



+ **Xpansiv**[®]

Scaling Up Carbon Markets Infrastructure (CMI): Priority Area II

Agenda

- **Purpose and Key Takeaway**
- **The Importance of Priority Area II: Information Security and Transaction Integrity (KYC/AML/ABC)**
- **World Bank's Mandates for Priority Areas**
- **Assessment Framework for Sub-categories**
- **Timeline Review**
- **Stakeholder Engagement and Next Steps**

Working Group Purpose and Key Takeaway

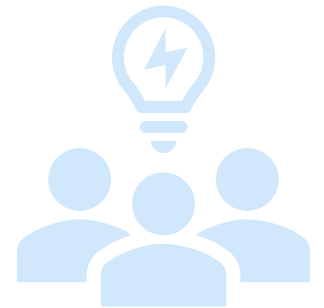
Purpose:



The focus of this working group is to create comprehensive Guidance Notes to help emerging, developing, and mature participants in the Carbon Markets Infrastructure (CMI) to effectively implement compliant Information Security (IS) and Transaction Integrity (TI) programs. By reinforcing the principles and trustworthiness of interconnected carbon markets on the global stage and highlighting current best practices, this effort aims to enhance CMI transparency and robustness, thereby increasing investor confidence and mobilizing the private sector.

Key Takeaway:

The key takeaway of this session is to secure a commitment from participating stakeholders for ongoing collaboration, emphasizing the sharing of knowledge and skills, and continuous feedback. The goal is to foster productive dialogue that leverages collective expertise to create a more comprehensive and effective Guidance Note by June 2025, ultimately strengthening Information Security (IS) and Transaction Integrity (TI) in the CMI.



The Importance of Priority Area II

Information Security

Implementing a well-crafted information security program in support of KYC, AML and ABC improves transaction robustness and transparency, ensures regulatory compliance, and strengthens trust by safeguarding data and preventing financial crime.

Use Case #1 – 2016 Data Breach

- **Information Security Failures:**
 - Lack of Encryption – aided unauthorized access to data
 - Inadequate Data Retention Practices – allowed unnecessary storage of sensitive data that should have been securely deleted equating to increased breach exposure
 - Failure to Maintain Audit Trails – prevented accurate identification of breach scope and perpetrators
- **Key Takeaway:**
 - When encryption, data retention, and audit trails are not properly implemented, organizations face severe risks, including data breaches, challenges in breach response, and legal and regulatory consequences

Use Case #2 – 2019 Data Breach

- **Information Security Failures:**
 - Insufficient Data Protection – improperly implemented security controls for storage configurations permitted a vulnerability exploit resulting in unauthorized access
 - Weak Access Control – Overly permissive access controls allowed an individual without a legitimate business need to steal data
 - Inadequate Monitoring Systems – Ineffective monitoring systems failed to identify the data loss, which only came to light when an external party reported the leaked data
- **Key Takeaway:**
 - Failure to properly implement data protection, access control, and monitoring systems can lead to significant breaches, exposing sensitive data and resulting in loss of trust, along with regulatory and legal consequences

The Importance of Priority Area II

Information Security (Continued)

The Guidance Note's Information Security section will focus on areas with regulatory mandates tied to KYC, AML and ABC programs. It is important to note that Information Security mandates cover additional areas that are not part of the current scope of this effort.

- **Data Protection** - safeguarding information from unauthorized access, disclosure, alteration or destruction.
- **Encryption** – used to protect the confidentiality of data both when it is stored (at rest) and when it is transmitted (in transit).
- **Access Control** – security mechanism involving authentication (verifying identity) and authorization (granting/restricting permissions based on roles or needs).
- **Data Retention** – policies and procedures for secure storage, archiving and/or deleting data in compliance with legal, regulatory, or business requirements.
- **Monitoring Systems Security** – continuous oversight and improvement regarding security related activities/systems deployed to detect, prevent and respond to security incidents to identify potential threats or breaches.
- **Maintaining Audit Trails** – the process of recording and preserving logs of all significant actions or events within an information system which can be used for compliance, forensic investigations and ensuring accountability.

The Importance of Priority Area II

Transaction Integrity

A key element to CMI development is stakeholder confidence, at the onset and continuing thereafter. Preventing the entry of bad actors as well as ensuring the underlying market is used to derive positive outcomes for all involved is foundational to this objective. Furthermore, failure to deploy controls in support of Transaction Integrity could result in violation of sanctions laws and undue exposure to bribery and corruption risk.

Use Case #3 – KYC/AML

- **Online Payment Company**
 - Domiciled in a jurisdiction with less stringent AML regulations
 - Account opening process did not require identity verification (i.e., anonymous accounts)
 - Lack of basic KYC controls attracted criminals, particularly cybercriminals
- **Take Away**
 - Bad actors will be drawn to markets where KYC requirements are below standard and anonymity is allowed

Use Case #4 – Anti-Bribery and Corruption

- **Voluntary Carbon Market Scams**
 - Fraudulent claims about carbon offset projects, where projects either did not exist or failed to deliver the promised environmental benefits
 - Defrauded buyers experienced financial losses, which deterred future investments in the carbon market and affected market liquidity
- **Take Away**
 - In addition to severe financial consequences, taking part in bribery or corruption-related activities deepens reputational risks while placing the sector under greater scrutiny

The Importance of Priority Area II

Transaction Integrity (Continued)

The Guidance Note's Transaction Integrity section will focus on implementation of KYC, AML and ABC programs. It is important to note that Transaction Integrity mandates cover additional areas that are not part of the current scope of this effort.

- **Know Your Customer (KYC)** – the process used by financial institutions to 1) verify the identities of their clients and individuals with significant control (e.g., beneficial owners and directors) and 2) assess the risk associated with clients. It ensures that clients are who they claim to be, helping to prevent fraud and financial crimes.
- **Anti-Money Laundering (AML)** – procedures and regulations designed to prevent criminals from disguising illegally obtained money as legitimate. It requires financial institutions to monitor and report suspicious activities.
- **Anti-Bribery and Corruption (ABC)** – policies and practices that prevent bribery, corruption and fraud within organizations. It ensures that business dealings are conducted ethically and in compliance with anti-corruption laws.

World Bank's Mandate for Priority Areas

Key Areas for Strengthening

In your individual markets (e.g., countries or regions), what are the known (or anticipated) **pain points**?

What risks are most likely to **impact the successful rollout** of CMI in your markets?

What risks should be prioritized **after rollout**?

Beneath the Priority Area II categories, are there specific topics that should be targeted?

Learning from Good Practices

How strong of a reliance will be placed **on third parties** to develop CMI in your market?

Do you foresee challenges in **aligning to industry standards** or established good practices? Are these unique to your market?

What forums or opportunities would be most impactful to **assess and employ** standards and good practices?

Standards and Certifications to Adopt

Will **regulatory obligations be triggered** to operate CMI in your markets?

Is it likely **customers** in your market will **require certain certifications**? (e.g., SOC II and ISO 27001)

Are regional partnerships likely? Will these partnerships require shared technical standards?

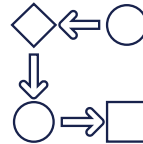
Further Coordination Opportunities

What level emphasis should be placed on **interoperability**? Between markets? Between transaction platforms?

How might regional or bi-lateral **partnerships add integrity and liquidity** to your markets?

How can we **improve/balance** data sharing and transparency among carbon market participants **while ensuring data privacy and security**?

Sub-Category Assessment Framework



Likely Risks

- Identification of applicable risks is the essential to secure and well-designed processes.
- Risk-based controls drive effective mitigation and efficient deployment of resources.

Strengths When Implemented

- A strong control framework supports market integrity while limiting disruptions.
- Reliable, well functioning processes enable stakeholder confidence and facilitate new market entrants

Implement Good Practices

- Deploying a set of risk-based tools and processes is critical to CMI's initial and ongoing success.
- Proper execution and periodic updates are essential to ongoing risk mitigation.
- Established forums to share lessons-learned

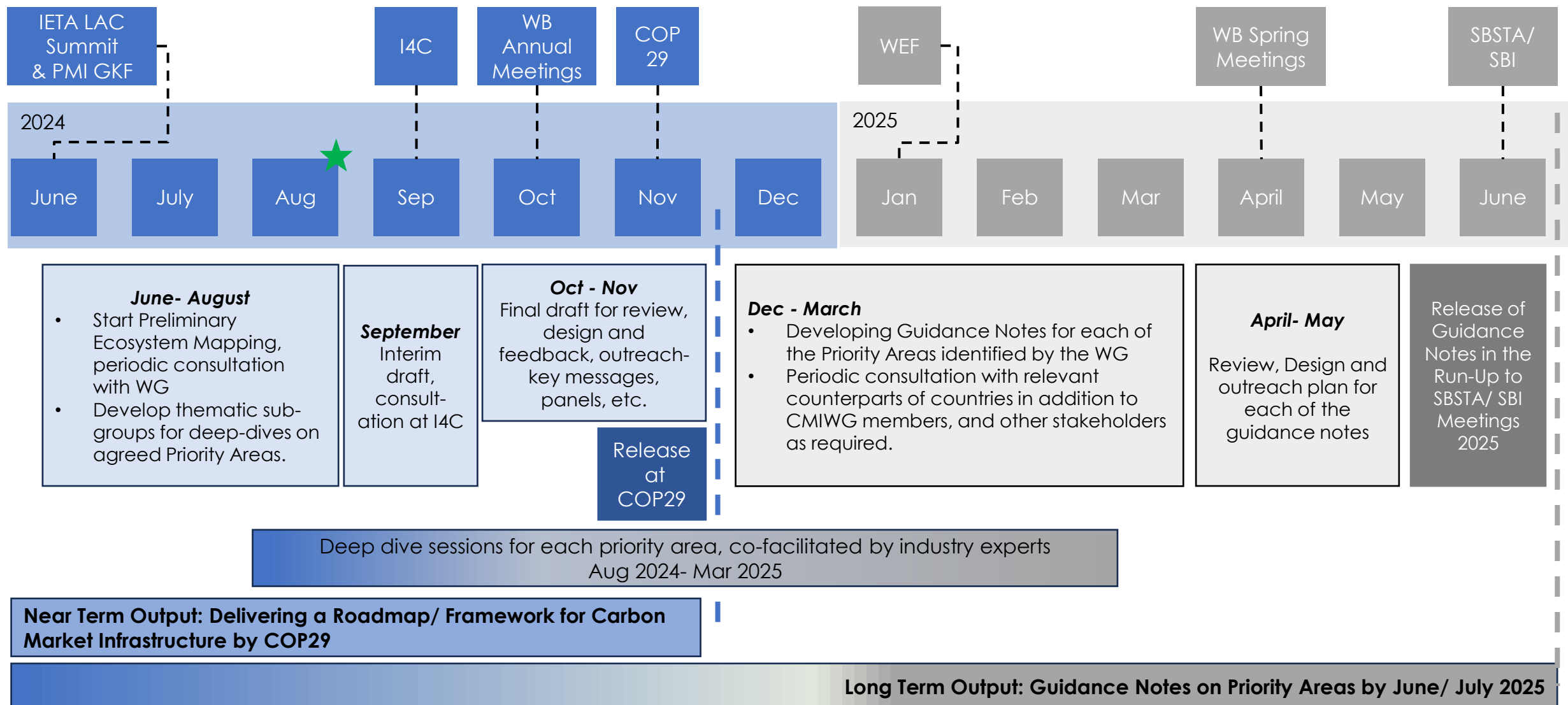
Constraints and Considerations

- Understanding limitations and constraints is necessary for effective, timely deployment of tools and processes.
- Collaboration across the CMI could decrease constraints while promoting stronger risk mitigation across the sector.

Tools and Techniques

- Comparable sectors can provide helpful use cases when deploying technology to mitigate risk effectively.
- Existing, mature programs within the CMI possess proven techniques tailored to our unique market dynamics.

Timeline of Activities



Bilateral/ one-on-one meetings are interspersed

Stakeholder Engagement and Next Steps

- Participate in Priority Area targeted sessions
 - Apply subject matter expertise and experience to identify Guidance Note's points of emphasis
 - Collaborate with fellow CMI stakeholders to identify synergy opportunities
 - Provide input to Guidance Note structure
- Review and provide feedback on drafted content
 - Continued participation in Priority Area targeted sessions
 - Contribute to the components and timing of Guide Notes roll-out



**November 2024 - CMI
Roadmap Release at COP29**

Next Steps:

- Inform Priority Area II leads what topics you're able to contribute
- Participate in subsequent working group sessions to provide input on Guidance Notes' points of emphasis
- As appropriate, include colleagues who possess SME in these areas






Appendix








Potential Deliverable Table of Contents

- **Executive Summary**
- **Mandate Outcomes**
 - **Key Areas of Strengthening**
 - **Learning From Good Practices**
 - **Standards and Certifications to Adopt**
 - **Further Coordination Opportunities**
- **Category Assessments**
 - **Assessment Framework**
 - **Information Security Assessment**
 - **Transaction Integrity Assessment**
- **Looking Ahead**
- **Conclusion**






Working Model: Information Security

| | Factor | Description | Examples |
|--|---------------------------------------|---|---|
|  | Likely Risks | <i>Breaches of information security comprise data and disrupt market functionality resulting in decreased confidence and reliability.</i> | <ul style="list-style-type: none">• Cloud security flaws• Data breach• Ransomware attack |
|  | Strengths from Control Implementation | <i>Enhanced capabilities to prevent external and internal actors gaining inappropriate access while limiting the impact of successful entry attacks.</i> | <ul style="list-style-type: none">• Multi-factor authentication• Rule-based access controls• Penetration Testing |
|  | Implementation Good Practices | <i>Practices accounting for vulnerabilities end-to-end from vendor due diligence, secure coding practices, network encryption, testing, and training.</i> | <ul style="list-style-type: none">• Vendor penetration testing• Secure configuration management• Intrusion prevention systems |
|  | Constraints and Considerations | <i>Resource limitations, whether financial or human capital, influence the breadth and speed in which information security controls are deployed.</i> | <ul style="list-style-type: none">• Resource allocation from development to remediation• Vendor prioritization decisions |
|  | Tools and Techniques | <i>Proven technology and best-practices are available in comparable markets and should support CMI development</i> | <ul style="list-style-type: none">• Identity and Access Management Systems• Endpoint Detection and Response• Network Traffic Analysis |

Working Model: KYC/AML

| | Factor | Description | Examples |
|---|---------------------------------------|---|---|
|  | Likely Risks | <i>Market integrity is directly linked to the ability of bad actors leveraging the market in support of their own objectives.</i> | <ul style="list-style-type: none"> • Individuals with fraud-related convictions gaining access to the voluntary carbon market • Layering of ill-gotten funds through the buying and selling of voluntary carbon credits |
|  | Strengths from Control Implementation | <i>Risk-based controls are essential to CMI development, continual effectiveness, and maintaining stakeholder confidence</i> | <ul style="list-style-type: none"> • KYC processes to identify high-risk market participants • Screening participants and their owners against sanctions, PEPs, and adverse media lists |
|  | Implementation Good Practices | <i>Processes and controls are to be fit-for-purpose while incorporating 'lessons learned' from comparable partners or similar sectors (e.g., commodity derivatives)</i> | <ul style="list-style-type: none"> • Controls should be risk-based to facilitate resource allocation • Where possible, automation can elevate control effectiveness |
|  | Constraints and Considerations | <i>Available SME and resource availability are inputs to effective control, whether manual or technology-based, design and implementation.</i> | <ul style="list-style-type: none"> • Adjudication of screening alerts requires SME to account for materiality of events • Deploying automated solutions amongst additional workflows requires high level of technical acumen and planning resources |
|  | Tools and Techniques | <i>Proven technology and best-practices are available in comparable markets and should support CMI development</i> | <ul style="list-style-type: none"> • Competitive marketplace for cloud-hosted KYC screening solutions • Ongoing monitoring of customer information is a strong risk mitigant |

Working Model: ABC

| | Factor | Description | Examples |
|---|---------------------------------------|---|--|
|  | Likely Risks | <i>The geographic footprint and the breadth of industry/sector representation elevates exposure to bribery and corruption risk thus influencing reputational risk and overall scrutiny.</i> | <ul style="list-style-type: none"> • Payments to government officials to secure land • Gifts and travel to sway procurement decisions |
|  | Strengths from Control Implementation | <i>Robust controls can effectively mitigate the bribery and corruption risks faced by an organization. Inherently, lowering one's exposure to ABC risk lessens exposure to reputational risk.</i> | <ul style="list-style-type: none"> • Training • Gifts and Expense Policy • Risk-based expense approvals and reviews |
|  | Implementation Good Practices | <i>Processes and controls should incorporate 'lessons learned' from similar sectors while taking into account the unique risks faced by any one organization</i> | <ul style="list-style-type: none"> • Prioritize control implementation where impact is greatest (e.g., training vs expense management software) • Identified risks should drive control design |
|  | Constraints and Considerations | <i>Available resources and in-house SME will likely influence what controls are deployed to mitigate against this risk.</i> | <ul style="list-style-type: none"> • Content depth and frequency of training • Expense preapprovals vs value thresholds |
|  | Tools and Techniques | <i>Proven technology and best-practices are available in comparable markets and should support CMI development</i> | <ul style="list-style-type: none"> • Incorporate PEP and adverse media in your screening processes • Third party expense management vendors |

World Bank's Mandate for Priority Areas

Key Areas for Strengthening

- What is the importance of implementing IS, KYC, AML and ABC towards ensuring a robust CMI?
- How does IS, KYC, AML and ABC implementation produce key strengths in the CMI?
- What do phased approaches focus on when implementing IS, KYC, AML and ABC in emerging, developing and mature CMI?

Learning from Good Practices

- What are good practices for implementing IS, KYC, AML and ABC within the CMI?
- What are considerations/constraints to consider when implementing IS, KYC, AML and ABC within the CMI?
- Are there other areas to be considered for inclusion when looking to implement robust CMI information security and transaction integrity?

Standards and Certifications to Adopt

- What emerging trends or new standards/certifications in the carbon market are you most interested in or concerned about?
- What factors do you consider most important when evaluating a carbon certification standard for your projects?
- How do you think adopting robust certification standards impacts the overall credibility of the carbon market?
- How do certification standards align with national and international regulations in your view?
- What role do you think certification standards should play in ensuring compliance with climate agreements?

Further Coordination Opportunities

- In what ways could current carbon market infrastructure be improved to better support coordination between market participants?
- What are the potential benefits and challenges of integrating different carbon market platforms and registries?
- How can we improve data sharing and transparency among carbon market participants while ensuring data privacy and security?
- What innovative approaches or technologies do you think could transform carbon market infrastructure and enhance coordination?
- How can we better engage diverse stakeholders, including smaller market participants and local communities, in the carbon market infrastructure?
- What lessons have been learned from past coordination efforts, and how can these lessons be applied to current and future initiatives?