Deep Science Publishing, 2026
https://doi.org/10.70593/978-93-7185-975-2_1

DeepScience
Open Access Books

Chapter 1: Foundations of Secure and Governed Enterprise Intelligence

1.1. Introduction

Enterprise Intelligence (EI)—intelligence generated and used within an organization—encompasses the governance of networked data, information, knowledge, insights, intellectual capital, metadata, user perceptions, and opinions. Fundamentally, it is about the management of an organization's data resources—not just the management of facts, but their thoughtful use, evaluation, ingestion, filtering, assessment, curation, and analysis for both present and future purposes. Analysis capability consists of providing the right filter at the right time to the right community but is only part of the overall management process. Governance involves establishing policies and processes with accountabilities to ensure protected, secure, and abused information across the network. An Enterprise Intelligence function (potentially with some outsourced components) manages all data and information resources within Domain Authority specifications to satisfy business objectives. A future scenario: business demand an increase in intelligence community membership but with a simultaneous reduction in cost, hence the concept of Enterprise Intelligence arises in return.

The review underpinning this research, involving discussions with over 200 stakeholders in intelligence production and use, revealed what "Enterprise Intelligence" must have been in the past and should include in the future. Nine areas of "governed" intelligence should intersect: Sources, People, Information, Data, Analysis, Perceptions, Views, Results, and User's Push. A successful gap analysis will generate a clear grouped priorities statement for all intelligence development and/or production activities. A sample analysis will validate the principles and the process, also revealing the point of equilibrium between assets and demand through sensitivity analysis.

1.1.1. Overview and Objectives

Enterprise intelligence (EI), defined as "knowledge of an enterprise which typically derives from data within the enterprise, data from external sources and discovery through the application of data science", is subject to increasing acceptance and interest among business people and management 'thought leaders'. Knowledge of government is another major driver of data science. Data scientists working for governments at national or federal, state or provincial, regional and local levels read news media, examine online data sources, attend seminars, workshop and conferences, consult subject-matter experts and build intellectual networks to learn about government actions and decisions, political issues, public interests, community needs, and the history, cultural heritage and traditions of the country, state, region and community. Their objectives are often to help governments meet objectives associated with wellbeing/security of citizens/society, economic growth, peace, and natural and built environment. Intelligence enables business and government to achieve sustainable advantages/disadvantages in the marketplace.

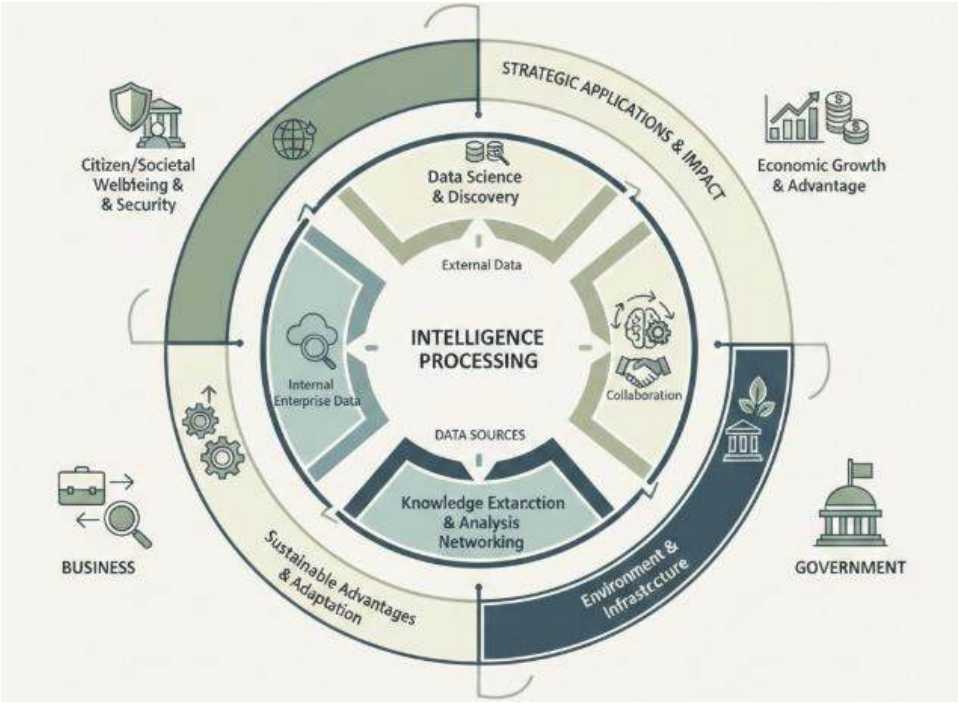

Fig 1.1: Cross-Sectoral Intelligence Ecosystems: Integrating Enterprise Data Science and Public Knowledge for Strategic Advantage and Societal Resilience

When people working for business, government or a not-for-profit organisation need knowledge of someone else's operation or intention, they typically engage in intelligence gathering, which may entail a formal investigation, the use of consultants and

researchers, or it may simply involve reading news media, surfing the web, or talking with others. This peaks during a merger, acquisition, investment or new partnership with a rival, competitor or business neighbour in the supply or distribution chain. Emerging and developing countries, particularly their governments, have a greater need for intelligence than advanced economies because their economies are or have been in a state of transition or change. Their governments, as a result, and even the government of a business or not-for-profit organisation, need to have a careful watch of the changes taking place in the country. Successful participants in these industries become the targets of espionage.

There is also growing interest among business leaders in placing industry knowledge into a business intelligence context, taking advantage of expertise and intelligence gathering in their own operations and other operations throughout the world. The industry is putting in great effort into developing systems to put industry knowledge within reach of company executives within the industry or the related group of industries. Businesses are sharing knowledge to assist their suppliers and customers in the hope of aligning their management strategies, thereby generating benefits for them all. Business Intelligence is cooperating with market research firms to provide facts and forecasts on the industry.

1.2. Conceptual Foundations

Enterprise intelligence occurs within an enterprise intelligence ecosystem comprising four interconnected elements: the enterprise, intelligence, enterprise intelligence, and the enterprise intelligence process. These four terms ground the research, clarify the recurrent use of "enterprise" as an adjective, and explain the processes that create intelligence within an enterprise through the enterprise intelligence process.

Enterprises are social constructs for collective action within a framework of stable personnel and resources, supported by laws, markets, and contracts. Enterprises alone possess full property rights over valuable data, identifiable private data, and information products. Such data held by external parties is valuable and serve as the foundation of intelligence. Intelligence is defined as deep observations on which well-informed actions can be reliably based. Enterprise intelligence is thus deep observations of its external context—an enterprise's environment, competitors, and other relevant actors—on which that enterprise's actions can be reliably based. Enterprise intelligence is seldom articulated in either its active or passive form. An enterprise's ability to make intelligent decisions is limited only by the amount of data it can afford to acquire and govern, but fight against high volume and complexity still leads to more decisions being made on gut feel.

The enterprise intelligence process refers to the repeated organization and characterization of raw data obtained from controlled observation and the acquisition of knowledge into well-structured observations that inform foreseeable actions of the enterprise and that are governable by its board. In summary, enterprise intelligence is the repeated process of acquiring knowledge from external information, characterizing that knowledge, and then governing its representation within the board's framework of law, risk, and overall strategy

1.2.1. Definitions of Enterprise Intelligence

Enterprise intelligence is the deployment of appropriate analytical methodologies—descriptive, diagnostic, predictive, prescriptive, cognitive, and even generative—against the appropriate enterprise data for a given enterprise problem or decision context, while implementing appropriate security and governance measures. Other definitions of enterprise intelligence explicitly mention security and governance. Decision intelligence integrates all aspects of decision-making. Combining decision intelligence with a secure and governed enterprise data foundation yields enterprise intelligence—the foundation of enterprise data management.

Security and governance objectives include the identification of—at a minimum—sensitive, confidential, classified, proprietary, and personally identifiable information; ensuring that relevant regulations (e.g., PCI DSS, HIPAA) are met; and preventing unintentional or malicious use or exposure of such information. Data anonymisation or de-identification—a group of methodologies for safeguarding sensitive information (e.g., PII)—acts as a control measure with wide applicability. Other controls focus on preventing and detecting leaks, breaches, or abuse; ensuring third-party access is narrowly tailored; and augmenting regulatory compliance. Security involves the use of measures, technologies, and procedures to detect, identify, and prevent threats; to monitor; and to respond to incidents. Security is aided by a proper foundation of internal control, segregation of duties, reliable information, monitoring, and preventive controls.

Successful enterprise transformations require strategic alignment and engagement, delivery of business value, and the establishment of an enterprise data and artificial intelligence foundation that support stakeholder adoption and decision intelligence. Security and compliance concerns regarding data retention and the deploying, developing, and implementing of suitable data science methodologies must be overcome appropriately. The responsible, ethical, and transparent use of enterprise data and its supporting artefacts must be ensured. Enterprise intelligence—secure, governed, and trusted enterprise data with associated artificial intelligence, data science, and business analytics—aligns with the relevant principles of the Corporate Data Charter, including

the definitions of data intelligence and data governance and the Responsible Artificial Intelligence Principles.

1.2.2. Security and Governance as Core Pillars

In order to build on open and collaborative sharing and use of enterprise intelligence, the foundations of security and governance must be laid first. Enterprise intelligence constitutes organisations' knowledge of the present, the environment in which they act, and the potential future. McKinsey redefined knowledge as awareness of some aspect of the enterprise gained through data and intelligence as knowledge synthesised with insight ; further, it defined insight as knowledge synthesised with judgment. Intelligence can thus be understood as awareness synthesised with judgment. For individuals and organisations, knowledge is important not only in its own right, but also with respect to its quality as determined by its availability, accuracy, currency, comprehensiveness, coherence, consistency, relevance, and timeliness.

For organisations, security and governance define and underpin the principles of responsible sharing and use of enterprise data, knowledge and intelligence. In the context of enterprise intelligence, security encompasses the protection of data, knowledge and intelligence against disclosure to unauthorised parties, modification by unauthorised parties, and destruction, interruption, degradation or loss. Disclosure may be intentional or accidental, and information may be made available to individuals, groups, or other systems external to the organisation or to individuals within the organisation who are not entitled to access it. The concept of governance refers to the framework laid down by the organisation within which enterprise data, knowledge and intelligence are shared and used securely. These principles, encompassing the notions of availability, integrity and confidentiality, also underpin the architecture of secure enterprise systems as a whole.

1.3. Architectural Principles for Security and Governance

Any deployment and integration of enterprise intelligence must provide and exhibit neutrality, security, and trustworthiness in internally initiated communications within, and externally initiated communications across, the enterprise boundary. Internal and external communications not provided or controlled by the traditional communications service provider may be susceptible to man-in-the-middle and/or replay attacks. Such attacks are generally difficult to counter without the intense scrutiny for intrusion and unauthorized data exfiltration desirable in enterprise-deployed and non-enterprise-deployed data repositories. Internal communication paths between enterprise employees, systems, and cache servers and external paths to trusted partners should therefore also be considered within scope of enterprise intelligence architecture. These

communications paths, as well as their exchanged data, should remain secure under a traditional inverse-security definition with an additional requirement for neutrality in a formal-client-server-client context defined for artificial intelligence.

Enterprise intelligence is intended to facilitate the management and protection of enterprise data collected and maintained for traditional enterprise functions. These functions should continue to be provided by traditionally deployed and governed enterprise systems, even accounts of a heretofore-secure hacking campaign. Indeed, traditional separation of duties within and between enterprise departments, rather than added concentration of powers, should again enable detection and mitigation of malevolent acts, as described in . Any architecture for enterprise intelligence should therefore conform to principles of traditional enterprise information control. Specifically, exposure of enterprise intelligence data repositories and the intelligence functions of enterprise employees, systems, and cache servers should be controlled, and accessible data monitored for unauthorized misuse or exfiltration during internally initiated communications.

1.3.1. Data Architecture and Provenance

Enterprise intelligence includes the provenance of the component data and processes that support deriving enterprise intelligence (EI). Provenance encompasses the complete set of abstractions, logical structures, representations, materials, resources, processes, and contexts associated with certain aspects of data and information—hence, with intelligence. Such intelligence builds on facts obtained from temporal observations of suitable entities. The facts are processed by valid operations to derive further information, knowledge, insights, foresights, and warnings. The provenance of the EI results from the use of the abstractive and logical resources and applications being exploited in the generation of the intelligence. Natural language provides insights and warnings of a suggestive nature.

The component data therefore require appropriate characterisation, coverage, collection, preparation, accessibility, and storage in a suitable, physically or logically integrated structure. For the data to be fit for use, appropriate selection constraints are needed, supported by necessary transformation processes. A suitable data architecture supports the connected enterprise through its component data, their preparation, associations, relationships, and capacities. Provenance management should support all data management processes during the entire lifecycle of the connected enterprise and its components. Maintenance of the necessary and sufficient data that are prepared and fit for use has to be governed and controlled over the lifecycle of the data architecture, the connected enterprise, and the component entities.

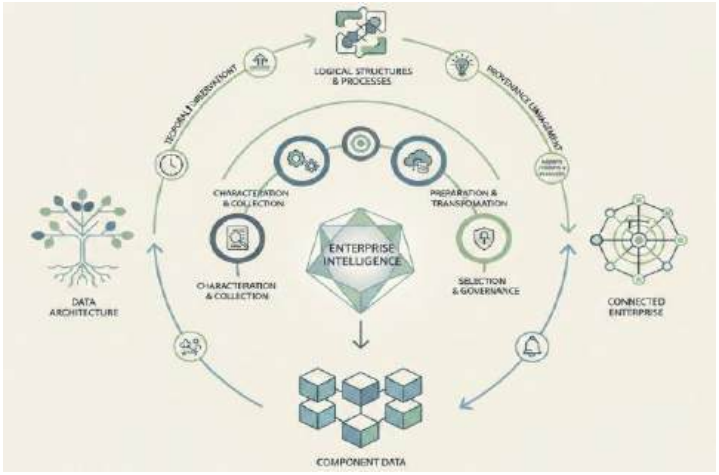

Fig 1.2: Lifecycle Provenance Architecture: A Framework for Data Integrity and Veracity in Connected Enterprise Intelligence

1.3.2. Identity, Access, and Entitlement Management

The development of enterprise intelligence requires a clear, strategic articulation of categories, definitions, processes, technologies, and flows relevant to the issue of identity and access, which is essential for ensuring privacy, security, and compliance. The provisioning of identity is the basis for securely modelling and controlling enterprise platforms, services, resources, models, data, processes, and features, meaning that the accesses and entitlements allocated to individuals, the organisation, and its partners must be carefully designed, implemented, and governed. A digital identity defines an entity in cyberspace; identity management builds digital identities scalable to today's global and cloud-reliant economy. Individuals, devices, agents, and the connections between them need identity management.

Identity management governs the creation, maintenance, and use of identities for individuals, devices, services, systems, processes, and applications. With a reliable digital identity, services, devices, and processes can act on an individual's behalf. Identity management establishes the processes, technologies, and controls required for identity. Access management assesses and provision access to information based on characteristics of user identities, data, applications, and systems. Controls govern access management by determining who and what should have what type of access to applications, systems, data, and other enterprise resources. Access management includes authentication, authorisation, access rights, and entitlements. It assesses whether a user should have access to a web application. Access control for an application determines what a user can access based on entitlement. An entitlement is a particular indication of a user's access, such as permission to modify or read a document.

1.4. Data Management for Enterprise Intelligence

Security and governance are essential prerequisites for enterprise intelligence. Protecting sensitive enterprise data from malicious actors and maintaining the integrity of data for decision-making and analytics is critical. Inadequate governance, malicious manipulation, or unauthorized access to enterprise data can have catastrophic consequences.

Enterprise data management (EDM) incorporates processes, standards, and technologies for managing enterprise data as an asset. EDM defines various roles, responsibilities, processes, and technology to manage enterprise data securely and efficiently while also enabling analytics. EDM encompasses both technical and nontechnical components for data management, including security, privacy, governance, integration, quality, and lifecycle management.

Data management and governance frameworks describe the processes that should be established for enterprise data management, define essential roles and responsibilities, categorize enterprise data, and determine criteria for the classification of enterprise data. Three types of enterprise data are important for enterprise intelligence: operational data, external data (external to the enterprise but needed in operational decision-making), and analytic data (data used primarily to perform analytics and predictive modelling).

1.4.1. Data Quality and Lineage

Effective enterprise intelligence hinges on high-quality data that users completely trust. Evaluating quality involves examining multiple elements across six distinct characteristics, including accuracy, completeness, consistency, timeliness, uniqueness, and validity. Accompanying tools examine data lineage—tracking the movement and transformation of data as it flows across sources and through numerous intermediate datasets and reports. Establishing essential checks and balances allows operable BI solutions for which data sources and modelling methods can survive probing scrutiny during audits.

BI is an enabling technology for tasks that help organizations gain greater insights from business data. Together, data warehouse systems and BI tools—frequently underpinned by relational databases—have enabled new insights by correlating data from disparate sources. BI has become permeated with data quality awareness, as the classic truism "garbage in, garbage out" continues to hold true. Yet developing and deploying analytical systems that address enterprise decision-making needs remains difficult and fraught with risk. Users are wary of data quality, and have an established norm to "trust but verify," especially for business-critical decisions. Indeed, the obstacles hindering widespread acceptance of business analytics, and the resultant value from the

investments, frequently rest with deficiencies in the population's overall quality and traceability.

Organizations need to be able to quickly assess data quality. The most meaningful assessments come from good-quality business rules, which define what accurate data should look like. Thus BI solutions need to incorporate robust data-quality checking capabilities at all stages of operation. Although the adoption of BI may be limited partly to the population's lack of formal training in statistical and analytical concepts and techniques, good-quality data should enable less-knowledgeable users more comfortably to take advantage of self-service BI tools.

1.4.2. Metadata Management

Regardless of information system architecture, enterprise intelligence platforms rely on the effective management of metadata. Metadata describes the context, structure, meaning, relationships, characteristics, operational readiness, and quality of information. It enables information integration, discovery, usage, and governance. Without effective metadata management, information integration is not possible and enterprise-level data quality cannot be effectively assured.

Information system metadata can be classified into five categories:

• Technical metadata (data about data): physical information about data (e.g., locations in hardware)

• Process metadata: information about when, where, how, and by whom data is created and the lifecycle of those data

• Domain metadata: definition of terms specific to an enterprise

• Business metadata: information that provides brief descriptions of data and their structures and relationships for end users

• Operational metadata: data quality attributes as defined by users (e.g., freshness, alignment with business rules, accuracy)

Information quality metadata is critical for the integrity of information exchanges. Data areas and source systems need to be assessed against these requirements, and only then can assessment ratings for news quality, report quality, and so on be assigned.

1.5. Technologies Enabling Secure and Governed Intelligence

Secure and governed enterprise intelligence depends on underlying technologies that provide essential capabilities. A suitable real-time enterprise platform must support natural-language observations for continuous enterprise intelligence applications. Natural-language observations ease access, reducing the effort to ask the right questions to derive actionable insights. Extra-linguistic integrations simplify expression of insights. Integration simplifies and enriches product architectures, ensuring real-time availability and consistency across the intelligence pillars.

With the extended enterprise and third-party data resources warranting third-party compute services, secure and governed enterprise intelligence relies on cloud platforms that can deliver and compute effectively in real time. Natural-language interface and modelling capabilities depend on machine-learning capabilities that can be usefully triggered with relatively few labelled training examples or interactively refined by power users as part of a broader model-management capability.

The technologies underlying secure and governed enterprise intelligence have reached sufficient maturity to enable real-time implementations in a business-friendly manner. Secure and governed enterprise intelligence can achieve suitable configurations through judicious sourcing and integration of services and capabilities delivered both as business APIs and cloud services in real time.

1.5.1. Analytics Platforms and Compute Separation

A compute separation architecture with clear Tier-0 and Tier-1 control principles is a key characteristic of an Analytics platform. The key purpose of Analytics is to deliver Business Intelligence (BI), Data Science models, and Advanced Analytics nudges to support informed decisions, predictive views, and control of the future. Achieving a reliable outcome often requires analysing a large volume of data and spending a significant amount of time in a Tier-0 compute platform. The objective should be to lessen the chances of a Tier-0 requirement and at least execute queries that can operate at scale. Rather than reinventing the wheel, analytics use the Business Intelligence, Data Marts, and Data Warehouse frameworks built by the Data Operations Domain. This setup should empower a self-service enterprise standard for BI that is integrated, governed, and trusted.

Tier-1 Analytics should be for Data Science modelling and Advanced Analytics capabilities, leveraging best-of-breed Data Science, AI, ML, and Advanced Analytics frameworks. These models could either be cost-optimised or perform basic predictions or recommendations, or fast-in-colour-and-3D deep-analysis models that tap the Tier-0 compute class. ML- and AI-based nudges for each domain convert Advanced Analytics

into a virtual Tier-0. This setup enables heavy nudges but diminishes the control and trust aspect. Here Advanced Analytics becomes strong-enough nudges, explaining the detected patterns on the data but not indicating the way forward. Such nudges should be supplied from Third-Parties to lessen the risk exposure while enabling deeper understanding and acceptance.

1.5.2. Data Lakes, Warehouses, and Lakehouses

An enterprise data lake stores raw data that can be transformed into formats that a data lake house or data warehouse can consume. Enterprise data lakes surface new analytic capabilities by offering data consumers the flexibility to freely explore all the available raw data while simultaneously enabling analytics teams to efficiently stage and prepare data for consumption via lakehouse tables. Some of these analytics are performed by data scientists working for the enterprise, while other data consumers are typically line of business users seeking answers to business questions using simple reporting or visualization tools enterprise architecture.

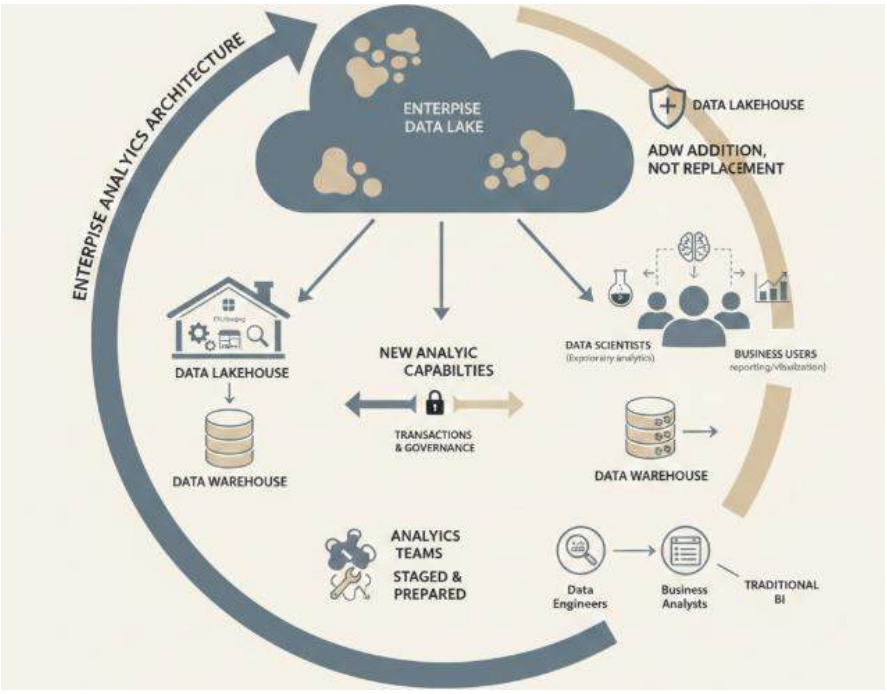

Fig 1.3: The Tripartite Analytics Architecture: Integrating Data Lakes, Lakehouses, and Warehouses for Multi-Persona Enterprise Intelligence

Enterprise data warehouses are the most traditional repositories for analytics but do not support the breadth of analytics required in today's organizations. In recent years, a new

class of data repositories called data lakehouses have emerged to fill this gap. While still nascent, the concept of a data lakehouse combines features from both data warehouses and data lakes with the support of ACID transactions that enable both BI use cases and Machine Learning workloads. Such capabilities, among others, make lakehouses an important addition to the enterprise analytics architecture, yet they cannot replace data warehouses. Aside from governance, a second reason why prevention clause-on-architectures should be heeded is that different types of analytics teams need different types of analytics solutions. Data scientists, data engineers, and line of business analysts require the ability to explore and analyze large sets of easily accessible data. A data lake provides this capability and is, therefore, an important component of enterprise analytics architecture.

1.6. Risk Management and Compliance

Regulatory compliance is a significant driver for the adoption of data protection technology, but key management aspects are frequently neglected. Over 65 percent of respondents indicated that their organizations deploy monitoring and alerting solutions merely to fulfill specific regulatory requirements rather than acting as a baseline for risk management.

The GDPR, PCI-DSS, and SOX regulations are three of the most important in the industry. Nonetheless, only slight differences can be identified in how organizations in different regions respond to them:

- The GDPR is the regulation that commands most attention in Europe, although PCI-DSS is still adopted by a high percentage of organizations in the continent.

- In North America, the weighting attributed to PCI-DSS is even more accentuated.

- Although the Sarbanes-Oxley act has little explicit relevance to Europe, it is still recognized as a key regulation.

A large percentage of organizations highlight the importance of risk management and compliance, but the actual implementation within companies remains flawed. Data protection for security and risk management should be viewed as a holistic combination of technology for prevention, detection, and response with a security/theft protection compliance burden priority-serving mindset, rather than as a roundabout solution just to satisfy regulatory obligations.

1.6.1. Regulatory Frameworks and Standards

In today's world, enterprises are required to comply with a variety of international, federal and state laws, regulations and industry standards. Laws governing privacy, data protection, information security, quality assurance, digital marketing, consumer protection, environmental protection, financial reporting and other aspects of operation apply to enterprises in every industry. The General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) are significant pieces of privacy legislation, with worldwide implications. Compliance with such regulatory frameworks and industry standards can significantly increase the level of risk against which the enterprise needs to protect itself. Regulatory change is also an important consideration; the emergence of artificial intelligence and machine learning systems, the use of big data and analytical models, and further regional regulatory initiatives make additional privacy regulations likely.

Non-compliance creates a very real business risk. Violations can lead to lawsuits, civil actions, fines, penalties and loss of business, as well as damage to reputation and customer trust. The growing consequences of breaches mean that data mining may often be used as prosecutorial evidence, to the detriment of the enterprise and the individuals involved. As failure to comply with legislation can also be viewed as a failure of governance, boards of directors must ensure that their organizations are aware of applicable regulations and comply with them. Privacy impact assessments can be employed to assess the likely effects of systems and projects on privacy and data protection rights. Further, establishing appropriate privacy policies is a common requirement and essential good practice.

1.6.2. Risk Assessment Methodologies

Active risk management requires the ongoing assessment of threats and vulnerabilities that may affect the enterprise's ability to achieve its objectives, along with the consideration of risk mitigation. Standard assessment methodologies in this area include the probabilistic risk assessment; the qualitative risk assessment; and the quantitative risk analysis.

Probabilistic risk assessment (PRA) is widely applied in the risk management of complex engineering systems, such as nuclear energy systems, space missions, and large-scale manufacturing plants. The methodology entails the identification of mission-critical functions within individual (sub)systems, the modeling and propagation of failure probabilities, and the subsequent analysis of the failure consequences—characteristically using fault and event tree analysis techniques.

Qualitative risk assessment (QRA) combines a significance-based categorization of hazards with expert opinion on vulnerability. Technically, the process culminates in a prioritization of risks in terms of the significance of their possible impact (effect value) and the perceived likelihood of their occurrence (occurrence value). A risk matrix summarizes the prioritized risks, forming a basis for risk mitigation planning. QRA is well suited to smaller enterprises and emergent problems, or where resources are insufficient for undertaking a more thorough assessment. As an alternative, the same principles may be applied in a systems assessment of safe enterprise operation with respect to risk acceptance criteria.

1.7. Conclusion

Information technology evolves at an unrelenting pace, but the fundamentals of using physical systems to replicate human cognition remain unchanged: build reliable models of the world, act based on inferences derived from those models, and observe those actions to detect unmodelled phenomena. The research and development of enterprise intelligence has explored this process from technical, security, and governance perspectives to determine how businesses can successfully leverage information technology to enhance insight and decision making. Enterprise intelligence is an application of enterprise architecture principles to enable enterprise-wide sensor and actuator networks to implement information systems capable of satisfying a defined decision performance envelope. It is akin to an application of the Internet of Things paradigm to support business psychology and involves the safer and more efficient application of artificial intelligence within an enterprise context.

The enterprise intelligence discussion framework provides deeper enterprise architecture insights and practical heuristics into enabling the secure, governed, and trustworthy application of artificial intelligence to critical helper functions. The managed separation of enterprise questions and answers greatly simplifies the enabling architecture by separating knowledge creation from knowledge application, thus removing concerns over algorithmic labor replacement. Business-as-usual job task execution can comfortably coexist with exploratory app development—potentially even driving it—ensuring organizational learning of emergent KDD toolsets. The on-demand nature of KDD potentially enables cost-effective enablement of a managed system of insight and intelligence, on top of a secure and governed managed information system. It is important for enterprise architecture practitioners, especially designers of managed information systems, to recognize the underlying analogy with the Internet of Things to appreciate instantiation needs and minimal design requirements for operation.

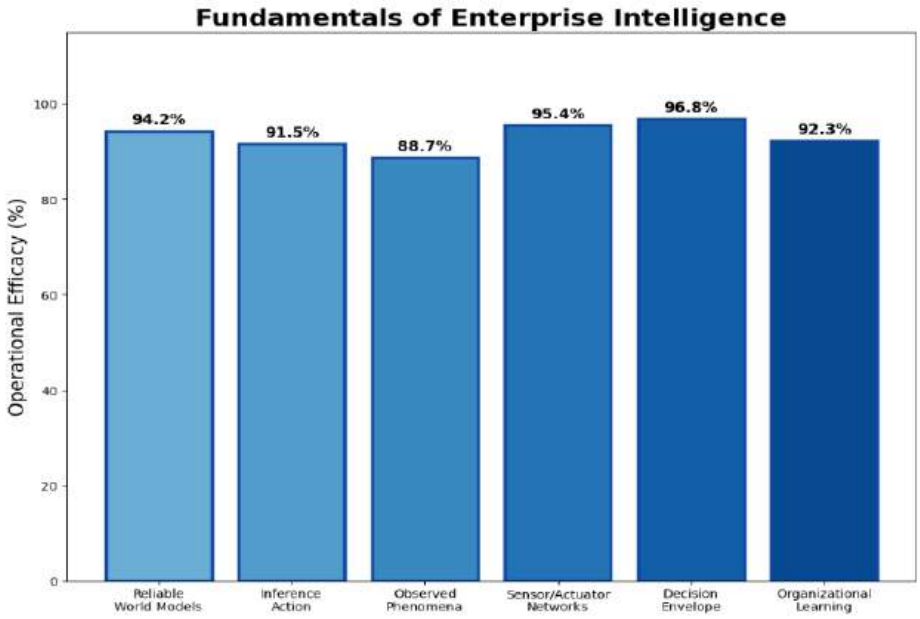

Fig 1.4: Fundamentals of Enterprise Intelligence

1.7.1. Key Takeaways and Future Directions

Enterprise intelligence forms the basis for an enterprise to become an intelligent enterprise—one that can learn and adapt over time. The key learnings from the development of an enterprise-intelligence foundation can be summarised into four clusters.

First, for an enterprise to obtain insights into business activities, capabilities, and needs across the life span of business, the basis for this enterprise intelligence must be built on an enterprise-wide repository of structured and unstructured information covering the relevant past experiences and the requisite knowledge of stakeholders and advisory/external residents (e.g., customers, suppliers). Second, to ensure that the enterprise can trust the insights and conclusions stemming from the modelling and analysis of these information resources, the required and enabled level of enterprise intelligence must be governed by a business intelligence framework and supporting governance processes and solutions. Third, for the above-mentioned enterprise intelligence to become actionable intelligence for higher-level business modelling and decision-making for subsequent business activities, the lower-level intelligence must be continuously processed in real time, augmented with business rules, risk assessment, and business-value-impact factors. For these models and decisions to become executable, the related business activities must be supported by task-centric and personalized intelligent assistants.

Fourth, while these clusters focus on the acquisition of business insights and intelligence for a particular business execution or cycle phase, for the future orientation of the enterprise, the information warehouse also needs to include future business trends predicted by external agents or the collective business intelligence of the prediction market combined with the real-time social sentiment analysis system for the functioning country or industry. Moreover, the intelligence-for-intelligence cycle of the prediction market mentioned above also contributes toward the foundation for continual enterprise adaptation.

References

European Commission. (2024). Artificial intelligence act. Publications Office of the European Union.

Thutari, R. T., Garapati, R. S., BM, M., & RK, S. (2025, October). Adaptive Access Control and Authentication Management for IoT Using Attention-GRU and Reinforcement Learning. In 2025 2nd International Conference on Software, Systems and Information Technology (SSITCON) (pp. 1-6). IEEE.

Varshney, K. R. (2020). Trustworthy machine learning. XRDS, 27(2), 30–35.

GUNTUPALLI, R. (2025). EXPLAINABLE AI IN CLINICAL DECISION SUPPORT: INTERPRETABLE NEURAL MODELS FOR TRUSTWORTHY HEALTHCARE AUTOMATIONEXPLAINABLE AI IN CLINICAL DECISION SUPPORT: INTERPRETABLE NEURAL MODELS FOR TRUSTWORTHY HEALTHCARE AUTOMATION. TPM–Testing, Psychometrics, Methodology in Applied Psychology, 32(S9 (2025): Posted 15 December), 462-471.

Stahl, B. C., Timmermans, J., & Mittelstadt, B. (2021). Ethics of computing: A systematic literature review. ACM Computing Surveys, 54(2), 1–38.

Floridi, L., Cowls, J., Beltrametti, M., et al. (2022). The European approach to artificial intelligence: AI Act and beyond. Philosophy & Technology, 35(1), 1–17.

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. (2020). Regulating a revolution. Fordham Journal of Corporate & Financial Law, 23(1), 31–103.

Kshetri, N., & Voas, J. (2022). Blockchain-enabled financial services. IEEE Security & Privacy, 20(1), 35–43.

Bai, T., Zheng, Z., Ren, K., & Shi, S. (2024). Cloud-native machine learning systems. IEEE Software, 41(1), 50–58.

Aitha, A. R., & Jyothi Babu, D. A. (2025). Agentic AI-Powered Claims Intelligence: A Deep Learning Framework for Automating Workers Compensation Claim Processing Using Generative AI. Available at SSRN 5505223.

Chen, Y., & Zhang, L. (2022). Data engineering for real-time analytics. IEEE Transactions on Services Computing, 15(4), 2288–2302.

PIONEERING SELF-ADAPTIVE AI ORCHESTRATION ENGINES FOR REAL-TIME END-TO-END MULTI-COUNTERPARTY DERIVATIVES, COLLATERAL, AND ACCOUNTING AUTOMATION: INTELLIGENCE-DRIVEN WORKFLOW

COORDINATION AT ENTERPRISE SCALE. (2025). Lex Localis - Journal of Local Self-Government, 23(S6), 8598-8610. https://doi.org/10.52152/a5hkbh02.

Newman, S. (2021). Building microservices (2nd ed.). O'Reilly Media.

Vajpayee, A., Khan, S., Gottimukkala, V. R. R., Sharma, D., & Seshasai, S. J. (2025). Digital Financial Literacy 4.0: Consumer Readiness for AI-Driven Fintech and Blockchain Ecosystems. International Insurance Law Review, 33(S5), 963-973..

Gounaris, A., & Tzortzis, G. (2021). Platforms for scalable data analytics and AI in the cloud. Journal of Cloud Computing, 10(1), 45.

Rongali, S. K. (2025, August). Deep Learning for Cybersecurity in Healthcare: A Mulesoft-Enabled Approach. In 2025 International Conference on Artificial Intelligence and Machine Vision (AIMV) (pp. 1-6). IEEE.

Kief, M. G., & Bick, G. (2021). Digital transformation in financial services. Springer.

Nagabhyru, K. C., Rani, M., Reddy, D. S., & Krishnaraj, V. (2025, August). Machine Learning-Driven Fault Detection in Electric Vehicles via Hybrid Reinforcement Learning Model. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-6). IEEE.

Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2021). Homomorphic encryption: A survey. ACM Computing Surveys, 54(6), 1–35.

Taddeo, M., & Floridi, L. (2022). Artificial intelligence as a force for good. Science, 361(6404), 751–752.

Jobin, A., Ienca, M., & Vayena, E. (2019). Global landscape of AI ethics guidelines. Nature Machine Intelligence, 1, 389–399.

Makridakis, S., Spiliotis, E., & Assimakopoulos, V. (2022). Statistical and machine learning forecasting methods. PLOS ONE, 17(3), e0265480.

Lim, B., Arık, S. Ö., Loeff, N., & Pfister, T. (2021). Temporal fusion transformers. International Journal of Forecasting, 37(4), 1748–1764.

Segireddy, A. R. (2025). GENERATIVE AI FOR SECURE RELEASE ENGINEERING IN GLOBAL PAYMENT NETWORK. Lex Localis: Journal of Local Self-Government, 23.

van der Aalst, W. M. P. (2021). Process mining. Springer.

Gama, J., Žliobaitė, I., Bifet, A., et al. (2020). Concept drift adaptation. ACM Computing Surveys, 46(4), 44.

Amistapuram, K. (2025). Agentic AI for Next-Generation Insurance Platforms: Autonomous Decision-Making in Claims and Policy Servicing. Journal of Marketing & Social Research, 2, 88-103.