

DIGITAL CFO SOLUTIONS

MANAGING FINANCE IN THE AI ERA — TRAINING SERIES

MODULE 7

AI-Enabled Enterprise Risk Management, Internal Controls, Compliance and Governance

From periodic assurance to continuous, predictive governance intelligence

Risk Sensing

Internal Controls

Compliance

Fraud Prevention

AI Governance

About This Module



How this module is structured and how to get the most from it



Read

Work through each numbered section in sequence



Reflect

Pause at each Executive Insight and Knowledge Check



Apply

Relate each concept to your own risk and control environment



Review

Use the Key Takeaways slide as a revision summary

MODULE FORMAT

This module contains four short Knowledge Checks, five illustrative case studies, illustrated process lifecycles, an Annexure quick-reference guide, and a closing summary. Allow approximately 75–95 minutes for a first read-through.



What You Will Be Able to Do (1 of 2)

- 1** Explain how AI is transforming ERM from periodic, reactive assessment into continuous, predictive risk intelligence.
- 2** Evaluate AI-enabled techniques including real-time risk sensing, scenario modelling, Digital Twins and continuous monitoring.
- 3** Assess how AI strengthens internal controls through Continuous Controls Monitoring, automated testing and SoD analysis.
- 4** Explain how AI enhances regulatory compliance through regulatory intelligence and continuous compliance monitoring.



What You Will Be Able to Do (2 of 2)

- 5** Evaluate AI's use in fraud detection and financial-crime prevention through behavioural and network analytics.
- 6** Apply responsible AI governance principles including transparency, explainability, accountability and human oversight.
- 7** Develop an integrated AI-enabled Governance, Risk and Compliance (GRC) framework aligned with strategy and risk appetite.



What This Module Covers

Six themes across the enterprise Governance, Risk and Compliance landscape

7.1–7.2

Evolution

From periodic review to continuous intelligence

7.4

Internal Controls

Continuous Controls Monitoring

7.6

Fraud Detection

Behavioural and network analytics

—

Case Studies

Five illustrative AI scenarios

7.3

Enterprise Risk

The AI-enabled ERM lifecycle

7.5

Compliance

Regulatory intelligence and reporting

7.7

AI Governance

Responsible AI and Board oversight

—

Summary

Key takeaways and module review



SECTION 7.1

Introduction: Risk Management Enters the Age of Continuous Intelligence

Analysing financial, operational, customer, supply chain, market and external data in near real time



Risk Management Enters the Age of Continuous Intelligence

- Risk is inherent in business — financial volatility, operational disruption, regulatory change, cybersecurity threats, geopolitical uncertainty and climate-related events.
- Traditional ERM has relied largely on historical data, periodic reviews, and manual controls, making risk identification relatively reactive.
- AI can identify emerging risks, detect anomalies, assess control effectiveness, predict potential failures, and support timely corrective action.

CENTRAL MESSAGE

The CFO's challenge is to integrate ERM, internal controls, compliance, fraud prevention, cybersecurity and AI governance into a unified Governance, Risk and Compliance (GRC) framework.



SECTION 7.2

The Evolution of Risk Management in the AI Era

From traditional to AI-enabled intelligent risk management

7.2 THE EVOLUTION

From Traditional to AI-Enabled Intelligent Risk Management



Traditional Risk Management	AI-Enabled Intelligent Risk Management
Periodic risk assessments	Continuous risk monitoring
Historical reporting	Predictive and prescriptive analytics
Silo-based risk functions	Integrated enterprise risk intelligence
Rule-based monitoring	Machine learning and adaptive analytics
Reactive incident response	Early warning and proactive intervention
Periodic scenario planning	Digital Twin and dynamic scenario simulation



KNOWLEDGE CHECK 1

What role do Digital Twins play in AI-enabled enterprise risk management?

- A They automatically accept material risks on management's behalf
- B They enable organizations to simulate disruptions and strategic alternatives before decisions are implemented** 
- C They eliminate the need for a risk appetite statement
- D They replace the Board's responsibility for risk oversight

Why: Digital Twins enable organizations to simulate disruptions and strategic alternatives before decisions are implemented, helping management balance risk, resilience and opportunity — but they do not transfer accountability for risk.



SECTION 7.3

AI-Powered Enterprise Risk Management (ERM)

AI strengthens each stage, creating a continuous and adaptive risk-management process



The AI-Enabled Enterprise Risk Management Lifecycle

1

Intelligent Risk Identification

Continuously scans internal and external data for emerging risk signals.

2

Dynamic Risk Assessment

Updates likelihood and impact assessments as conditions change.

3

Predictive Risk Analytics

Forecasts potential risk events before they materialize.

4

Scenario Analysis & Digital Twins

Simulates disruptions and strategic alternatives before implementation.

5

Continuous Risk Monitoring

Tracks key risk indicators and exposures in near real time.

6

Intelligent Risk Response

Recommends and coordinates mitigation and corrective action.

7

Continuous Learning

Refines models as new risk events and outcomes are observed.



Key Enterprise Risks Managed Using AI

Risk Category	Illustrative AI Application
Strategic	Market intelligence, forecasting and scenario analysis
Financial	Liquidity, covenant and financial-risk monitoring
Credit & Market	Default prediction; interest rate, FX and commodity risk modelling
Operational	Process anomalies, failures and operational disruption
Supply Chain & Third Party	Supplier health, concentration and logistics risk
Cybersecurity	Threat detection and incident intelligence
ESG & Climate	Climate scenarios, emissions and sustainability-risk analytics

7.3 ENTERPRISE RISK



Illustration: The AI-Driven Enterprise Risk Dashboard



A compact dashboard should focus on critical indicators rather than every available metric.



KNOWLEDGE CHECK 2

What is the recommended design principle for an AI-enabled Enterprise Risk Dashboard?

- A It should display every available risk metric to be comprehensive
- B It should focus on critical indicators such as top emerging risks, KRIs and risk-appetite utilization rather than attempting to show every metric** 
- C It should only show historical, backward-looking data
- D It should be updated no more than once per year

Why: The chapter is explicit that a compact dashboard should focus on critical indicators rather than attempting to display every available risk metric — clarity and focus matter more than exhaustive coverage.



SECTION 7.4

AI-Enabled Internal Controls

From sample-based testing to full-population assurance

7.4 INTERNAL CONTROLS

From Sample-Based Testing to Full-Population Assurance



Traditional Internal Controls	AI-Enabled Internal Controls
Manual approvals and workflows	Intelligent workflow automation
Sample-based testing	Full-population transaction analysis
Rule-based controls	Adaptive, risk-based analytics
Retrospective detection	Predictive and early-warning controls
Manual reconciliations	Automated intelligent reconciliations
Manual exception review	AI-prioritized exception management



AI Across the Internal Control Lifecycle

1

Intelligent Control Design

Designs controls proportionate to risk and process complexity.

2

Continuous Controls Monitoring

Evaluates transactions and control activities continuously.

3

Automated Control Testing

Tests control operation across complete populations.

4

Intelligent Segregation of Duties

Detects SoD conflicts across systems and roles.

5

Intelligent Reconciliations

Automates matching and identifies reconciling items.

6

AI-Based Exception Management

Prioritizes exceptions by financial and control significance.

7

Continuous Control Assessment

Assesses control design and operating effectiveness continuously.



Internal Controls Across Business Processes

Business Process	Illustrative AI-Enabled Controls
Revenue-to-Cash	Revenue anomalies, credit monitoring, pricing validation
Procure-to-Pay	Duplicate invoices, vendor anomalies, approval compliance
Record-to-Report	Journal monitoring, reconciliations, close controls
Treasury	Payment authorization, liquidity and FX controls
Payroll	Employee anomalies, payroll reconciliation, access controls
Inventory & Fixed Assets	Inventory variances, asset verification, depreciation checks

ON CONTINUOUS ASSURANCE

Continuous Assurance does not eliminate independent audit or professional judgement. It enables Internal Audit to focus greater attention on high-risk exceptions, model reliability and systemic control weaknesses.



SECTION 7.5

AI in Compliance and Regulatory Reporting

From periodic review to continuous compliance



From Periodic Review to Continuous Compliance

Traditional Compliance	AI-Enabled Continuous Compliance
Periodic compliance reviews	Continuous regulatory monitoring
Manual regulatory research	AI-driven regulatory intelligence
Spreadsheet-based tracking	Integrated compliance dashboards
Reactive remediation	Predictive compliance-risk management
Static compliance registers	Dynamic compliance-risk scoring



AI-Enabled Compliance Management Lifecycle

1

Regulatory Intelligence

Monitors and classifies regulatory publications across jurisdictions.

2

Regulatory Impact Assessment

Maps new requirements to affected entities and processes.

3

Continuous Compliance Monitoring

Tracks compliance status against requirements continuously.

4

Automated Regulatory Reporting

Assembles and validates data for regulatory submissions.

5

Compliance Risk Analytics

Scores and prioritizes compliance risk exposures.

6

Automated Policy Management

Drafts and maintains policies aligned with current requirements.

7

Regulatory Examination Support

Prepares evidence and responses for regulatory examinations.



Major Compliance Areas Supported by AI

Compliance Domain	Illustrative AI Applications
Financial Reporting	Accounting compliance and disclosure validation
Tax	GST/VAT validation, tax analytics and transfer-pricing review
Data Privacy & Cybersecurity	Privacy, access and security-compliance monitoring
ESG & Sustainability	Sustainability-data validation and regulatory disclosures
Treasury	Covenants, sanctions and investment-limit monitoring
Corporate Governance	Policy compliance and governance reporting



KNOWLEDGE CHECK 3

Who remains responsible for determining applicability, interpretation and formal compliance conclusions when AI is used?

- A The AI system itself, once regulatory intelligence is generated
- B Qualified professionals — AI can identify regulatory developments and map them to processes, but interpretation and conclusions require human judgement** 
- C No one; formal compliance conclusions are no longer required
- D Only the external regulator

Why: Qualified professionals must determine applicability, interpretation and formal compliance conclusions — AI supports continuity and coordination but does not replace professional compliance judgement.



SECTION 7.6

AI in Fraud Detection and Financial Crime Prevention

From rule-based detection to adaptive fraud prevention



From Rule-Based Detection to Adaptive Fraud Prevention

Traditional Fraud Management	AI-Enabled Fraud Prevention
Rule-based detection	Adaptive machine learning models
Reactive investigation	Predictive fraud analytics
Individual transaction review	Behavioural and network analytics
Static fraud rules	Continuously learning models
Manual case prioritization	AI-driven risk scoring
Isolated fraud systems	Integrated enterprise fraud intelligence



AI-Enabled Fraud Management Lifecycle

1

Fraud Risk Identification

Identifies areas of highest inherent fraud exposure.

2

Behavioural Analytics

Builds behavioural baselines for customers and employees.

3

Anomaly Detection

Flags deviations from expected patterns in near real time.

4

Fraud Risk Scoring

Assigns dynamic risk scores to transactions and entities.

5

Intelligent Investigation Support

Assembles evidence and case summaries for investigators.

6

Continuous Fraud Prevention

Embeds preventive controls into transaction workflows.

7

Continuous Learning

Refines models as new fraud typologies emerge.



AI in Anti-Money Laundering and Financial Crime

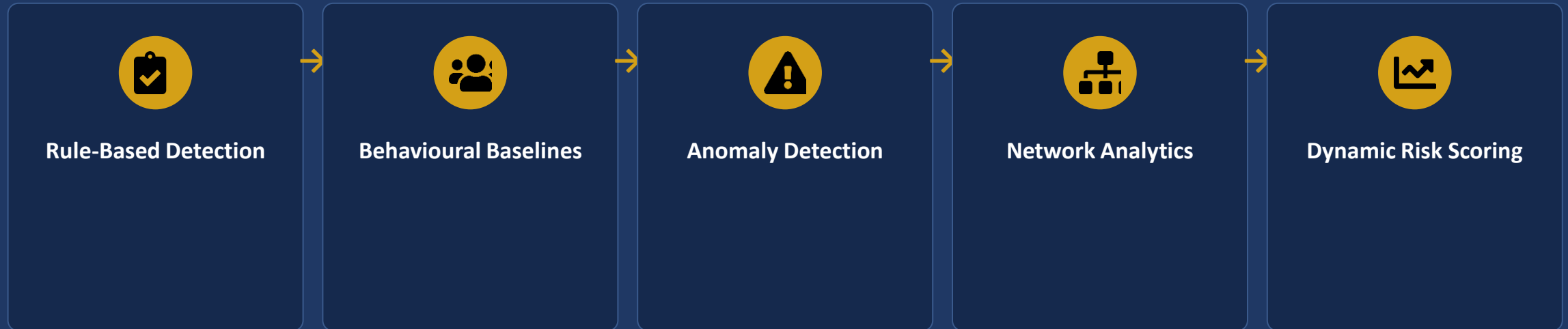
Area	Illustrative AI Applications
KYC & Customer Due Diligence	Identity verification, beneficial ownership, PEP, sanctions and adverse-media screening
Transaction Monitoring	Cross-border payments, high-risk jurisdictions, structuring and rapid movement of funds
Network Analytics	Shell companies, hidden ownership, circular transactions and collusive networks

GOVERNANCE AND HUMAN OVERSIGHT

AI can identify patterns, prioritize cases and support preventive action, but it cannot determine intent or culpability on its own. Professional scepticism, procedural fairness and independent oversight remain essential.



From Rules to Relationship Intelligence



EXECUTIVE INSIGHT

Machine learning and graph analytics can identify emerging patterns, hidden connections and coordinated activity that predetermined thresholds may not capture.



KNOWLEDGE CHECK 4

Why do modern fraud-detection systems combine behavioural and network analytics with rules-based detection?

- A Because rules-based systems can detect every possible fraud scheme on their own
- B Because machine learning and graph analytics can identify emerging patterns, hidden connections and coordinated activity that predetermined rules may not capture** ✓
- C Because network analytics eliminates the need for any human investigation
- D Because behavioural analytics only applies to customers, not employees

Why: Traditional rule-based approaches may fail to identify emerging or previously unseen patterns, while machine learning and graph analytics can identify hidden relationships and coordinated activity that rules alone would miss.



SECTION 7.7

AI Governance, Ethics, Cybersecurity and Responsible AI

Building trust in AI-enabled financial decision-making



Pillars of Responsible AI



Transparency & Explainability



Accountability



Fairness



Privacy



Security



Reliability & Safety



Human Oversight



Sustainability

AI Model Lifecycle Governance



Governance should be proportionate to the materiality, complexity, autonomy and potential impact of the application.

AI-SPECIFIC CYBERSECURITY THREATS

Data poisoning, prompt injection, model theft, adversarial attacks, unauthorized access, API compromise, deepfake fraud, identity spoofing, model manipulation, and sensitive-data leakage should be integrated with the enterprise cybersecurity framework.



AI Governance Across the Three Lines Model

Governance Function	Primary Responsibilities
First Line – Business & Finance	Own AI use cases, validate outputs, operate controls, maintain human oversight
Second Line – Risk, Compliance & InfoSec	Establish policies, oversee model and regulatory risks, assess ethical issues
Third Line – Internal Audit	Provide independent assurance over AI governance, models, controls and compliance
Board / Audit Committee	Oversee AI strategy, risk appetite, governance principles and material AI-related risks



The CFO's Role in AI Governance

- Aligning finance-related AI initiatives with strategy and risk appetite.
- Ensuring material financial models and outputs are reliable and explainable.
- Supporting strong data and model governance.
- Coordinating with Risk, Compliance, Technology, Cybersecurity, Legal and Internal Audit.
- Reporting material AI risks, performance and governance matters to executive management and the Board.

Ensuring AI strengthens rather than compromises financial integrity and enterprise governance.



Key Takeaways from Module 7

- AI transforms ERM from periodic assessment into continuous, forward-looking risk intelligence — at greatest value when integrated with enterprise decision-making.
- An AI-generated alert does not establish that a control breach or fraud has occurred; professional judgement, reliable evidence and procedural fairness remain essential.
- Fraud and financial-crime detection benefit from combining rules with behavioural and relationship analytics that predetermined thresholds may not capture.
- Greater AI authority requires stronger controls — permissions, approval thresholds and audit trails should become progressively stronger as authority increases.
- Management and the Board retain accountability: AI may detect, predict, explain and recommend, but it does not set risk appetite or assume fiduciary responsibility.



Questions Finance Leaders Are Asking

Q: What is Continuous Controls Monitoring (CCM)?

A: Technology and analytics that continuously evaluate transactions and control activities, identify exceptions, and prioritize high-risk issues across entire populations.

Q: Why has AI governance become a Board-level responsibility?

A: AI increasingly influences strategic, financial and regulatory decisions, so the Board should oversee material AI risks, ethics and alignment with strategy.

Q: Can AI replace professional judgement in finance?

A: No. AI strengthens analysis and automation, but accountability for significant decisions remains with management and the Board.

Q: What are the principal cybersecurity risks associated with AI systems?

A: Data poisoning, prompt injection, model theft, adversarial attacks and sensitive-data leakage — governed within the broader cybersecurity framework.

Combining Intelligent Automation with Responsible Governance



THE CENTRAL MESSAGE

AI enables organizations to move from periodic and reactive processes toward continuous, predictive and integrated governance. Technology alone cannot ensure effective governance — sustainable AI adoption requires reliable data, robust controls, cybersecurity, ethical principles and clear accountability.

LOOKING AHEAD

Module 8 examines how AI is transforming Strategic Finance, Financial Analysis, Capital Allocation and Investment Decision-Making.



SECTION 7.8

Illustrative Case Studies: AI Across Enterprise Risk and Governance

Five global organizations applying AI across risk, controls, compliance and fraud prevention

A Note on These Cases



- The following cases are hypothetical composite illustrations developed for learning purposes.
- The organizations, circumstances, and outcomes are fictional.
- Any numerical amounts, timeframes, or performance improvements are illustrative scenario estimates rather than reported results or assured forecasts.
- Each case is broken into three parts: the Business Situation the organization faced, the AI Initiative it undertook, and the resulting Business Impact and lessons.



AI-Powered Enterprise Risk Management

Global Tech Manufacturing Ltd. — Multinational Engineering and Industrial Equipment Manufacturer

- ERM relied on quarterly assessments and manually maintained risk registers.
- Supplier concentration, FX, logistics, cybersecurity, and geopolitical exposures were often identified only after they began affecting operations.

Global Tech Manufacturing: Continuous Enterprise Risk Sensing



Business Situation

ERM relied on quarterly assessments and manually maintained risk registers. Supplier concentration, FX, logistics, cybersecurity, and geopolitical exposures were often identified only after they began affecting operations.



AI Initiative

An AI-enabled ERM platform combined Machine Learning risk prediction, NLP regulatory monitoring, Graph Analytics of supplier dependencies, and selective Digital Twin simulation — with alerts routed under predefined escalation protocols.



Business Impact

The platform revealed excessive supplier dependence, concentrated FX positions, port congestion, and ransomware exposure. Risk reporting moved from a periodic compliance exercise to a continuous, forward-looking process.



AI-Enabled Continuous Internal Controls Monitoring

RetailMart International Ltd. — Multinational Retailer with Stores, Online Channels and Distribution Centres

- Sample-based testing and quarterly reviews meant duplicate payments, unauthorized price overrides, and SoD conflicts were frequently detected only after the relevant accounting period had closed.



RetailMart International: Full-Population Controls Monitoring



Business Situation

Sample-based testing and quarterly reviews meant duplicate payments, unauthorized price overrides, and SoD conflicts were frequently detected only after the relevant accounting period had closed.



AI Initiative

An AI-enabled Continuous Controls Monitoring platform used Machine Learning, Process Mining, and Graph Analytics across ERP, procurement, payroll, and POS systems, automating routine reconciliations and scoring higher-risk exceptions.



Business Impact

Complete transaction populations replaced sampling; exceptions were detected closer to occurrence; exception-resolution and close cycles shortened; and Internal Audit focused on systemic weaknesses and judgemental areas.

CASE STUDY 7.3

AI-Based Fraud Detection and Anti-Money Laundering Monitoring



GlobalTrust Bank Plc. — Multinational Commercial and Investment Bank

- Rule- and threshold-based financial-crime systems generated a high volume of false alerts and struggled to identify mule accounts, synthetic identities, collusive networks, and complex cross-border laundering patterns.

GlobalTrust Bank: Financial Crime Intelligence Platform



Business Situation

Rule- and threshold-based financial-crime systems generated a high volume of false alerts and struggled to identify mule accounts, synthetic identities, collusive networks, and complex cross-border laundering patterns.



AI Initiative

An integrated Financial Crime Intelligence Platform combined behavioural analytics, Graph Analytics of hidden relationships, NLP adverse-media screening, Computer Vision identity verification, and Generative AI investigation summaries.



Business Impact

Dynamic risk scores let investigators focus on higher-risk cases; detection speed and prioritization improved while unnecessary customer interruptions fell — material cases still required authorised human decisions.

CASE STUDY 7.4

AI-Driven Regulatory Compliance and Intelligent Regulatory Reporting



PharmaLife Global Ltd. — Multinational Pharmaceutical and Biotechnology Company

- Compliance spanned financial reporting, GMP/GCP, pharmacovigilance, anti-bribery, privacy, and ESG obligations across jurisdictions — relying on spreadsheets and manual research, causing duplicated work and inconsistent interpretation.



PharmaLife Global: Regulatory Intelligence Platform



Business Situation

Compliance spanned financial reporting, GMP/GCP, pharmacovigilance, anti-bribery, privacy, and ESG obligations across jurisdictions — relying on spreadsheets and manual research, causing duplicated work and inconsistent interpretation.



AI Initiative

An AI-enabled Regulatory Intelligence platform used NLP to classify regulatory publications, Knowledge Graphs to map requirements to entities and processes, and Generative AI to draft policy updates subject to specialist validation.



Business Impact

Management gained earlier visibility of overdue filings, policy gaps, and inspection findings; compliance professionals spent less time gathering information and more time interpreting requirements and advising the business.

CASE STUDY 7.5

Building an Intelligent Enterprise Governance Platform



Global Consumer Products Group — Multinational Manufacturer Grown Through Acquisitions

- Multiple ERP systems, local control practices, and separately maintained risk registers meant interconnected risks — supplier disruption, FX, cyber incidents, control failures — were evaluated independently rather than together.



Global Consumer Products: Intelligent Governance Platform



Business Situation

Multiple ERP systems, local control practices, and separately maintained risk registers meant interconnected risks — supplier disruption, FX, cyber incidents, control failures — were evaluated independently rather than together.



AI Initiative

A three-year programme standardised risk classifications and controls, then progressively introduced Machine Learning anomaly detection, predictive analytics, a controlled AI agent for workflow coordination, and a limited Digital Twin for combined-shock simulation.



Business Impact

Cross-functional risk visibility, transaction coverage, and forecasting improved substantially — following the progression Standardise → Automate → Detect → Predict → Explain → Coordinate → Simulate, with an explicit authority matrix throughout.



Concluding Perspective Across the Five Cases

- Global Tech Manufacturing and RetailMart show how continuous risk sensing and full-population controls monitoring surface exposures far earlier than periodic review.
- GlobalTrust Bank demonstrates how behavioural and network analytics identify hidden fraud and money-laundering patterns that fixed rules alone would miss.
- PharmaLife Global illustrates how regulatory intelligence can free compliance professionals to focus on interpretation and advice rather than information-gathering.
- Global Consumer Products shows that an intelligent governance platform is built progressively — standardize, automate, detect, predict, explain, coordinate, then simulate.
- Across all five cases, AI expands visibility and speed, but professional judgement, escalation protocols, and Board accountability remain central to every material decision.



SECTION 7.9

Annexures: Frameworks, Maturity, and Board Dashboard

Reference frameworks for implementation and Board oversight



AI-Enabled Enterprise Governance Framework

Integrating finance, risk, compliance, cybersecurity and sustainability into one governance ecosystem

Governance Component	AI-Enabled Approach	Primary Benefit
Enterprise Risk Management	Continuous AI-powered risk sensing	Early risk identification and improved resilience
Internal Controls	Continuous Controls Monitoring (CCM)	Stronger control effectiveness, reduced manual effort
Regulatory Compliance	Continuous regulatory intelligence	Reduced compliance risk and improved readiness
Fraud Risk Management	Behavioural, network and predictive analytics	Lower fraud losses and faster detection
Cybersecurity	AI-enabled threat intelligence and anomaly detection	Improved cyber resilience
AI Governance	Formal governance with model validation	Responsible, transparent, explainable AI

AI Governance, Risk and Control (GRC) Maturity Assessment



Level 1: Initial → Level 5: Autonomous Enterprise

Assessment Area	Level 2: Developing	Level 4: AI-Enabled	Level 5: Autonomous Enterprise
Enterprise Risk Management	Quarterly risk reviews	Predictive AI risk analytics	Autonomous continuous risk sensing
Internal Controls	Automated workflows	AI-assisted control optimization	Self-learning adaptive controls
Regulatory Compliance	Compliance software	AI regulatory intelligence	Continuous autonomous compliance
Fraud Detection	Rule-based monitoring	Predictive fraud intelligence	Autonomous fraud prevention
AI Governance	Initial AI policies	Continuous model monitoring	Enterprise-wide Responsible AI governance



Board-Level AI Governance, Risk and Assurance Dashboard

Illustrative thresholds — organizations should calibrate to their own risk appetite

Governance Dimension	Board KPI	Illustrative Target
Enterprise Risk	Enterprise Risk Score	Within approved risk appetite
Financial Controls	Internal Control Effectiveness	>98%
Compliance	Enterprise Compliance Score	>98%
Fraud	Fraud Risk Index	Low
Cybersecurity	Critical Security Incidents	Zero
AI Governance	High-Risk Models Validated	100%



BD CHATTERJEE

FCA, ACMA, ACS, DipIFR ACCA (UK)

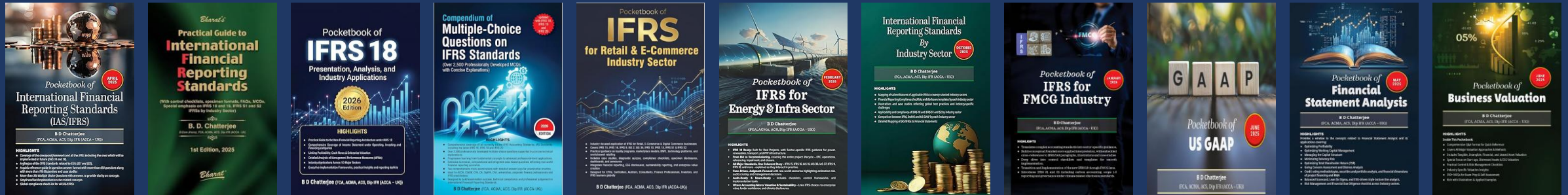
Founder, Digital CFO Solutions

ABOUT THE AUTHOR

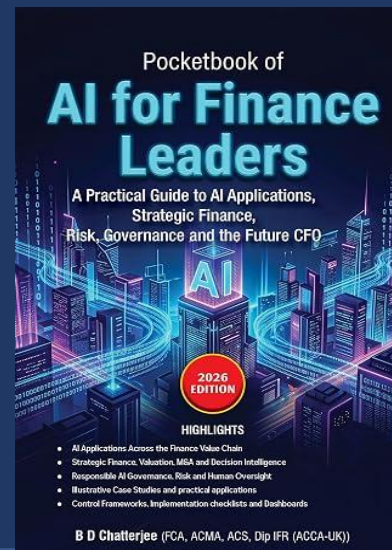
A Career Built on Making Finance Understandable

- Over 35 years of CFO and industry experience across manufacturing, services, and financial reporting leadership roles.
- Author of the Pocketbook of IFRS series and multiple finance titles spanning IFRS, US GAAP, Ind AS, industry applications, and business valuation.
- Builds institutional-grade financial workbooks, IFRS/US GAAP presentation decks, and governance frameworks under the Digital CFO Solutions brand.
- Teacher and mentor to finance professionals worldwide, focused on making complex financial concepts practical and understandable.

Books by B D Chatterjee — IFRS & GAAP Library



Available at bdchatterjee.com • Amazon Kindle & Paperback





THANK YOU

*Module 7: AI-Enabled Enterprise Risk Management,
Internal Controls, Compliance and Governance*

BDCHATTERJEE.COM

Digital CFO Solutions | Managing Finance in the AI Era — Training Series