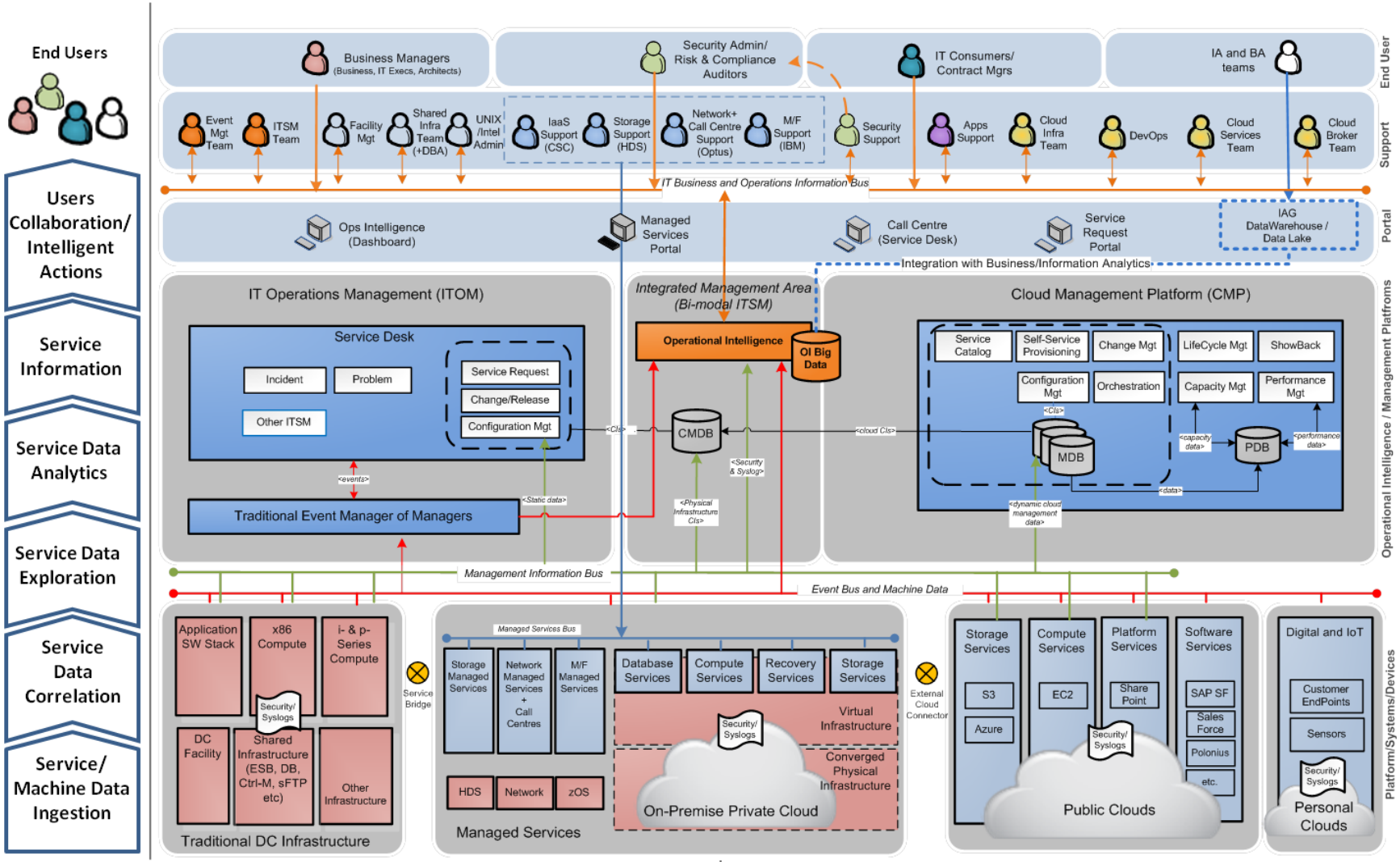
Operational Intelligence Approach

An OI approach begins with data ingestion followed by data correlation and the ability for users to explore and enrich data. The approach includes taking data through an analytics value chain to add contextual (historical) and situational (predictive) awareness capability before allowing OI users to collaborate and make impactful decisions for intelligent action outcomes. The context of an OI approach in the target state XYZ Hybrid IT environment is shown below.



- **Data Ingestion will include not just streaming service and machine data, but also have access to the organisation's Data Warehouse and Data Lakes.**
- **Desirable features of an OI data ingestion capability include:**

Fast and Flexible Data Input	• The OI tool must have the ability to collect and index data from just about any source imaginable: network traffic, web servers, custom applications, application servers, hypervisors, GPS systems, sensors, stock market feeds, call centre, social media and pre-existing structured databases. • No matter how the data is sourced, or what format it is in, it has to be indexed the same way - without any specific parsers or connectors to write or maintain. • The service data ingestion method must be fast and easy in order to quickly realise the value of the information contained in the data.
Lightweight Data Forwarders	• Not all the data needed for OI is available over the network or visible to the server where OI software is installed. Data forwarders are required to collect reliable, secure and real-time universal data from diverse data sources. • These forwarders should be lightweight and easily deployed to monitor local application log files, clickstream data, status commands outputs, performance metrics, etc. from virtual or non-virtual sources, or watch the file system for configuration, permissions and attribute changes
Real-time indexing	• The data ingestion tool must be able to continually index service and machine data in real time; this including logs, configuration data, change events, the output of diagnostic commands, data from APIs and message queues, logs from custom applications, etc.
Captures All Data	• The data ingestion tool must be able to store both raw data and the rich index in an efficient, compressed, redundant, file-system-based data store, with optional data signing and auditing to prove data integrity. • As with BI, the huge volume of OI data lends itself to Big Data management and technologies.
Flexible Schemas	• Together with the flexibility required for data input, the tool must not have predefined schema requirements. • Solutions that rely on brittle schemas have limited flexibility to answer new questions and break when data formats change. Any interpretation that needs to be done on the data, such as extracting a common field, or tagging a subset of hosts, is carried out at search time
Automated Chronology	• Extracting and normalizing timestamps is very important for streaming data inputs. The OI software will automatically determine the time of any event - even with the most atypical or non-traditional formats. Data missing timestamps must be handled by inferring timestamps based on context

- **Note: End-to-end service models will require capture of system and service data across all underlying infrastructure and service components. Whilst these data are easily accessible from XYZ-owned assets in legacy and Private Cloud infrastructure, this can be difficult for Managed Services and Public Clouds, in which case essential service data must be negotiated for availability to XYZ.**

- **After service data is ingested, the ability to make complex correlations across multiple streams and diverse data formats will produce the greatest insights.**
- **New insights are often created when vastly different types of data are brought together.**
- **Event correlation also allows a series of related events to be tracked as a single transaction to measure duration or status.**
- **The following are some key considerations for service data correlation:**

Diversity of Data Sources	• As XYZ continue to make inroads into cloud computing, Digital and Web-scale IT, there will be an increasing diversity of data sources . This will introduce many new data types and sources where their schema can be somewhat unpredictable. • The new norm involves “flexible schemas,” meaning data structures that are unpredictable or regularly evolving. For example, parent-child relationships can vary in the hierarchies of XML documents, and just about any data structure may appear in a message from an RSS feed. • Furthermore, data schema will naturally evolve, as best practices evolve concerning the data output from sensors, machinery, mobile devices, and so on.
Data Latency	• OI practice assumes that data is also diverse in terms of latency. For example, latent data (from a DW or similar database) provides a historic context for real-time events. This applies to many use cases, for example: tailoring a insurance purchase recommendation (based on prior purchases), detecting potential fraud (as when an insured motorist is involved in multiple similar losses over time), etc.
Native Data Formats	• OI solutions must be able to adapt to schema changes gracefully as well as handle extremes of richly structured and loosely structured data. • Likewise, the OI solution must be able to handle Big Data and streaming formats (e.g., XML, JSON) in their native form, without the need to transform and normalize the data into a standard schema. • Because these data sources rarely have metadata, a tool that can deduce metadata automatically is highly desirable
Bi-Modal IT Service Data	• In the XYZ Hybrid IT environment, service data correlation may initially happen in the traditional ITOM domain and Cloud Management Platform (CMP) domain, before these data feed into an integrated management area where the OI tool correlation takes over. This will then allow the bi-modal ITSM to operate in XYZ’s Hybrid IT environment.

- **With OI, data exploration usually focuses on studying the streaming data delivered by one or more streams.**
- **The study involves both data in motion (arriving via a stream) and data at rest (stored in a file or database).**
- **Stream exploration and discovery is important to streaming analytics and OI in the following aspects:**

Discover Pattern and Process	• OI is concerned with pattern and process discovery, not just data or stream discovery. • The OI tool should auto-detect meaningful patterns in service and machine data, regardless of data source or type. It then enables XYZ users to zoom in and out using a visual timeline so they can identify trends, spikes and drill down into the results. • Seeing event patterns and business processes unfolding in one or more streams provides evidence for understanding online customer behaviour and improving business processes. In fact, XYZ OI users can explore streams to discover what actually happens in a business process, which is knowledge at a level of accuracy they can't get elsewhere
Explore Streams and Related Data	• This ability allows OI developers to get a sense of how processes work, so they can build a dataset, model, and rules that yield a correlation advantageous to XYZ. • This is also how a developer discovers new sources and understands their applicability to specific use cases. A lookup facility can be used to enhance, enrich, validate or add context to data collected in the OI tool. For example, correlating intrusion detection data (IDS) with data from an asset management system can reduce IDS false-positives, such as: an attack based on a Windows OS vulnerability seen by an IDS can be correlated with data from an asset being attacked.
Continuous, Automated Discovery	• A mature OI platform will continuously and automatically process streaming data and relationships, to discover business activity patterns, exceptions, and bottlenecks; it then proactively responds based on discovered insights. Examples of activity patterns that can be quickly uncovered, analysed, and acted upon include those related to financial transactions, orders, claims, vehicles, online customers, etc
Search and investigate	• The OI tool must allow XYZ users to search and navigate their data from one place. • Freeform search should be supported, as familiar to anyone comfortable on the web. This allows XYZ users to quickly iterate and refine their searches without knowing anything about specific data formats. • The search facility should include real-time, time-range and transaction searches. • Sub-searches should allow taking the results of one search and use them in another to create if/then conditions. • Using a sub-search allows users to see the results of a search only if a set of other conditions are met (or not).
Search Time Knowledge Mapping	• Unlike traditional approach, the OI tool will allow mapping knowledge to data at search time. There is no more need for the complex management of custom parsers and connectors. The ability to enrich service and machine data with information from external asset management databases, configuration management systems, user directories, etc. allows a flexible way to manage data changes. In addition, as each XYZ OI user add their own knowledge as they go, the OI system is made smarter for everyone else.

- **Advanced analytics techniques provide deeper insights. The ability to make impactful decisions and immediately act on these insights largely depends on how fast the analytics can be executed across the past, present, and future timeframes.**
- **Most analytic operations are scheduled to run on a 24-hour or longer cycle. Getting the most out of streaming data, however, requires analytics that execute or update every few seconds or milliseconds to process each event, message, record, transaction, or log entry as it arrives in case the new data signals a business event that requires immediate attention. In other words, continuous analytics go hand-in-hand with streaming data. The results of a query can be incrementally updated with each new event, without needing to rerun the query against all pertinent data.**
- **Likewise, continuous analytics may rescore an analytic model, recalculate a statistic, remap a cluster, and so on - but as efficient, incremental updates, not execution from scratch.**
- **Achieving timely actions requires the OI methodology and technology to move through all of the steps of the analytics value chain (i.e., streaming, historical, predictive, and prescriptive analytics) in real-time. The critical "last mile" for timely outcomes depends on the ability to execute analytics in real-time across the analytics value chain with relevant contextual and situational data. Combining this with the ability to take the next best action in any particular scenario creates the greatest value.**
- **The increasing analytics value chain refines the data and adds more value and context to service information, with each step, as described below:**

Real-time Streaming Analytics	• This helps to quickly analyse and decipher continuously flowing streams of data from applications and systems. • Faster analytics depends on the ability to process incoming streams while they are happening. • Streaming analytics incorporates several analytic methods, all considered advanced because of the great diversity of data types and structures found in a stream, as well as the many real-world use cases that analytics may serve.
Historical Analytics	• The refined data is then correlated with contextual and historical data to provide a baseline for advanced analytics. • Contextual data can include information such as GIS data relating to an application. • Historical analytics is one of the key baselines in unifying all analytics. • Faster analytics depends on unification with the foundational historical analytics in place today. Replaying how past behaviour compares with current and predicted behaviour enables powerful insights for real-time decision making and actions

Predictive Analytics	• The next step of the OI analytics value chain is to predict exceptions, anomalies, or patterns, that are based on machine learning over historical and situational data, such as external events like weather. • Predictive analytics leverages all data to generate predictive models for OI applications and use cases. • Continuous machine learning techniques can be used to learn predictive tasks in an automated way. • Likewise, it can be instrumental in coping with online learning, as well as with structural changes. For example, when used with regression analysis, continuous machine learning techniques can discover sudden changes in underlying model parameters immediately, such as a sudden shift in customer demand or a new baseline for system loading. • Such rapid detection can enable systems to dynamically adapt to change. • As the unification of predictive models with the rest of the analytics types and platform enables faster analytics and smarter actions, the business imperative of reduced time-to action is achieved.
Prescriptive Analytics	• This final step in the analytics value chain is to determine the next best action to take. • The goal of many streaming analytics applications is to predict the class or value of new instances in the data stream, given some knowledge about the class membership or values of previous instances in the data stream. • A mature OI platform will support multiple approaches, including Bayesian techniques, the prediction of near-term opportunities and threats, and recommendations for the next best action, whether that is to guide a customer to a purchase, avoid a process bottleneck, or mitigate a threat. • Streaming analytics enables predictions to be continuously rescored and re-evaluated to reflect the most recent data updates and changes in the business situation
Event Processing Network (EPN)	• EPN is a kind of “secret sauce” for OI and streaming analytics. • An EPN models complex event analytics and patterns as multi-stage flows, allowing event processing to be decomposed into simpler event processing steps. • The resulting analytics and complex events from one EPN can feed other EPNs, thereby forming a network of EPNs. The network enables critical and innovative functionality, such as correlations across multiple streams and other data structures, parallel processing, incremental analytic updates, stream discovery, and continuous real-time operation. • Hence, EPN modelling coupled with streaming analytics is fundamental to developing event-driven solutions for OI.

- **The final key step of the OI analytics value chain is the ability to take intelligent action, based on the unified analytics and service information. Continuous analytics should interact seamlessly and in real time with automated responses based on intelligent process management.**
- **OI developers can then define software processes for automated responses (based on business rules and application logic), which are then automatically executed at run time (based on discovered insights). For example, an automated response from an OI solution may trigger a fraud investigation, a repair process, or a personalised marketing offer.**
- **Response processes can continually monitor analytic results and adapt the behaviour of the response as the situation evolves, leading to better and faster business outcomes. Ability to dynamically adapt processes is essential for seizing one-to-one marketing opportunities and mitigating security incidents with rapidly escalating threat levels and reach.**
- **OI implementation should consider the following end-user implications:**

User Portal	• An OI portal will give business people visibility into streams and processes via dashboards. • Dashboards provide users with a picture of current performance, and visually highlight anomalies and exceptions. • XYZ users can drill into specific activities or transactions to get the context and take the appropriate action. • Dashboards should be easy to compose and personalise (without programming) by business analysts and similar power users, assembled from diverse data sources. • Time sensitive data should be updated in dashboards in real time.
Involve Business People	• Involving business people in “hands-on” streaming analytics yields better results. • Business people can more accurately perform data governance, data stewardship, and other forms of governance and compliance. • Involvement of business people tends to increase the likelihood of success with sponsorship, funding, and the perception of ROI. • The business people involved should be domain experts so they can provide valuable knowledge transfer
Empower Business Users	• A self-service OI tool function will allow many data analysts and other power users to define and monitor key analytics for streaming data. • Empowering business users enables the pervasive use of analytics, encourages experimentation by the domain experts, democratises streaming analytics, and allows for the “crowd-sourcing” of analytical ideas by all stakeholders. • It removes bottlenecks that can cripple the widespread adoption of streaming analytics - such as a lack of available IT resources and the shortage of technicians skilled in programmatic analytics tools.
Collaboration	• The OI tool function should automate user collaboration. • This assumes a unified development environment for streaming analytics and OI, including functionality for both technical and non technical XYZ users. • This enables business users to view data and development artefacts and work on common workflows. Collaboration will also allow XYZ users to annotate and mark streams and other data sources of interest for a particular project

As evident from the value propositions, Operational Intelligence will open up new opportunities for XYZ to derive real business value from service data and service information. Recent weeks have seen a surge in interest from several XYZ IT domains for capabilities to obtain more insights into operational events and our customer behaviours. The following are some of the areas where use cases are coming from, that can leverage shared use of a strategic enterprise-wide OI platform.

Application Delivery

- OI provides E2E visibility across XYZ's Hybrid IT infrastructures; troubleshoot across application environments; monitor for performance degradation; trace transactions across distributed systems and infrastructure.

DevOps

- OI accelerates development and test cycles; support DevOps and advanced development methodologies such as agile and continuous delivery; integrate XYZ enterprise applications with APIs, SDKs and other modern web technologies; build enterprise-class applications that leverage OI APIs.

Security, Compliance & Fraud

- OI provides rapid incident response, real-time correlation and in-depth monitoring across data sources; conduct statistical analysis for advance pattern detection and threat defence; identify compliance and security breaches, then halt and correct them immediately; spot and stop fraudulent activity even as fraud is being perpetrated. OI facilitates XYZ's APRA compliance and reporting requirements.

Infrastructure and Operations Management

- OI proactively monitor across IT silos to ensure uptime; rapidly pinpoint and resolve problems; identify infrastructure service relationships, establish baselines and create analytics to report on SLAs or track SLAs of service providers. Monitor and maintain the availability, performance, and capacity of interconnected infrastructures across XYZ clouds and managed services

Business Analytics

- OI gains visibility and intelligence on XYZ customers, services and transactions; identify trends and patterns in real time; fully understand the impact of new product features on back-end services; gain a deeper understanding of user experience to improve customer satisfaction, prevent drop-offs, improve conversions and boost online revenues.

Customer Experience

- OI allows XYZ to understand customer behaviour, as seen across multiple channels, so as to improve the customer experience as it's happening. As business transaction execution spans public and private infrastructure, IT operation loses control of much of the execution environment. Application monitoring and trXYZe then become key capabilities for managing both vendor and user relationships. OI solutions are key to deliver these capabilities. Apart from the ability to monitor and measure end user activity, OI can provide intelligence about user behaviour by integrating and analysing on-line and off-line customer data to improve customer service efforts.

Monitoring AWS

- OI tools like Splunk allows XYZ to gain in-depth visibility and rapid insights into AWS administration and account activity. Splunk integrates with AWS CloudTrail and AWS Config, and offers a prebuilt knowledge base of critical dashboards and reports. This will then allow XYZ to gather important insights into security-related activity such as unauthorized access attempts, network configuration changes and access level changes. With these reports and the ability to analyse activity in detail, the tool will also allow XYZ to:
  - › Accelerate AWS deployment through increased visibility into user behavior and resource utilisation in an AWS account.
  - › Ensure adherence to security and compliance standards with a full audit trail.
  - › Continuously monitor user actions and meet PCI and other audit requirements.

- **OI complements BI/DW** - from the perspective of information delivery speeds and user response times, OI and traditional business intelligence (BI) and data warehousing (DW) functions are complementary with very little, if any, overlap.

- **OI focus on extreme real-time and streaming analytics** - this places OI at the far end of the temporal spectrum compared to traditional BI/DW infrastructures, which are most often applied to latent data at rest. The majority of BI/DW applications serve long term strategic decision making, where real-time data and its processing simply isn't a requirement.

- **Do not attempt to retrofit BI/DW** - although ample technology exists for "near real-time retrofits" for BI/DW infrastructure, almost none exists for adding true real time. For that reason - plus the fact that OI and BI/DW are complementary - organizations needing true real-time analytics should not attempt a retrofit to BI/DW. Even when near real-time capabilities are retrofitted onto BI/DW technologies - as is common with the practices of operational BI and performance management - users usually expect responses in the range of two to four hours, whereas in real-time OI, intelligent responses can be arrived at in milliseconds. Hence, rather than retrofit BI/DW, organisations should seek OI and streaming analytics solutions that rapidly integrate with their existing BI/DW infrastructure, as well as with similar data platforms such as NoSQL databases, Big Data frameworks and Hadoop.

- **Use pre-built and pluggable connectors** – that are non-intrusive and make seamless the end-to-end process of exchanging information between BI/DW applications/sources and OI solutions and data streams. Such integration between OI and BI/DW enables real-time intelligence to be correlated with historical trends, which can reveal whether current real-time observations are anomalous or expected. Such correlations can avoid both false positives (e.g. sales that increase due to seasonality instead of current marketing campaigns) and false negatives (e.g. cyber attacks that hide in the noise of peak business application and network activity).