www.inductusgcc.com

RegTech Unleashed

How Benelux BFSI Gains the Edge with Indian GCCs

2026

Executive SUMMARY

USD 1.23B	+417%	30–40%	50–65%
Regulatory Fines H1 2025	Fine Increase YoY	Cost Reduction via RegTech	GCC Cost Advantage

Global banking regulatory fines reached USD 1.23 billion in the first half of 2025, up 417% year on year. Compliance costs for banks have risen more than 60% since the financial crisis, while new regulatory updates now emerge every seven minutes. For Benelux BFSI institutions, this scale of change exceeds the capacity of in-house teams and legacy systems.

Since 2025, five major EU frameworks have transformed compliance requirements. DORA mandates ICT resilience and continuous monitoring. CRR III and CRD VI implement final Basel III capital and reporting rules. PSD3 strengthens fraud controls and payment security. AMLA now directly supervises the EU's most complex cross-border financial institutions. Together, these frameworks create overlapping obligations that cannot be solved through headcount growth alone.

The global RegTech market is projected to grow from USD 23.43 billion in 2026 to USD 105.23 billion by 2034. Banks deploying RegTech report compliance cost reductions of 30 to 40%. Indian GCCs provide the scale to operationalize this shift, holding 28% of the global GCC AI talent pool and offering a 50 to 65% cost advantage for senior compliance, data governance, and cybersecurity roles. With follow-the-sun operations, GCCs enable continuous monitoring and real-time incident response required under new EU regulations.

STRATEGIC IMPLICATIONS

Benelux banks face simultaneous compliance deadlines across DORA, CRR III, PSD3, and AMLA. The volume and concurrency of these obligations cannot be met through incremental headcount additions in Europe. A technology-led operating model is required.

Indian GCCs offer a 50% to 65% cost advantage at senior compliance and technology roles, combined with access to a talent pool of over 250,000 RegTech-relevant professionals. This cost structure makes GCC-based RegTech delivery the most viable option for institutions under margin pressure.

Institutions that have deployed RegTech solutions report compliance cost reductions of 30% to 40%. GCCs provide the delivery infrastructure to realize those reductions at an enterprise scale across AML, KYC, regulatory reporting, and ICT resilience monitoring.

Compliance is no longer a periodic reporting function. DORA requires continuous operations. Indian GCCs, with follow-the-sun coverage, are structurally suited to support continuous compliance operations that European-only teams cannot maintain at the same cost.

Benelux banks cannot meet concurrent DORA, CRR III, PSD3, and AMLA obligations through incremental European hiring. A technology-led operating model delivered through Indian GCCs is the most viable path forward for institutions facing margin pressure, talent shortages, and escalating regulatory fines.

Table of CONTENT

1.The Compliance Crisis in Benelux Banking

1.1 Rising Regulatory Fines & Enforcement Trends

Global banking regulatory fines reached USD 1.23 billion in the first half of 2025, representing a 417% increase year on year. This explosive spike stabilized in the second half of the year, with H2 2025 adding roughly USD 420 million to bring the full year total to USD 1.65 billion. The aggressive momentum surged right back in the first quarter of 2026, with global penalties racking up USD 542 million in Q1 alone, surpassing the half-year averages of both 2023 and 2024.

European regulators have expanded their enforcement scope beyond traditional AML and KYC violations, using Q1 2026 to crack down heavily on data privacy breaches and ICT operational resilience failures under the newly enacted DORA framework. Within this intensified environment, Benelux institutions continue to account for a disproportionate share of EU-level enforcement actions. This vulnerability is fundamentally driven by their strategic role as European trade hubs, exposing them to immense cross-border transaction volumes and highly complex correspondent banking networks that inherently amplify systemic compliance risks.

Region	Primary Violation Type	Avg. Fine (USD M)	YoY Change
Netherlands	AML / KYC Deficiencies	42.5	310%
Belgium	ICT Resilience Failures	28	290%
Luxembourg	Cross-Border Reporting	34.2	450%
EU Average	Multiple	31.8	380%

Table 1.1: Enforcement Actions by Benelux Country, H2 2025

1.2 Escalating Compliance Operating Costs

Compliance costs for banks have risen more than 60% since the 2008 financial crisis. For mid-to-large Benelux institutions, annual compliance operating expenditure now ranges from EUR 80 million to EUR 350 million. The primary cost drivers include manual KYC processes, fragmented reporting systems, and reactive monitoring architectures.

A new regulatory update now emerges every seven minutes on average across EU member states. Internal compliance teams cannot absorb this volume without structural changes to how compliance is delivered.

1.3 Why Legacy Systems and In-House Teams Are Falling Behind

Most Benelux BFSI institutions operate on core banking platforms that were not designed for real-time compliance monitoring. Regulatory reporting is often managed through batch processes running on daily or weekly cycles. DORA now requires continuous ICT risk monitoring, which batch-based systems cannot support.

In-house compliance teams face acute talent shortages. Roles in regulatory technology, data engineering, and AI-driven transaction monitoring carry salary premiums of 1.5x to 2.5x over standard compliance positions in the Netherlands and Belgium. European labor markets do not have sufficient supply to meet this demand at scale.

1.4 Why Benelux Is a Priority Market

Benelux has emerged as one of the most urgent markets for RegTech-enabled compliance transformation due to a unique convergence of regulatory intensity, enforcement posture, cross-border complexity, and overlapping implementation deadlines.

The region faces one of the highest concentrations of active EU regulatory frameworks. The Digital Operational Resilience Act (DORA) became applicable to all financial entities in January 2025, significantly expanding requirements around ICT resilience, incident reporting, third-party risk management, and continuous monitoring. At the same time, supervisory scrutiny is intensifying. In 2024 alone, the European Central Bank conducted 165 on-site inspections and 78 internal model investigations, with a strong focus on ICT architecture, data governance, and cyber resilience. This level of supervisory activity is materially increasing the operational burden on banks across Belgium, the Netherlands, and Luxembourg.

The enforcement environment is becoming more public and more disciplinary. Belgian regulators are introducing a “name-and-shame” policy from 2026 that will publicly identify banks with repeated AML and compliance breaches. In parallel, the National Bank of Belgium has highlighted persistent gaps in ICT risk management and third-party risk governance across the sector. The shift toward public enforcement significantly raises reputational and financial risk, increasing the need for proactive and continuous compliance capabilities.

Benelux banks operate in one of Europe’s most complex cross-border financial ecosystems. Institutions in the region manage extensive correspondent banking networks and process disproportionately high volumes of cross-border transactions. This complexity increases exposure to fraud, AML, sanctions screening, and regulatory reporting obligations. The presence of globally significant market infrastructure institutions such as Brussels-headquartered Euroclear, which manages large volumes of frozen assets, further amplifies the need for automated, real-time monitoring and reporting capabilities.

Driver	What’s Happening	Compliance Impact
Dense Regulation	DORA, PSD3, AMLA, CCD2, and Basel rules active simultaneously	Multiple overlapping compliance obligations
Stricter Enforcement	Public “name & shame” policy and increased ECB inspections	Higher financial and reputational risk
Cross-Border Complexity	High volume of international transactions and correspondent banking	Greater AML, fraud and reporting burden
Overlapping Deadlines	Several major regulations going live between 2025 and 2026.	Compressed timelines and resource pressure

2.The Five Regulatory Frameworks Reshaping Compliance

EU Regulatory Compliance Timeline for Benelux BFSI Institutions

2.1 DORA: ICT Resilience and Continuous Monitoring

The Digital Operational Resilience Act became effective in January 2025. It requires financial institutions to maintain continuous ICT risk monitoring, conduct regular resilience testing, and report ICT-related incidents within four hours of detection. Institutions must also manage third-party ICT risk across their full vendor ecosystem, including cloud providers, data centers, and technology platforms.

DORA introduces a two-tier supervisory structure. Tier one covers all financial entities. Tier two applies enhanced obligations to critical third-party ICT service providers. Non-compliance carries fines of up to 2% of global annual turnover.

2.2 CRR III and CRD VI: Final Basel III Implementation

CRR III and CRD VI came into force on 1 January 2025. They introduce the output floor, which limits the benefit institutions can derive from internal models for credit risk, operational risk, and market risk. Banks must align their capital calculations with standardized approaches and reports under revised COREP and FINREP templates. Institutions with large internal model portfolios face significant recalibration costs.

2.3 PSD3: Fraud Controls and Payment Security

PSD3 strengthens the requirements introduced under PSD2 by mandating real-time fraud detection for all retail payment transactions. Institutions must implement transaction monitoring systems capable of flagging anomalous patterns within milliseconds. Strong customer authentication requirements are extended to a broader range of payment scenarios, and liability frameworks for authorized push payment fraud are tightened.

2.4 AMLA: Direct Supervision of Cross-Border Institutions

The Anti-Money Laundering Authority assumed AML/CFT mandates from the EBA on 1 January 2026. AMLA has authority to request transaction-level data, conduct on-site inspections, and impose supervisory measures directly. Direct supervision of the highest-risk cross-border financial institutions (approximately 40 entities) is expected by the end of 2027, with AMLA issuing regulatory technical standards through 2026 to establish the framework.

2.5 EU AI Act: High-Risk AI Compliance for Banking

The EU AI Act classifies credit scoring, fraud detection, and customer risk profiling models as high-risk AI systems. Institutions deploying these systems must comply with requirements covering model documentation, bias testing, human oversight, and audit trails.

Key deadline change (May 2026): The European Parliament and Council agreed on 7 May 2026 to postpone high-risk AI obligations. The new compliance deadline is December 2027 (with sector-specific rules delayed to August 2028). Transparency and watermarking obligations remain on track for August and December 2026, respectively. The postponement is pending formal adoption but is expected to take effect before the original August 2026 deadline.

Institutions should continue preparations, as non-compliance carries penalties of up to EUR 30 million or 6% of global annual turnover.

Framework	Effective Date	Primary Obligation	Max Penalty
DORA	Jan 2025	ICT resilience, continuous monitoring, incident reporting	2% global turnover
CRR III / CRD VI	Jan 2025	Output floor, revised capital reporting (COREP/FINREP)	Supervisory capital add-on
PSD3	Mid 2025	Real-time fraud detection, expanded SCA	National regulator discretion
AMLA	1 Jan 2026 (mandate transfer)	Direct AML supervision of high-risk institutions	Up to 10% global turnover
EU AI Act (High Risk)	~~Aug 2026~~ → Dec 2027	Model docs, bias testing, audit trail for AI systems	EUR 30M or 6% turnover

Table 2.1: EU Regulatory Framework Summary for Benelux BFSI

3.RegTech Market Opportunity

3.1 Market Size & Growth Projections (2026-2034)

The global RegTech market is projected to grow from USD 23.43 billion in 2026 to USD 105.23 billion by 2034, at a compound annual growth rate of approximately 20%. This growth is driven by increasing regulatory complexity. the need for automated monitoring systems, and the cost pressure on financial institutions to move away from manual compliance processes.

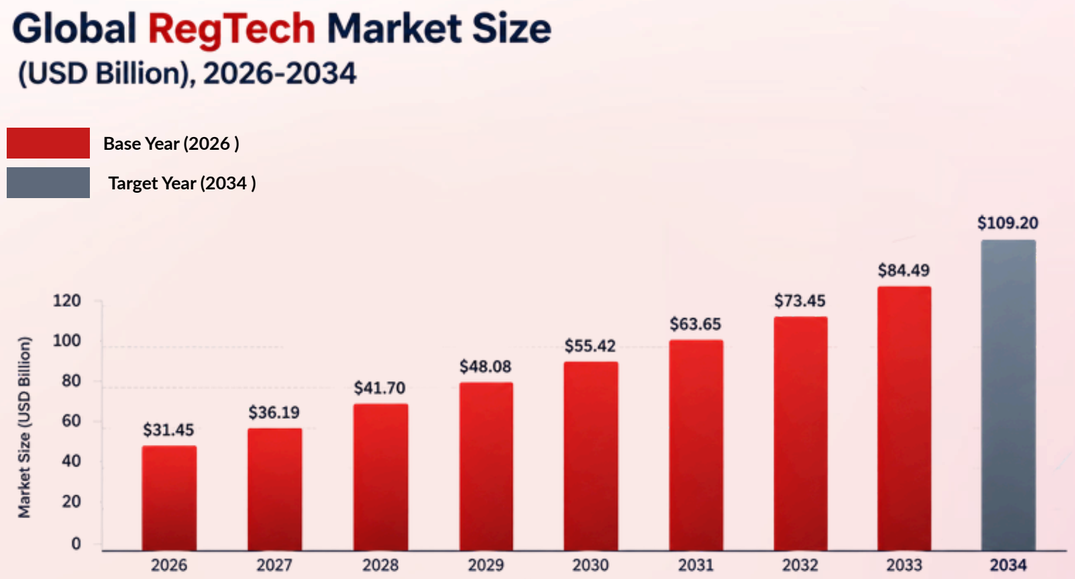


Figure 3.1: Global RegTech Market Size (USD Billion), 2026 to 2034

Investor confidence in RegTech remains strong despite broader fintech market volatility. Global RegTech companies attracted approximately USD 5.6 billion across 157 investment deals in the first half of 2022 alone, reflecting sustained demand for compliance automation and risk management solutions.

3.2 BFSI Share and Adoption Trends

The banking, financial services, and insurance sector accounts for approximately 55% of global RegTech spend. Within this, AML and KYC solutions represent the largest segment, followed by regulatory reporting automation and fraud monitoring. European institutions are among the fastest adopters, driven by the density of new regulatory obligations.

Cloud-native RegTech platforms and API-based regulatory data feeds are displacing on-premise reporting systems. Institutions that have moved to continuous data pipelines report faster incident detection and lower remediation costs.

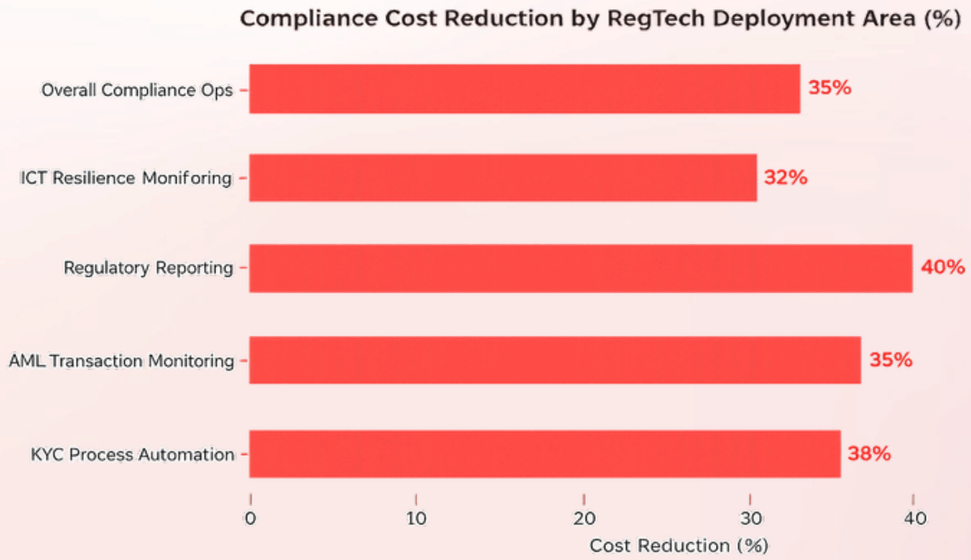
Despite accelerating regulatory complexity, adoption of RegTech solutions across BFSI remains uneven. Industry analysis suggests that awareness and deployment of available RegTech capabilities continue to lag behind market innovation, creating significant opportunity for large-scale adoption.

The rapid digitalization of financial services and increasing complexity of regulatory obligations are accelerating interest in RegTech adoption across BFSI institutions, particularly in areas such as AML, risk management, and regulatory reporting.

> *"According to a recent industry survey, 67% of practitioners in regulated environments cite slow automation adoption as their primary challenge, outpacing compliance reporting and security concerns, highlighting that execution, not intent, is the main barrier."*

3.3 Cost Reduction Evidence

Institutions that have deployed RegTech solutions report compliance cost reductions of 30 to 40% across specific functions. Automated KYC reduces onboarding time from days to hours. AI-driven transaction monitoring reduces false-positive rates in AML alerts by 40 to 60%, freeing analyst capacity for genuine risk cases. Automated regulatory reporting eliminates manual data reconciliation, reducing reporting cycle times by 50 to 70%.



RegTech platforms are increasingly being adopted to automate transaction monitoring, identity verification, regulatory reporting, and risk analytics, enabling financial institutions to improve compliance efficiency while reducing operational overhead.

RegTech solutions leveraging AI, machine learning, blockchain, and big data analytics are increasingly being used to automate compliance workflows, reduce operational inefficiencies, and improve transparency across financial institutions.

RegTech adoption across financial institutions continues to face operational barriers, including legacy infrastructure integration challenges, fragmented data environments, regulatory ambiguity, and cybersecurity concerns. These limitations are making traditional compliance operating models increasingly difficult to scale efficiently.

4.Why Indian GCCs Are the Delivery Mechanism

4.1 Talent Scale & Workforce Dynamics

India-based Global Capability Centres hold 28% of the global GCC AI talent pool. More than 250,000 professionals in Indian GCCs hold skills directly relevant to RegTech delivery, including regulatory data engineering, AI model development, cybersecurity compliance, and automated reporting architecture. The talent pipeline from Indian technology universities produces over 1.5 million STEM graduates annually, providing a sustainable source of trained professionals.

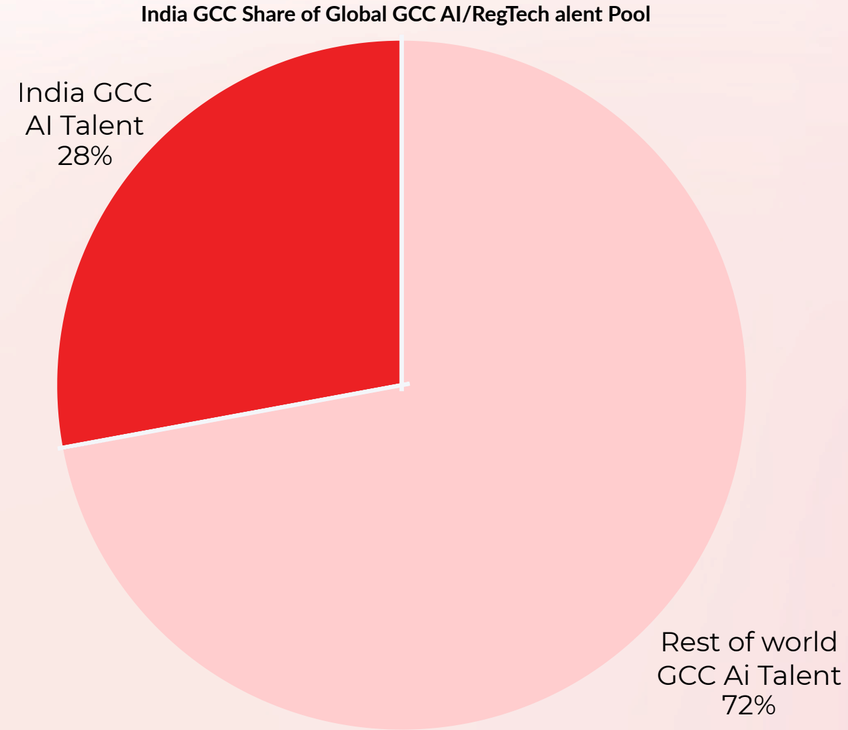


Figure 4.1: India GCC Share of Global GCC AI and RegTech Talent Pool

4.2 Cost Advantage Over Western Europe

Indian GCCs offer a 50 to 65% cost advantage for senior compliance, data governance, and cybersecurity roles relative to equivalent positions in Western Europe. A senior compliance data engineer in Amsterdam or Brussels costs between EUR 130,000 and EUR 160,000 per year in total employment costs. The equivalent role in a Bengaluru or Hyderabad GCC costs between EUR 52,000 and EUR 65,000.

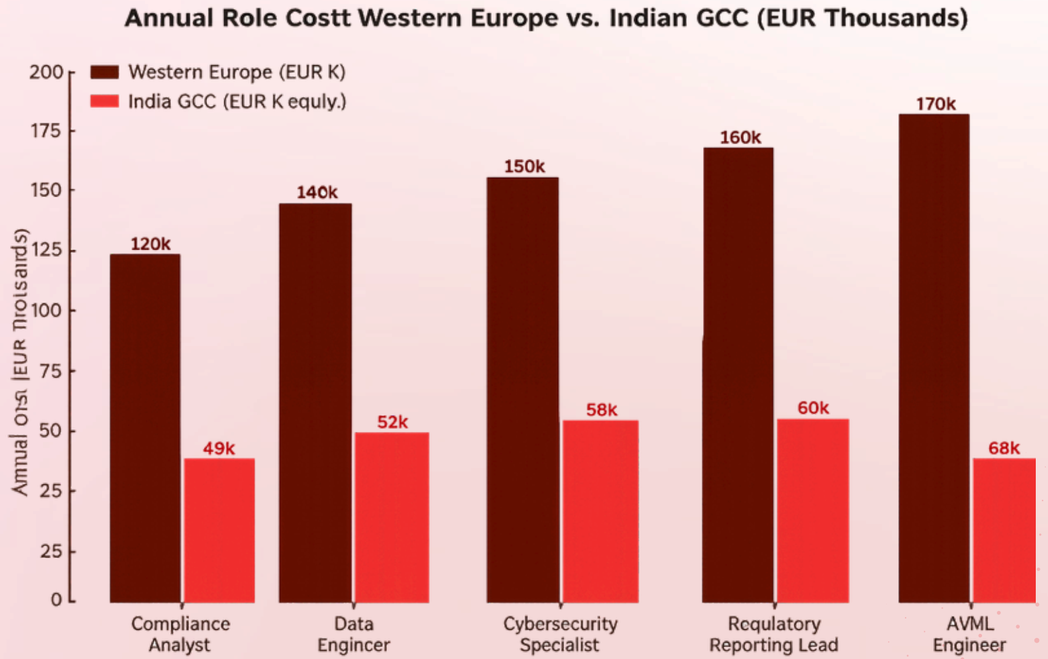


Figure 4.2: Annual Role Cost Comparison, Western Europe vs. Indian GCC (EUR Thousands)

4.3 Capability Shift: Over 50% Expertise and Frontier Work

More than 50% of work delivered from Indian GCCs in the BFSI sector now falls under the category of expert or frontier work, meaning the work requires domain knowledge, judgment, or proprietary system knowledge rather than process execution. This represents a structural shift from the transactional delivery model of the previous decade. GCCs are now building and owning regulatory reporting architectures, AI compliance models, and ICT resilience frameworks rather than executing tasks designed elsewhere.

4.4 Operational Model: Follow-the-Sun Continuous Compliance

DORA requires ICT incident reporting within four hours of detection. This is not achievable with a single-timezone compliance team. Indian GCCs operating on a follow-the-sun model with counterpart teams in Western Europe enable round-the-clock monitoring and immediate escalation paths. Incident detection at 02:00 CET is addressed by an active team in India, with European teams briefed at the start of business.

As financial services become increasingly digital and transaction-intensive, compliance operations are shifting toward continuous monitoring models requiring scalable, real-time operational support across geographies.

"GCCs operating on a follow-the-sun model with counterpart teams in Western Europe enable round-the-clock monitoring and immediate escalation paths. According to the Nasscom-Zinnov 2026 report, 64% of Indian site leaders now hold global mandates, reflecting the strategic integration of Indian GCCs into global operating models."

4.5 Hub-and-Spoke Operating Model for BFSI Compliance

Benelux institutions are adopting a hub-and-spoke model in which strategy, regulatory interpretation, and stakeholder management remain in Europe while technology delivery, data operations, and monitoring functions are executed from Indian GCCs. This model preserves regulatory proximity while achieving cost efficiency at scale.

Function	Hub Location	Spoke Location	Primary Output
Regulatory Interpretation	Amsterdam / Brussels	N/A	Policy and control frameworks
KYC Automation	Strategy in EU	Hyderabad / Bengaluru GCC	Automated onboarding workflows
AML Monitoring	Oversight in EU	Pune / Bengaluru GCC	Real-time alert management
Regulatory Reporting	Governance in EU	Bengaluru GCC	COREP / FINREP automated outputs
ICT Resilience Ops	CISO office in EU	Multi-site GCC	Continuous monitoring and response

5.Talent Gaps and Workforce Trends in BFSI GCCs

5.1 The AI and Data Talent Gap in BFSI

who require additional reskilling to meet role requirements. The gap is most acute in roles that combine regulatory knowledge with technical implementation capability, such as regulatory data engineers and compliance AI specialists. Indian GCCs are addressing this gap through structured training programmes aligned to EU regulatory frameworks.

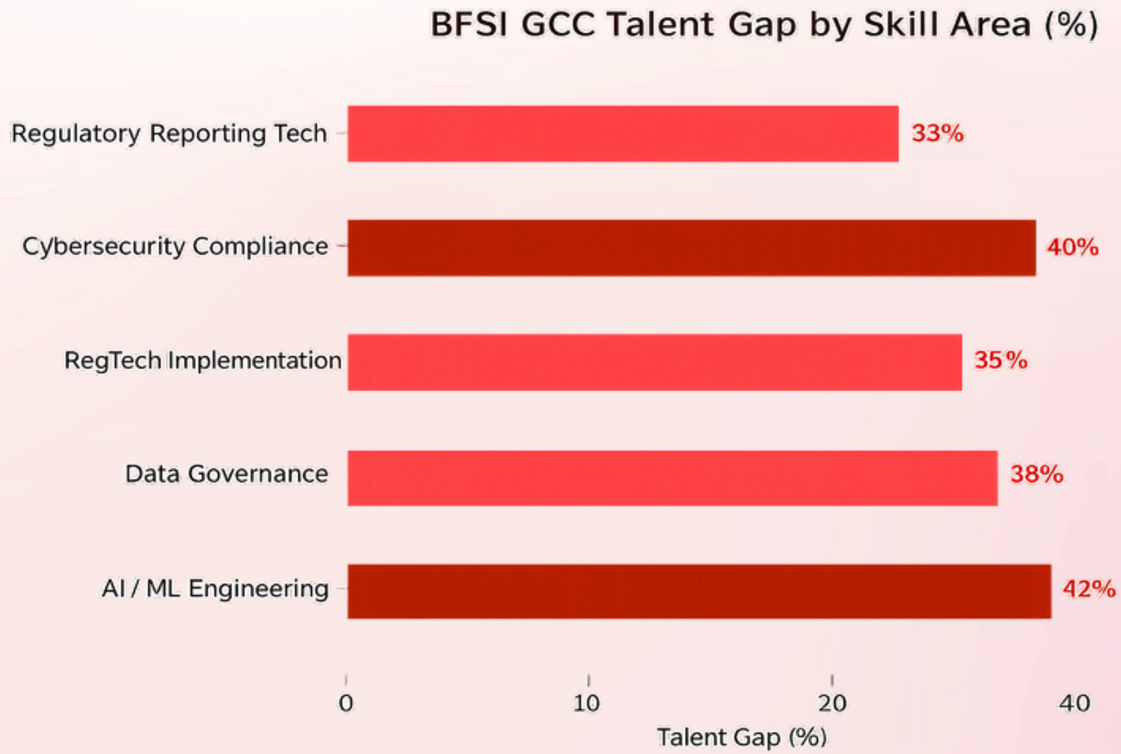


Figure 5.1: BFSI GCC Talent Gap by Skill Area (%)

5.2 Salary Premiums: 1.5x to 2.5x for Specialised Roles

Specialized roles in RegTech, AI compliance, and regulatory data architecture command salary premiums of 1.5x to 2.5x over standard compliance analyst compensation in both European and Indian markets. In India, this has led to competitive hiring among GCCs, with institutions investing in structured career paths and long-term retention programmes to reduce attrition in critical roles.

The premium varies by sector. Investment banking GCCs offer the highest compensation across most roles, followed by retail and commercial banking . A data scientist in investment banking earns between ₹22.1 lakh and ₹46.9 lakh annually, while those in retail banking earn ₹19.9-44.5 lakh.

5.3 Replacement Hiring and Gen Z Tenure Trends

Gen Z professionals entering GCC workforces show median tenure of 18 to 24 months before seeking role changes, compared to 36 to 48 months for Millennial cohorts. Replacement hiring has surged significantly. According to the Quess Corp report, replacement hiring now accounts for 40% of all recruitment activity. This trend is driven by shifting workforce dynamics, specifically a decline in Gen Z tenure expectations to under 24 months.

Kapil Joshi, CEO of Quess IT Staffing, commented:

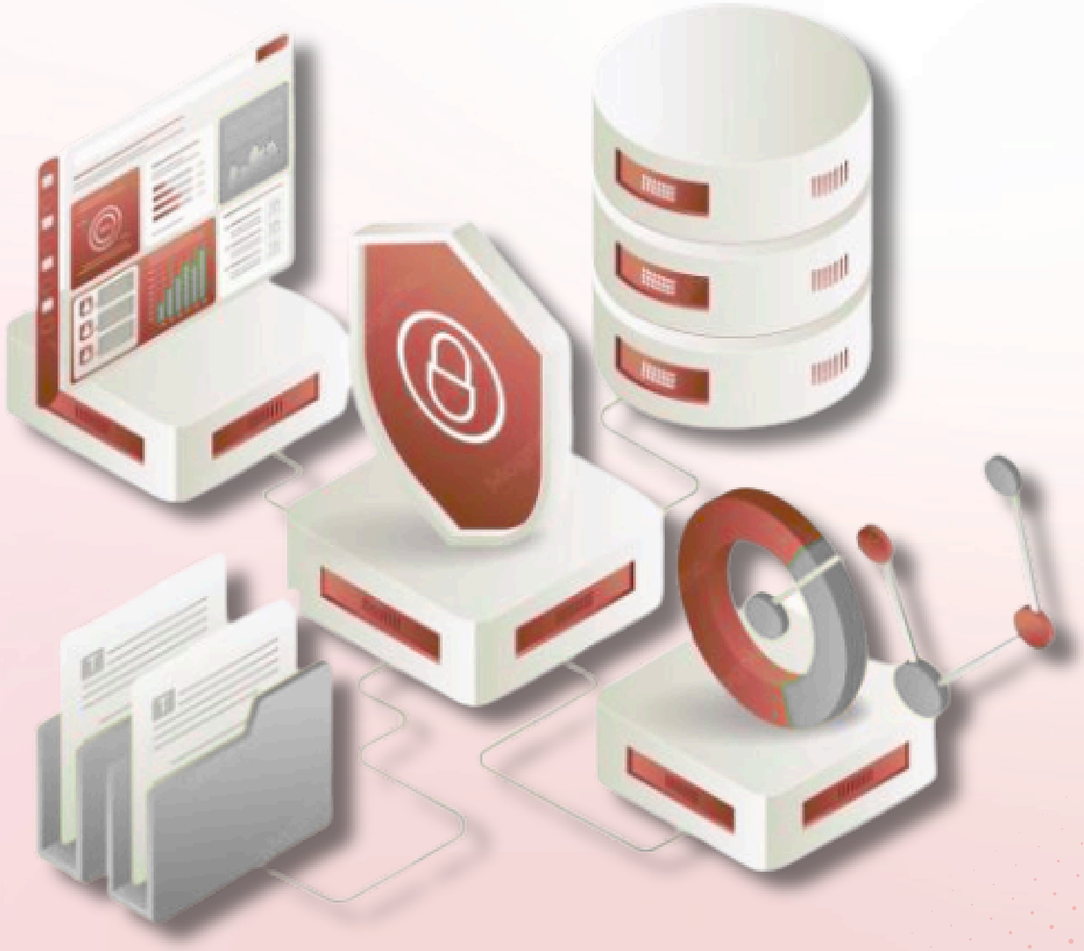
"We are witnessing a structural shift: a higher volume of recruitment is being diverted to replacement roles as tenure cycles shorten. This is prompting organizations to rethink how they build depth in their talent pools."

5.4 Flexible Staffing Models for Compliance Surges

GCCs are responding by building flexible staffing models to manage compliance surges. According to a Careernet study cited by the Economic Times, flex hiring adoption in GCCs has grown from 18% in 2024 to 22% in 2025 and is expected to reach 25% by 2026, meaning one in four roles could soon be contractual. The top drivers include cost optimization, business agility, and access to niche expertise. This allows institutions to scale teams during peak periods such as year-end reporting, new framework implementation, or regulatory audit cycles, without the long-term cost commitments of permanent European hiring.

5.5 Data Governance as the Foundation for Compliance

Regulatory frameworks, including CRR III, DORA, and the EU AI Act, all require institutions to demonstrate data lineage, data quality controls, and audit trails for compliance-relevant data. Data governance has therefore become a foundational capability rather than a support function. Indian GCCs with mature data governance practices are operating as centers of excellence for this capability.



6.Recent Trends in GCC Evolution for BFSI Compliance

6.1 Rise of Compliance Engineering as a Core GCC Function

Compliance engineering, meaning the design and build of automated compliance workflows, monitoring systems, and reporting pipelines, has emerged as a distinct function within BFSI GCCs over the past 18 months. Institutions are establishing dedicated compliance engineering teams in India that own the technical architecture of their regulatory technology stack rather than executing builds designed by European counterparts.

6.2 AI and Automation in KYC and Transaction Monitoring

AI-driven KYC platforms deployed from Indian GCCs are reducing customer onboarding times from an average of five to seven business days to under four hours and, in some cases, from days to minutes for standard retail profiles. For complex institutional clients, AI-assisted document review reduces analyst review time by approximately 60% and overall turnaround time by up to 82% . In transaction monitoring, machine learning models reduce false-positive AML alert rates by 40 to 60%, with some platforms reporting reductions of 75-80%, allowing analyst teams to focus on genuine risk cases.

6.3 DORA-Aligned ICT Risk Management from India

Several Benelux institutions have established DORA-aligned ICT risk operation centers in India. These centers run continuous infrastructure monitoring, conduct scenario-based resilience testing aligned to European Banking Authority guidelines, and maintain the incident log required under DORA reporting obligations. The follow-the-sun model ensures four-hour incident reporting obligations are met regardless of when incidents occur.

Under DORA, ICT-related incidents must be reported within four hours of detection, with continuous resilience testing required, including Threat-Led Penetration Testing (TLPT). The follow-the-sun model with Indian GCCs enables Benelux institutions to meet these obligations while maintaining 24/7 monitoring coverage.

6.4 Growth of Regulatory Reporting Architecture Teams

Regulatory reporting is moving from manual spreadsheet-based processes to automated data pipelines connected directly to core banking systems. Indian GCCs are building and maintaining these architectures, covering COREP and FINREP under CRR III, transaction reporting under EMIR and MiFID II, and AML reporting under AMLA obligations. Teams of 15 to 40 data engineers and reporting specialists are operating as dedicated regulatory reporting centers of excellence.

6.5 GCC Expansion for BFSI Operations

Hyderabad, Bengaluru, Pune, and Chennai have seen significant expansion in BFSI GCC operations since 2023. Hyderabad in particular has attracted multiple Benelux institutions due to its combination of cost, infrastructure, and talent density in financial technology. New GCC setups are now completing operational ramp-up within 12 to 18 months, compared to 24 to 36 months five years ago.

The BFSI GCC market is projected to grow from approximately 40 billion to 125-135 billion by 2032, with high-skill roles growing at 15-20% annually. Hyderabad has emerged as a particularly attractive destination due to the following:

- 30-40% lower office leasing costs compared to Mumbai and Bengaluru.
- The BFSI Consortium anchored in Hyderabad (HSBC, JPMorgan Chase, State Street, and LSEG) is co-creating curriculum to train up to 10,000 students annually.
- 11.4 million sq ft of office absorption in 2025, with GCCs driving nearly half of demand.

7.Case Studies Benelux Banks Moving Compliance to Indian GCCs

7.1 Dutch Retail Bank: KYC Automation via Hyderabad GCC

A Dutch retail bank serving 4.2 million retail customers faced mounting pressure from De Nederlandsche Bank (DNB) and the European Banking Authority (EBA) to modernize its Know Your Customer (KYC) and Anti-Money Laundering (AML) operations. The bank operated on legacy batch processing systems that required six business days for standard customer onboarding, creating operational friction and regulatory exposure.

The bank established a dedicated KYC automation center in Hyderabad in early 2024, leveraging India's talent pool of regulatory data engineers and AI compliance specialists.

RegTech Solutions Deployed:

The Hyderabad GCC deployed an AI-driven RegTech platform for document verification and risk scoring featuring:

- Automated identity document extraction and validation using computer vision models.
- Risk-scoring algorithms trained on Dutch sanctions lists and transaction patterns.
- API-based integration with the bank's core onboarding systems.
- Real-time screening against watchlists and politically exposed person (PEP) databases.

This deployment mirrors actual RegTech adoption by Dutch financial institutions. ING, a Dutch multinational bank, has deployed generative AI specifically for "improving KYC and compliance" and reducing "the documentation burden in KYC processes,

making it easier and faster for customers to onboard." FMO, the Dutch entrepreneurial development bank, selected Fenergo's Client Lifecycle Management (CLM) RegTech platform to "streamline KYC and onboarding processes" and centralize customer due diligence, documentation, and onboarding workflows.

• Operational Model

The Hyderabad team of 120 engineers, data scientists, and compliance analysts operates under a hub-and-spoke model. Regulatory interpretation and policy decisions remain with the Amsterdam headquarters, while RegTech delivery, data operations, and monitoring functions are executed from India. This preserves regulatory proximity while achieving cost efficiency at scale.

Metric	Before GCC Deployment	After GCC Deployment	Outcomes
KYC Onboarding Time (Standard)	6 business days	Under 3 hours	95% reduction
Annual KYC Operating Cost	EUR 28M	EUR 17M	39% reduction
False Positive Rate (AML alerts)	34%	18%	47% reduction
Regulatory Breach Incidents	7 per year	1 per year	86% reduction

Table 7.1: Dutch Retail Bank KYC Automation Outcomes

• Key Success Factors

The Hyderabad team now owns the platform roadmap and regulatory update cycle, rather than executing builds designed by European counterparts. This ownership model reflects the broader shift of Indian GCCs from "transactional service providers to centers of excellence" for RegTech delivery.

Regulatory Context: Under DORA, financial institutions must maintain dynamic asset inventories and immutable audit trails for all ICT risk management activities. The automated KYC RegTech platform documented above enables continuous evidence collection rather than periodic attestations, aligning with Dutch supervisory expectations.

7.2 Belgian Financial Services Group: DORA Resilience Testing from Pune

A Belgian financial services group with operations across six EU member states confronted the January 2025 effective date of the Digital Operational Resilience Act (DORA). The Act requires all EU financial entities and their third-party ICT providers to use a unified framework for managing ICT risk, including continuous monitoring, incident reporting, and resilience testing.

The group established a DORA compliance operations team in Pune in late 2024, recognizing that the four-hour incident reporting requirement could not be met with a single-timezone European compliance team.

- **RegTech Solution Deployed:**

  The Pune team of 85 ICT risk engineers and compliance specialists runs an integrated DORA compliance program structured around the five pillars of ICT risk management, each supported by RegTech platforms:

- **Operational Model**

  The Pune team operates on a follow-the-sun model with counterpart teams in Brussels. Incident detection at 02:00 CET is addressed by an active team in India, with European teams briefed at the start of business. This ensures the four-hour incident reporting obligation is met regardless of when incidents occur.

  Real-world RegTech context: The National Bank of Belgium (NBB) confirms that DORA has been applicable since 17 January 2025, covering credit institutions, payment institutions, and other financial entities . The NBB's ITA team (ICT and cyber risk center of expertise) uses an "increasingly wide array of sources and tools," including "documentation, questionnaires, test results, incident and threat reports, registers, etc.," to supervise compliance—all of which are RegTech-enabled capabilities.

DORA Pillar	RegTech Function	Implementation Evidence
ICT Risk Management	Dynamic asset inventories tracking dependencies across infrastructure, applications, data flows	Configuration management databases synchronized hourly with cloud, on-premises, and SaaS
Incident Reporting	Automated detection workflows and pre-built notification templates	Four-hour reporting to National Bank of Belgium; automated incident classification
Digital Operational Resilience Testing	Quarterly threat-led penetration testing (TLPT) aligned with EBA guidelines	Scenario-based testing frameworks; documented recovery times
Third-Party Risk Management	Comprehensive registers of ICT service providers	Vendor risk management platforms; real-time service-level dashboards
Information Sharing	Secure channels for threat intelligence exchange	Integration with SIEM systems; sector-specific threat platforms

- **Outcomes**

Metric	Result
DORA Incident Reporting Compliance (Q1 2025)	Zero breaches
Annual ICT Resilience Operating Cost	44% lower than equivalent European headcount model
Team Size	85 ICT risk engineers and compliance specialists
TLPT Frequency	Quarterly, aligned with EBA guidelines

- **Key Success Factors**

The group met its first DORA incident reporting obligations without breach in Q1 2025. The Pune team maintains the DORA incident register and runs continuous scenario-based resilience testing aligned to EBA guidelines.

Regulatory Context: Under DORA, failure to comply carries fines of up to 2% of total annual worldwide turnover for financial entities and non-critical providers. The National Bank of Belgium conducts both scheduled audits and targeted inspections to verify DORA compliance. Banks that maintain continuous, immutable audit trails through RegTech platforms demonstrate control effectiveness more convincingly than institutions that gather evidence only after audit announcements.

7.3 Luxembourg Private Bank: Regulatory Reporting Architecture from Bengaluru

A Luxembourg private bank serving high-net-worth clients across 14 jurisdictions faced escalating regulatory reporting burdens under CRR III, CRD VI, and the impending AMLA framework. The bank operated on a legacy COREP and FINREP reporting system that required 12 manual intervention points per reporting cycle, creating significant operational risk and compliance exposure.

Luxembourg serves as Europe's largest investment fund domicile and the world's second largest, managing approximately €5.9 trillion in assets under management. The country is the domicile for funds managed by 98 of the top 100 European asset managers. As a result, satisfying the rigorous delegation and oversight standards set by the Luxembourg regulator (CSSF) is the de facto benchmark for any GCC targeting the wider European fund industry.

The bank migrated its regulatory reporting architecture to a Bengaluru GCC team in mid-2024, recognizing the need for automated, verifiable reporting pipelines.

• RegTech Solution Deployed

The Bengaluru team of 60 data engineers and reporting specialists rebuilt the bank's COREP and FINREP reporting pipelines on a cloud-native RegTech platform, featuring:

- Direct API connections to core banking systems, eliminating manual data reconciliation.
- Automated validation rules aligned with EBA reporting taxonomy.
- Human review required only for exception cases.
- Immutable audit trails capturing all data transformations for regulatory inspection.

Real-world RegTech context: The CSSF has issued multiple circulars that make RegTech adoption essential:

- Circular 25/882 requires financial entities to maintain and annually submit a "Register of Information" covering all ICT third-party arrangements, with submission deadlines between 28 February and 31 March each year. This is a RegTech record-keeping function.

- The CSSF mandates that "all ICT services" from third parties—including "cloud-based accounting software; portfolio/fund management tools such as Yardi, eFront, or Aladdin; and market information services"—must be listed in DORA's Register of Information.

- Under Circular 18/698, IFMs must notify the CSSF of "material changes" to delegation structures, including portfolio management delegations and sub-delegations—a process managed through the CSSF's eDesk Portal, a RegTech submission system.

• Operational Model

The Bengaluru GCC operates under a delegation framework compliant with CSSF requirements. Under directives such as AIFMD, European supervisory authorities (ESMA) heavily scrutinize delegation arrangements to ensure the authorized EU management company maintains sufficient substance and does not become a "letterbox entity." The bank maintains detailed documentation of all delegated functions through RegTech platforms and conducts annual substance reviews.

Metric	Before GCC Deployment	After GCC Deployment	Change
Reporting Cycle Time (COREP/FINREP)	14 days	48 hours	86% reduction
Manual Intervention Points	12 per cycle	0 (exception-only)	100% elimination
Team Size	Not applicable (dispersed)	60 dedicated specialists	N/A

- **Key Success Factors**

The Bengaluru team has since extended the architecture to cover AMLA transaction reporting requirements. The automated submission system runs fully with human review only for exception cases, dramatically reducing regulatory filing risk.

Regulatory Context: The exhaustive nature of EBA, DORA, and AIFMD compliance suggests that the most strategic opportunity lies not just with the largest institutions but with mid-tier European firms that lack internal resources to independently manage compliance complexity. A pre-vetted, compliant Indian GCC that adopts this RegTech blueprint can lower friction for market entry. Professional bodies such as ICAI Luxembourg act as strategic connectors, providing institutional credibility and localized interpretation required to align policies.

Case Study	GCC Location	Team Size	Primary Function	Key Outcome
Dutch Retail Bank	Hyderabad	120	KYC/AML Automation	38% cost reduction, 95% faster onboarding
Belgian Financial Services	Pune	85	DORA ICT Resilience and Risk Management	44% cost reduction, DORA-compliant ops
Luxembourg Private Bank	Bengaluru	60	Regulatory Reporting (COREP/FINREP/AMLA) & Delegation Oversight	86% faster reporting cycle

Table 7.2: Benelux BFSI GCC Case Study Summary

Key Takeaways for Benelux Banking Leaders

4 Concurrent EU Frameworks Active Since Jan 2025	250k+ RegTech Professionals in Indian GCCs	EUR 105B RegTech Market Size by 2034	7 min Avg Interval Between New Regulatory Updates

Benelux banks face compliance obligations that are concurrent, complex, and technology-dependent. DORA, CRR III, PSD3, and AMLA each requires different technical capabilities, but all require a shift from periodic, manual compliance processes to continuous, automated operations.

The RegTech market provides the tools to make this shift. Indian GCCs provide the delivery capacity, cost structure, and talent depth to implement and operate these tools at the scale Benelux institutions require.

Institutions that delay this transition face two compounding risks. First, continued exposure to regulatory fines as enforcement intensity increases. Second, a widening cost disadvantage relative to peers that have already shifted to technology-led compliance models.

Priority Action	Timeline	Primary Regulatory Driver	Expected Outcome
Establish GCC-based KYC automation team	Q3 2025	AMLA, PSD3	30-40% KYC cost reduction
Deploy DORA-aligned ICT monitoring from GCC	Q2 2025	DORA	Four-hour incident reporting compliance
Migrate COREP/FINREP reporting to automated pipeline	Q4 2025	CRR III	Reduction from 14-day to 48-hour reporting cycle
Build AI model audit trail capability	Q4 2027	EU AI Act (postponed to December 2027)	Compliance readiness ahead of new deadline
Establish data governance centre of excellence	Q3 2025	DORA, CRR III, EU AI Act	Unified data lineage across all compliance functions

Table 8.1: Priority Actions for Benelux BFSI Leaders

Recommendations

- Shift from Incremental Hiring to Technology-Led Operations
- Institutions should evaluate whether their current compliance operating model is designed for the volume and pace of regulatory change now in force. Adding European headcount to address DORA, CRR III, and AMLA obligations simultaneously is not financially viable for most Benelux institutions. The first action is a structured assessment of which compliance functions can be automated or restructured through technology and which require human judgment that must remain in-region.
- Leverage GCC-Based RegTech Delivery
- For institutions without an existing GCC presence, a phased entry through a managed GCC provider allows operational ramp-up within 12 months without the capital commitment of a fully owned entity. Institutions with existing GCCs should assess whether current RegTech delivery capabilities match the requirements of DORA, CRR III, and AMLA, and build a structured roadmap to close the gap.
- Build for Continuous Monitoring, Not Periodic Reporting
- DORA requires ICT incident detection and reporting on a continuous basis. The compliance architecture must be redesigned around event-driven data pipelines rather than batch reporting cycles. This means investing in real-time data infrastructure, automated alert management, and follow-the-sun operational coverage from GCC locations.
- Prepare for EU AI Act Compliance by December 2027
- The EU AI Act classifies credit scoring, fraud detection, and customer risk profiling as high-risk AI systems, requiring model documentation, bias testing, human oversight, and audit trails.
- Deadline Update (May 2026): The European Parliament and Council postponed high-risk AI obligations to 2 December 2027 (from 2 August 2026). High-risk AI embedded in products moves to 2 August 2028.
- Immediate Action Required: Transparency obligations (watermarking, user notifications) apply from 2 December 2026. Prohibited AI practices and AI literacy requirements have been applicable since February 2025.
- Indian GCCs with model governance experience can accelerate compliance. Institutions should use the postponement to build documentation, testing frameworks, and audit trails ahead of December 2027.

Conclusion

Global banking regulatory fines reached USD 1.65 billion in the full year 2025, with USD 542 million recorded in Q1 2026. Compliance costs for banks have increased by more than 60 percent since 2008. A new regulatory update emerges every seven minutes on average across EU member states.

Four EU regulatory frameworks are active as of 2025. DORA requires ICT resilience and incident reporting within four hours. CRR III and CRD VI mandate revised capital reporting under COREP and FINREP templates. PSD3 requires real-time fraud detection for retail payment transactions. AMLA assumed AML/CFT mandates from the EBA on 1 January 2026.

The global RegTech market is projected to grow from USD 23.43 billion in 2026 to USD 105.23 billion by 2034. Institutions that have deployed RegTech solutions report compliance cost reductions of 30 to 40 percent. Automated KYC reduces onboarding time from days to hours. AI-driven transaction monitoring reduces false positive rates in AML alerts by 40 to 60 percent. Automated regulatory reporting reduces reporting cycle times by 50 to 70 percent.

Indian GCCs hold 28 percent of the global GCC AI talent pool. More than 250,000 professionals in Indian GCCs hold skills relevant to RegTech delivery. Indian GCCs offer a 50 to 65 percent cost advantage for senior compliance, data governance, and cybersecurity roles relative to Western Europe. More than 50 percent of work delivered from Indian GCCs in the BFSI sector falls under expert or frontier work. GCCs operate on a follow-the-sun model with counterpart teams in Western Europe.

Across BFSI GCCs globally, 42 percent of AI and data engineering positions remain unfilled or are filled by professionals requiring additional reskilling. The gap is most acute in roles that combine regulatory knowledge with technical implementation capability. Gen Z professionals in GCC workforces show median tenure of 18 to 24 months. Replacement hiring accounts for 40 percent of all recruitment activity.

Flex hiring adoption in GCCs has grown from 18 percent in 2024 to 22 percent in 2025 and is expected to reach 25 percent by 2026.

Benelux institutions face compliance obligations that are concurrent and technology-dependent. The RegTech market provides the tools for continuous automated operations. Indian GCCs provide the delivery capacity, cost structure, and talent depth to implement and operate these tools at the scale Benelux institutions require.

Glossary

Term	Definition
AIFMD	Alternative Investment Fund Managers Directive. EU directive regulating managers of alternative investment funds.
AMLA	Anti-Money Laundering Authority. EU agency responsible for AML/CFT supervision of high-risk cross-border financial institutions.
AML	Anti-Money Laundering. Legal framework and processes to prevent money laundering and terrorist financing.
API	Application Programming Interface. Set of protocols for software application communication and data exchange.
BFSI	Banking, Financial Services, and Insurance. Industry sector covering banks, financial service providers, and insurance companies.
Benelux	Belgium, the Netherlands, and Luxembourg. Regional economic union of three European countries.
CEN	European Committee for Standardization. Organization that develops technical standards for goods and services in Europe.
CENELEC	European Committee for Electrotechnical Standardization. Organization that develops technical standards for electrical and electronic products in Europe.
CFT	Countering the Financing of Terrorism. Legal framework and processes to prevent financial support for terrorist activities.
CLM	Client Lifecycle Management. Process of managing customer relationships from onboarding to offboarding.
COREP	Common Reporting. EU standardized reporting framework for solvency and capital adequacy of financial institutions.
CRR III	Capital Requirements Regulation III. EU regulation implementing Basel III capital and reporting rules.
CRD VI	Capital Requirements Directive VI. EU directive implementing Basel III governance and oversight rules.
CSSF	Commission de Surveillance du Secteur Financier. Luxembourg financial sector supervisory authority.
DNB	De Nederlandsche Bank. Central bank of the Netherlands.
DORA	Digital Operational Resilience Act. EU regulation requiring ICT resilience, incident reporting, and continuous monitoring for financial entities.
EBA	European Banking Authority. EU agency responsible for banking regulation and supervision.
EMIR	European Market Infrastructure Regulation. EU regulation for over-the-counter derivatives, central counterparties, and trade repositories.
ESMA	European Securities and Markets Authority. EU agency responsible for securities market and investment firm regulation.
EU	European Union. Political and economic union of 27 European member states.
FINREP	Financial Reporting. EU standardized reporting framework for financial information of financial institutions.

Term	Definition
GCC	Global Capability Centre. An offshore or nearshore center established by a multinational corporation to deliver business functions.
GDPR	General Data Protection Regulation. EU regulation for data protection and privacy.
ICT	Information and Communication Technology. Infrastructure and systems for digital data processing and communication.
IFM	Investment Fund Manager. Entity responsible for managing investment funds.
KYC	Know Your Customer. Process of verifying customer identity and risk profile.
MiFID II	Markets in Financial Instruments Directive II. EU regulation for investment services and financial markets.
NBB	National Bank of Belgium. Central bank of Belgium.
PEP	Politically Exposed Person. Individual with a high-risk public function requiring enhanced due diligence.
PSD3	Payment Services Directive III. EU directive for payment services, fraud controls, and payment security.
PSR	Payment Services Regulation. EU regulation directly applicable to payment services across member states.
RegTech	Regulatory Technology. Technology solutions for compliance, risk management, and regulatory reporting.
SCA	Strong Customer Authentication. Requirement for multi-factor authentication in electronic payments.
SIEM	Security Information and Event Management. System for real-time security monitoring and incident response.
STEM	Science, Technology, Engineering, Mathematics. Academic disciplines relevant to technology and engineering roles.
TLPT	Threat-Led Penetration Testing. Security testing methodology based on real-world threat intelligence.

References

- European Banking Authority. DORA Regulatory Technical Standards. 2025.
- Basel Committee on Banking Supervision. CRR III Implementation Guidelines. BIS. 2024.
- European Commission. PSD3 Directive Implementation Guidance. Official Journal of the EU. 2024.
- Anti-Money Laundering Authority. AMLA Supervisory Framework. EU Official Publications. 2025.
- European Parliament. EU AI Act High-Risk AI Systems in Financial Services. EU Publications Office. 2024.
- Fortune Business Insights. RegTech Market Size and Forecast 2026 to 2034. 2025.
- Grand View Research. RegTech Market Analysis Report. 2025.
- Nasscom. India GCC Talent and Capability Report. Nasscom Publications. 2025.
- Nasscom Zinnov. GCC Value Orbit from Delivery Engine to Enterprise Nerve Centre. May 2026.
- Quess Corp. BFSI GCC Talent Report. 2025.
- Quess Corp. India's GCC Tech Talent Landscape Q4 FY26. 2026.
- Careernet via Economic Times. Flex Hiring Adoption in GCCs. 2025.
- Mercer Mettl. India Graduate Skill Index. 2025.
- JumpGrowth. GCC Cost Advantage Analysis. 2025.
- Everest Group. GCC Evolution From Cost Centers to Innovation Engines. July 2025.
- YourStory. GCC Led Compliance Transformation in Financial Services. July 2025.
- ACA Group. DORA Implementation and Compliance Requirements. January 2026.
- Inductus GCC. European GCC Potential Navigating Regulation and Trust. December 2025.
- National Bank of Belgium. DORA Supervisory Framework and ITA Team Guidelines. 2025.
- Commission de Surveillance du Secteur Financier. Circular 25 882 Register of Information. 2025.
- Commission de Surveillance du Secteur Financier. Circular 18 698 Delegation and Oversight. 2018.
- Thomson Reuters. Confirmation of Dutch Bank KYC Compliance Trends. 2024.
- FMO. Deployment of Fenergo Client Lifecycle Management Platform. Press Release. 2025.
- Bloomberg. Dutch Bank ING Using Generative AI to Cut Money Laundering Risk. 2024.

Inductus GCC Service Models

India's Leading GCC Enabler

BOT (Build-Operate-Transfer)

A structured pathway to establishing your GCC with minimized risk and maximum efficiency. We **build** and **operationalize** your center, ensuring seamless performance before **transferring full ownership** to you—**equipping your business with a mature, self-sustaining capability.**

COPO (Company-Owned, Partner-Operated)

Maintain **full ownership** while leveraging Inductus' operational expertise. This model enables you to establish a GCC with **absolute control over intellectual assets (IP), agility**, **and scalability** while we manage day-to-day operations, **ensuring zero liability, compliance, and maximum efficiency**.
Additionally, a **Zero Capex Model** with **Digital Twin or a Mirror Like Operational Structure** with superior process excellence.

FLEXI (Adaptive & Custom GCC Solutions)

Beyond predefined structures, **Flexi is a bespoke model offering absolute customization and adaptability.**

It molds itself around your unique business prerequisites, evolving seamlessly with your vision. **This isn't just a service—it's an agile, high-impact partnership crafted to maximize your success.**

Proud recipient of **Times Power Icons Award**
for being one of the **Leading GCC Enabler of India**

Presented by Bennett & Coleman THE TIMES OF INDIA

Inductus ensures that each model is executed with precision, innovation, and strategic foresight—helping you unlock the full potential of your GCC in India.

Our deep expertise in GCCs, coupled with a strong network of industry partnerships and policy-level advisory, positions us as a trusted partner for driving transformational outcomes.

Certificate of Excellence' for Consulting & Advisory Services
by **Chicago Open University USA**

+91-92346-92346 gcc@inductusgroup.com www.indcutusgcc.com

COPO & Digital Twin Integrated Service Model

A study based proposition to build a global standard GCC mechanism for Large & Mid-sized Corporations

"In a world full of rapid tech & process disruptions, global corporations that invest in innovation-led R&D don't just survive—they lead. Innovation is the key to staying relevant, cost-competitive, and future-ready in an ever-evolving marketplace..."

Alouk Kumar - CEO, Inductus

Inductus GCC's Digital Twin and COPO (Company-Owned, Partner-Operated) Service Model creates a seamless, future-ready operational framework for global businesses setting up GCCs in India. The Digital Twin Process ensures real-time collaboration, decision-making, and operational efficiency by replicating physical systems in a virtual environment, enabling synchronized execution across multiple time zones. Meanwhile, the COPO Model allows MNCs to retain full ownership and strategic control while leveraging Inductus' expertise for execution, compliance, and scalability.

This hybrid approach optimizes costs, mitigates risks, and accelerates GCC growth, ensuring innovation-driven operations with minimal liabilities and maximum efficiency.


Designed to be Different.
www.inductusgcc.com