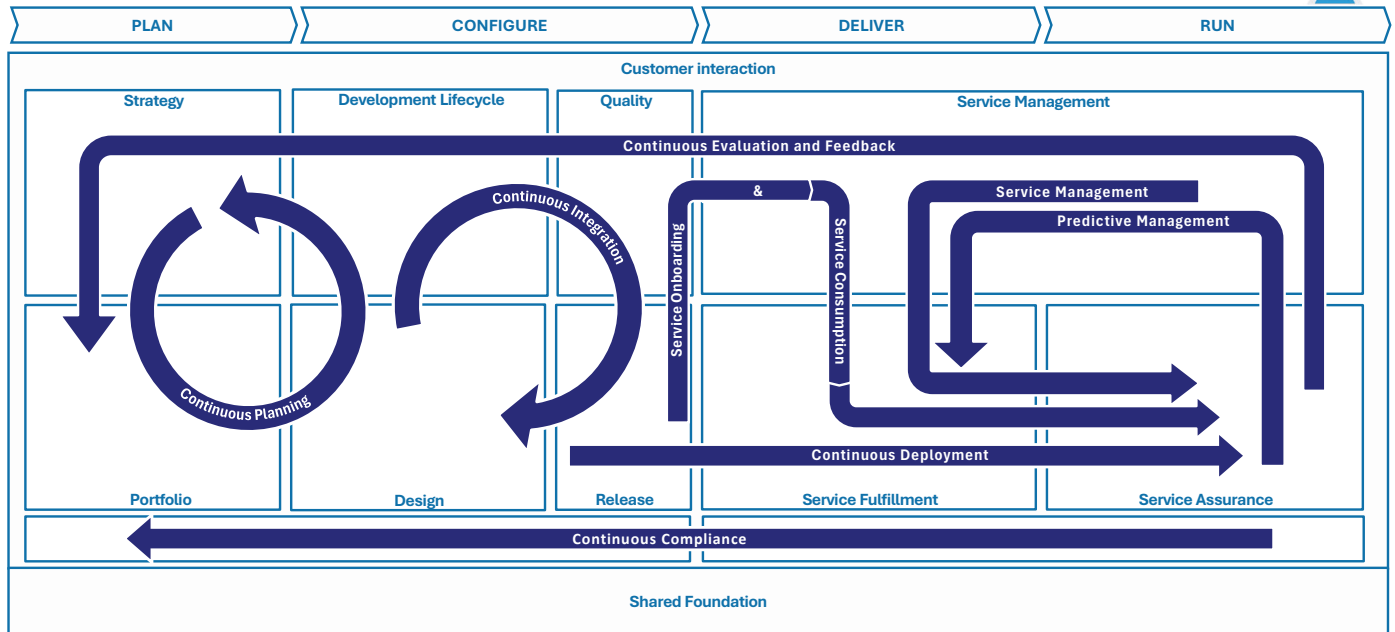


## Application Observability

- **End-to-End transaction tracing**  
Track data flow and application workflows to identify performance issues or unauthorized access.
- **Cross-System dependency mapping**  
Automatically identify weak points or unauthorized connections that might breach compliance protocols
- **Pro-active alerting**  
Quickly pinpoint the root cause of issues, reducing MTTR and improving system reliability.



# Service Integration & Management Value Streams



opentext™



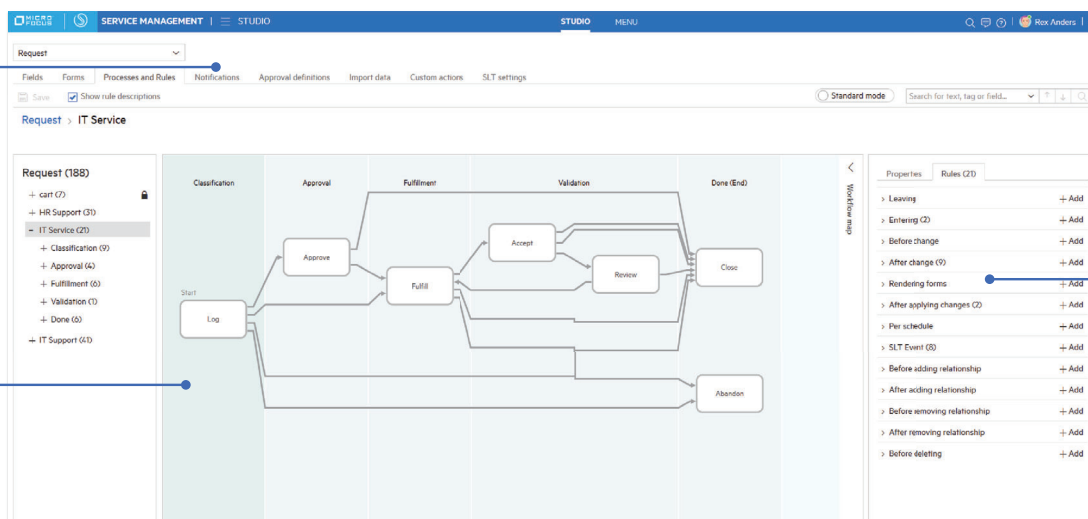
Open Text ©2023 All rights reserved 19

## Codeless configuration and out-of-the-box ITIL processes



Automatic notifications

Out-of-the-box workflows



Pre-defined business rules

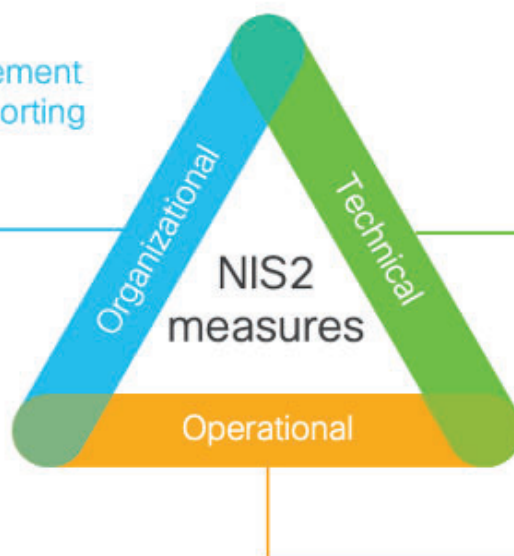
opentext™

OpenText ©2023 All rights reserved 20





Risk analysis and management  
Incident handling and reporting  
Crisis management  
Policies and procedures



Asset management  
Zero-trust access control  
Multifactor authentication  
Cryptography

Cybersecurity best practices  
Vulnerability management  
Supply chain security  
Workforce trainings

## Suggested Approach

### Phase I – Critical CI Inventory

Laying the foundation for IT visibility. Know what you have, where it is, and who owns it.

### Phase II – Full CI Inventory incl. Dependencies

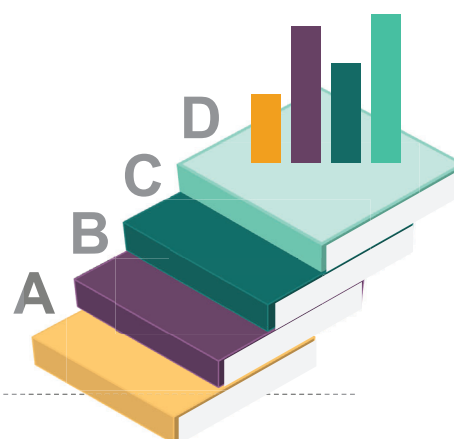
Beyond discovery: map relationships, reduce risks, and enable smarter IT decisions.

### Phase III – IT Asset Management

From chaos to control: maximize asset value, minimize costs, and stay compliant.

### Phase IV – IT Software Asset Management

Cut waste, avoid audits, stay compliant and optimize every software dollar spent.

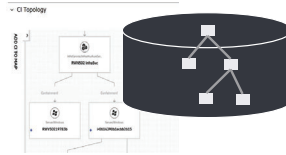


# Summary: Collect, report & Inform

It is all about data sources and Insights

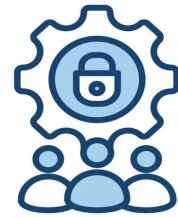


Observability (Monitoring)



Configuration Management System (Universal Discovery & CMDB)

Topology and Service Models (Context)



Cyber Security Management

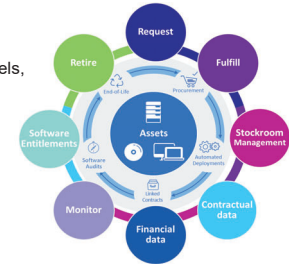


Service Management

Incidents Events



Asset Models, Locations



IT Asset Management

opentext™

OpenText ©2023 All rights reserved 23

## Opentext regulatory compliance advantages

### Increased IT Visibility & Control

- Faster IT audits due to centralized asset tracking and reporting.
- Significant reduction in shadow IT by mapping all assets and applications across on-prem & cloud environments.

### Compliance & Audit Risk Reduction

- Great reduction in compliance violations through automated asset discovery and software license tracking.
- Improved audit readiness by proactively managing software compliance risks.

### IT Cost & Asset Utilization Optimization

- Cloud cost savings with optimized Hybrid Cloud & FinOps strategies.
- Reduction in cloud waste through automated cost visibility and governance
- Annual savings from optimized IT asset lifecycle management.

### Improved Incident Response & Cyber Resilience

- Faster incident resolution by leveraging CMDB for automated impact analysis.
- Fewer SLA violations through optimized hybrid cloud and automated remediation.

### Risk Reduction & Business Continuity

- Lower software risks by ensuring license compliance and mitigating unapproved software usage.
- Fewer security breaches by continuously identifying vulnerabilities across IT assets.
- Strongly reduced risk on receiving hefty fines due to non-compliance with regulatory compliance.

opentext™

OpenText ©2023 All rights reserved 24



# Opentext Solutions

support compliancy with:



## Universal Discovery

Supports asset inventory accuracy and helps establish a comprehensive overview of the IT landscape, crucial for threat detection and vulnerability management.



## UCMDb

By tracking configuration changes and dependencies, a CMDB helps organizations respond efficiently to incidents and reduces misconfigurations that could lead to security risks.



## Asset Management Automation X

By maintaining an up-to-date inventory of assets, ITAM enables organizations to mitigate risks associated with outdated software and ensures they meet resilience and monitoring standards



## Observability

Delivers continuous system visibility and proactive anomaly detection, enabling organizations to monitor performance, detect vulnerabilities, and uphold resilience standards critical to regulatory frameworks.



## Service Management Automation X (SMAx)

Facilitates structured workflows, detailed incident tracking, and change management, ensuring risks are minimized, and compliance with regulatory documentation and response requirements is maintained.

opentext™

OpenText ©2023 All rights reserved 25

## Getting Engaged

Learn more about Asset Management & Universal Discovery and Universal CMDB

[opentext.com/products/universal-discovery](https://opentext.com/products/universal-discovery)

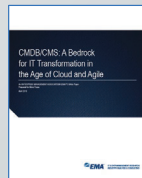
FLYER



DATASHEET



ANALYST REPORT



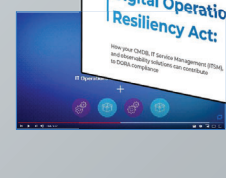
INFOGRAPHIC



CASE STUDY



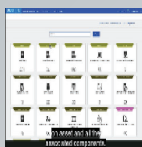
VIDEO



Product Webpage



AMX Infographic



Short Demo



Product Flyer



Hardware Asset Mgmt. Flyer



AMX Video

[opentext.com/products/asset-management-x](https://opentext.com/products/asset-management-x)

opentext™

OpenText ©2023 All rights reserved 26