

Blockchain readiness assessment checklist







VISION

ESCWA, an innovative catalyst for a stable, just and flourishing Arab region

MISSION

Committed to the 2030 Agenda, ESCWA's passionate team produces innovative knowledge, fosters regional consensus and delivers transformational policy advice. Together, we work for a sustainable future for all.

Blockchain readiness assessment checklist



Introduction

With blockchain technology increasingly influencing industries and governance, policymakers need a structured approach to assess their readiness for its adoption. The Blockchain Readiness Assessment Checklist provides a comprehensive framework to evaluate preparedness across three essential areas: pre-implementation phase, technical guidelines and policy guidelines.

- **1.** Pre-implementation phase: this stage examines fundamental prerequisites such as regulatory frameworks, infrastructure preparedness, energy efficiency and accessibility. It ensures that Governments and institutions have a clear road map for blockchain adoption.
- 2. Technical guidelines: this section focuses on the technological requirements of blockchain integration, including network design, security protocols, interoperability and scalability. A strong technical foundation is crucial for ensuring seamless and efficient implementation.
- **3.** Policy guidelines: this component assesses the regulatory landscape, alignment with international standards and governance structures. It helps policymakers establish a balanced framework that supports innovation while addressing security, privacy and ethical considerations.

By evaluating these three dimensions, policymakers can identify potential gaps, develop strategic action plans and ensure that blockchain adoption aligns with national objectives. This checklist serves as a practical guide to facilitate informed decision-making and drive sustainable blockchain implementation.

1 Pre-implementation phase

A. Infrastructure readiness

A.1. Assess technical infrastructure

A.1.1. Does the country have reliable Internet connectivity nationwide?

* Reliable Internet connectivity is essential for blockchain networks to function effectively, as they require constant data exchange between nodes.

A.1.2. Is electricity supply available and reliable across the country?

* Blockchain processes, especially those involving proof of work consensus mechanisms, require significant energy. Reliable electricity is crucial to maintain continuous operation of blockchain nodes.

A.1.3. Are data centres or cloud services available and secure?

* Data centres and cloud services provide the infrastructure necessary for hosting blockchain nodes and storing data securely. High security reduces risks of breaches and data loss.

Source: Gartner. Forecast: Data Center Sites, Worldwide, 2021-2027, 2023 Update, 2023.

A.1.4. Is there sufficient computational power to handle blockchain processes?

* Blockchain operations require significant computational resources, particularly for resource-intensive algorithms like proof of work. The availability of such power determines the feasibility of hosting blockchain operations.

Source: Equus Compute Solutions (ECS). A brief intro to the infrastructure requirements of blockchain, 2022.

A.1.5. Are there import restrictions on information communications technology (ICT) goods? Is the country a member of the Technology Agreements I and II of the World Trade Organization?

* Import restrictions on ICT goods can impede access to necessary hardware for blockchain infrastructure. Membership in the World Trade Organization Information Technology Agreements ensures tariff-free trade on various technology products.

Source: World Trade Organization. Information Technology Agreement, n.d.

A.2. Evaluate digital infrastructure

A.2.1. Are there established digital payment systems and financial technologies?

* Blockchain applications often integrate with digital payment systems and fintech solutions. Established systems indicate readiness to adopt blockchain in financial operations.

A.2.2. Is there an existing database system compatible with blockchain technology?

* Blockchain systems often integrate with existing databases to enhance functionality. Compatibility ensures a seamless transition and interoperability between systems.

Source: Oracle Cloud Infrastructure (OCI). Use cases: blockchain in healthcare, 2023.

B. Legislative and regulatory framework

B.1. Digital framework and data protection

B.1.1. Are there laws governing data protection and privacy?

* Data protection and privacy laws ensure that individuals' data are safeguarded, thereby establishing trust in blockchain technologies.

B.1.2. Does the country have laws governing electronic transactions following international best practices such as the United Nations Convention on the Use of Electronic Communications in International Contracts and/or the Model Law on Electronic Commerce of the United Nations Commission on International Trade Law (UNCITRAL)?

* Laws aligned with international standards such as the Model Law on Electronic Commerce promote legal certainty in electronic transactions.

Source: United Nations Commission on International Trade Law. <u>United Nations Convention on the Use of Electronic Communications in International Contracts</u>, 2005. New York.

B.1.3. Is there legal recognition of electronic evidence in judicial and administrative proceedings?

* Legal acceptance of electronic evidence ensures that blockchain data can be used effectively in legal and administrative contexts.

B.1.4. Does the country recognize electronic contracts and digital signatures? Are they based on the UNCITRAL Model Laws on Electronic Signatures and Automated Contracting?

* Recognition of electronic contracts and digital signatures is key to facilitating blockchain-enabled agreements.

Source: United Nations Commission on International Trade Law. UNCITRAL Model Law on Electronic Signatures, 2001.

B.1.5. Does the country have a law on electronic authentication that follows the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services?

* Such laws enable secure and verifiable electronic authentication across borders, which is essential for international blockchain operations.

Source: United Nations Commission on International Trade Law. <u>UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services</u>, 2022; Oluwapelumi Adejumo, <u>South Korea to regulate cross-border crypto trades by 2025</u>, 2024. CryptoSlate.

B.1.6. Does the law in the country define digital assets and tokens?

* Clear legal definitions ensure regulatory clarity for blockchain-based assets.

B.1.7. Are there law(s) regulating digital technologies and trade?

* These laws establish the foundation for integrating blockchain into digital technologies and trade.

B.1.8. Do these laws govern aspects such as cryptography, disclosure of source codes and/or algorithms, promotion of open software and the development of emerging technologies?

* This ensures a regulatory environment conducive to innovation.

B.1.9. Is there a law promoting e-government?

* E-government laws support blockchain adoption in public administration.

B.1.10. Does the country have a law protecting personal data?

* Such laws protect citizens while enabling blockchain use.

B.1.11. Does the law in the country regulate government (public) data and other non-personal data?

* This question checks if the country has rules governing the use, sharing and protection of public and non-personal data, crucial for blockchain compliance and transparency.

B.1.12. Does the country have a law on cross-border flows of data in general and public sector (government) data in particular?

* This question evaluates if the country regulates international and government data flows.

Source: Organisation for Economic Co-operation and Development (OECD). Cross-border data flows, n.d.

B.1.13. Is there a law on data localization?

* This question determines if data must be stored locally, impacting blockchain's reliance on distributed networks.

B.1.14. Does the law ensure the non-discrimination (national treatment and most-favoured-nation treatment) of digital products?

* This question assesses if digital products are treated equally in domestic and foreign markets.

B.1.15. Does the law ensure net neutrality and non-discrimination of different types of hardware?

* This question examines whether the country's legal framework guarantees equal access to the Internet and prohibits unfair treatment of devices or technologies, ensuring a level playing field for blockchain platforms and users.

B.1.16. Does the legal framework enable pilot programmes and regulatory sandboxes?

* This question evaluates if the country supports innovation by allowing controlled testing of blockchain solutions in regulatory sandboxes or pilot programmes.

Source: World Bank Group. Key data from regulatory sandboxes across the globe, 2020.

B.1.17. Is there a modern law protecting intellectual property (IP) related to industrial property (patents, utility models and trade secrets)? * This question assesses the existence of updated IP laws to safeguard innovations, crucial for blockchain-based solutions.

B.1.18. Do laws in the country guarantee freedom of contract?

* This question examines if parties have the legal right to freely negotiate terms, enabling blockchain smart contract implementation.

B.2. Implement specific blockchain rules

B.2.1. Is there a legal regulation on the liability of blockchain stakeholders?

* This question assesses whether the country's laws define the responsibilities and liabilities of blockchain participants, ensuring accountability within the blockchain ecosystem.

B.2.2. Does the country have a legal framework for dispute settlement mechanisms (litigation, arbitration, non-binding alternative dispute resolution, online dispute resolution)?

* Such a legal framework facilitates the resolution of blockchain-related disputes.

B.2.3. To facilitate cross-border dispute settlement, does the country have mutual legal assistance treaties, and does it recognize foreign judgements and/or arbitral awards?

* These elements facilitate the resolution of blockchain-related disputes.

B.2.4. Does the country have a national definition of distributed ledger technology or blockchain?

* This checks whether the country has an official definition for distributed ledger technology or blockchain, which helps establish clear legal boundaries for its application.

B.2.5. Do regulations cover the scope of blockchain technology?

* This evaluates if the country's regulations define and address blockchain use cases, such as smart contracts, cryptocurrencies or decentralized applications.

B.2.6. Does the country allow decentralized autonomous organization as a new form of cooperative business?

* This supports innovative business structures using blockchain.

Source: Wyoming Secretary of State, Business Division. Decentralized Autonomous Organization (DAO): frequently asked questions, 2022.

B.2.7. Does the country have technical regulations on blockchain?

* This question assesses whether the country has technical standards or regulations for blockchain implementation, covering interoperability, security and data management.

B.3. Check compliance and standards

B.3.1. Are anti-money-laundering and counter-terrorism financing laws in place?

* Such laws ensure that blockchain is used responsibly.

B.3.2. Does the Government adhere to international technology standards that support blockchain integration?

* This evaluates if the Government follows global technology standards, which is essential for effective blockchain adoption and integration.

B.4. Confirm stakeholder support

B.4.1. Is there political support for blockchain adoption?

* Political will drives adoption.

Sources: Malta Blockchain Island Initiative.

B.4.2. Are industry stakeholders (e.g. banks, telecom providers) willing to collaborate?

* This examines if key sectors such as banking and telecom are open to working together on blockchain projects, facilitating broader adoption.

Source: Sictic. Swiss Startup Ecosystem Map, n.d.

C. Human and institutional capacity

C.1.1. Is there a pool of professionals skilled in blockchain technology?

* Professionals with expertise in blockchain development, cryptography and system integration ensure the success of blockchain projects.

C.1.2. Are government personnel trained to understand and implement blockchain solutions?

* Government personnel need training to design, oversee and regulate blockchain projects effectively.

C.1.3. Are government institutions equipped to manage blockchain projects?

* Institutional capacity ensures that blockchain projects are effectively planned, executed and monitored.

Source: World Bank. Digital government readiness assessment, 2020.

C.1.4. Do existing public sector systems support innovation and experimentation, including public-private-academic partnerships?

* Collaboration among public, private and academic sectors fosters innovation in blockchain applications.

C.1.5. Does the public sector workforce have the technical literacy to adopt blockchain solutions?

* Technical literacy in this context includes familiarity with blockchain concepts, such as distributed ledgers, smart contracts and consensus mechanisms, as well as the ability to integrate these technologies into existing systems and processes.

Source: OECD. Blockchains Unchained: Blockchain Technology and its Use in the Public Sector, n.d.

D. Economic and market conditions

D.1.1. Are there mechanisms to secure sensitive data against breaches?

* Securing sensitive data is fundamental for blockchain implementation, as breaches can compromise trust and system integrity.

Source: International Business Machines Corporation (IBM). What is blockchain security? n.d.

D.1.2. Are there laws on cybersecurity and cybercrime? Is the country a party of the Council of Europe Convention on Cybercrime (Budapest Convention, ETS No. 185)?

* Cybersecurity laws and adherence to international conventions protect against cyber threats.

Source: Council of Europe. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols, n.d.

D.1.3. Does the country have laws on data sovereignty and localization?

* These legal frameworks regulate where data can be stored and how they are managed, particularly concerning data sovereignty and localization.

D.1.4. Does the country have a history of effectively managing digital threats?

* Digital threats are risks to digital systems and data, including cyberattacks, malware, data breaches and insider threats.

D.1.5. Are there standards to ensure that blockchain platforms can communicate with each other?

* Interoperability between blockchain platforms ensures seamless operation and data-sharing, which is critical for scaling and integrating blockchain systems.

D.1.6. Are firewalls, intrusion detection/prevention systems and other safeguards in place?

* Robust cybersecurity measures such as firewalls and intrusion detection systems protect blockchain networks from external threats and breaches.

D.1.7. Does the Government have partnerships with technology providers for resilient infrastructure?

* This question examines if the Government collaborates with tech companies to strengthen infrastructure resilience against challenges such as technological failures or cyber threats.

E. Visions and plans

E.1. Formulate a strategic vision

E.1.1. Does the country have a digital transformation or innovation strategy?

* A digital transformation or innovation strategy outlines how a country plans to evolve in the digital age. This strategy could involve advancements in digital infrastructure, services or economic growth through technology.

E.1.2. Does the country have a strategy for the adoption of emerging technologies?

* This question assesses whether a country has planned for adopting cutting-edge technologies such as artificial intelligence (AI), Internet of things (IoT) and blockchain.

E.1.3. Does the country have a dedicated blockchain strategy?

* A dedicated blockchain strategy outlines specific goals, use cases and projects related to blockchain technology.

E.1.4. Is blockchain aligned with national goals, such as economic development or transparency?

* This checks if blockchain adoption is seen as a tool for achieving broader national objectives such as fostering economic development, improving transparency in governance or enhancing data security.

E.1.5. Are international collaborations or partnerships being explored?

* Is the country engaging with international entities, Governments or organizations to explore blockchain use cases or to develop shared solutions?

E.2. Implement pilot projects

E.2.1. Are there successful small-scale pilot projects in blockchain to validate readiness?

* Pilot projects are an essential step in testing blockchain's feasibility on a small scale before large-scale deployment.

E.2.2. Is there a road map to scale successful pilot projects into national initiatives?

* This refers to whether the country has plans in place to expand successful blockchain pilot projects into full-fledged national initiatives that can be adopted across sectors.

Source: National Blockchain Strategy of India.

F. Economic and financial ecosystem

F.1.1. Is there funding allocated to blockchain research, start-ups or pilot projects?

F.1.2. Has the Government conducted a cost-benefit analysis of blockchain adoption in key sectors?

F.1.3. What is the anticipated return on investment from blockchain integration over the short and long term?

Source: PricewaterhouseCoopers (PwC). Blockchain's impact in fostering global financial inclusion, n.d.

G. Pilot and test cases

G.1. Conduct feasibility studies

G.1.1. Have feasibility studies been conducted for blockchain in priority sectors?

* Feasibility studies assess whether blockchain can be effectively implemented in priority sectors such as healthcare, finance, logistics or public administration.

G.1.2. What are the lessons learned from previous pilot projects (if any)?

* This question focuses on understanding the successes and challenges encountered in earlier blockchain pilots, helping refine future projects.

G.2. Foresee scalability and interoperability

G.2.1. Are pilot projects designed with scalability and interoperability in mind?

* Scalability ensures that the technology can handle larger volumes, while interoperability ensures that it can communicate with other technologies.

Source: IBM. TradeLens momentum grows with addition of two major ocean cargo carriers, 2019.

G.2.2. How are results being measured, and are they aligned with national goals?

* This question assesses whether the results are tracked using defined metrics that align with the country's broader goals, such as economic development, transparency or public sector modernization.

Source: OECD. Blockchains unchained: blockchain technology and its use in the public sector, n.d.

G.3. Regulations to promote use cases

6.3.1. Are there laws regulating electronic credentials, electronic wallets and electronic product identifiers?

* This question checks if the country has specific regulations for digital identity systems, electronic wallets or digital product identification. Such regulations are crucial for blockchain-based solutions in finance, trade and public services.

6.3.2. Does the country participate in international treaties, or does it have other instruments (memorandum of understanding, multilateral recognition agreement, etc.) of relevance to cross-border exchange of electronic credentials?

* This question examines whether the country participates in international agreements related to the recognition and exchange of electronic credentials. Such international agreements are important for cross-border transactions and e-commerce.

6.3.3. Does the country have specific legal or e-transactions rules for trade facilitation or paperless trade, including documentary aspects of customs clearance?

* These rules address the digital handling of trade-related documents, such as invoices, contracts and customs declarations, enabling smoother and faster customs clearance processes.

6.3.4. Are there (a) laws applicable to certificates of origin, and (b) international treaties or other instruments for mutual recognition of certificates of origin?

* Certificates of origin are essential for international trade. This question assesses whether the country has laws in place for certificates of origin and whether international agreements exist for recognizing them across borders.

6.3.5. What are (a) the rules and procedures on geographical indications and appellations of origin, and (b) the international treaties or other instruments for mutual recognition of these instruments?

* Geographical indications and appellations of origin are critical in protecting regional products.

Source: World Intellectual Property Organization (WIPO). Geographical Indications, n.d.

G.3.6. Is there any legislation on digital product passports?

* Digital product passports are a form of digital identity for products that can track their life cycle, including origin, ownership and use. This question assesses whether the country has laws for regulating digital product passports.

Source: European Union. EU's digital product passport: advancing transparency and sustainability, 2024.

6.3.7. Are there any laws regulating educational credentials and dedicated international instruments?

* This question checks if the country has laws regulating the recognition and use of educational credentials in digital formats, including international agreements to facilitate their recognition across borders.

Source: United Nations Educational, Scientific and Cultural Organization (UNESCO). Global Convention on Higher Education, 2019.

6.3.8. Are there any other relevant international treaties or other instruments (memorandum of understanding, multilateral recognition agreement, etc.) relevant to promote blockchain use cases?

* This question explores whether the country is involved in other international agreements that promote the use of blockchain or other emerging technologies across borders.

H. Environmental and social dimensions

H.1. Promote energy efficiency

H.1.1. Does the country have the capacity to implement energy-efficient consensus mechanisms such as proof of stake?

* Proof of stake requires significantly less energy than traditional consensus mechanisms such as proof of work.

Source: IBM. <u>Revolutionizing renewable energy certificate markets with tokenization</u>, 2021.

H.1.2. Are there renewable energy sources to mitigate the carbon footprint of blockchain technology?

* Renewable energy sources such as solar, wind or hydroelectric power can be leveraged to reduce the environmental impact of blockchain technology, particularly its energy consumption.

H.2. Ensure accessibility for small and medium-sized enterprises and social groups

H.2.1. Does the country promote accessibility to blockchain for small and medium-sized enterprises (SMEs), women, young people and minorities?

I. International cooperation

I.1.1. Does the country participate in international treaties and/or promote other legal instruments related to cross-border cooperation for blockchain implementation?

* This question evaluates whether the blockchain applications can be recognized and supported globally.

I.1.2. What cooperation activities does the country have to promote blockchain implementation?

* These activities could include collaborations with other countries, partnerships with international organizations or engagement in crossborder blockchain projects.

Source: CCN. Chinese Government Reveals Public Blockchain Platform for Belt and Road Initiative, 2024.

2 Technical guidelines

The technical guidelines for blockchain assessment focus on ensuring successful implementation through clear goals, rigorous testing and selection of appropriate platforms. These guidelines cover key aspects such as system design, security measures and seamless integration with existing technologies. Additionally, they emphasize the importance of continuous monitoring and evaluation to maintain performance and address evolving challenges. By following these guidelines, stakeholders can ensure that blockchain solutions are effective, secure and adaptable to future needs.

A. Infrastructure

A.1. Identify needs, define requirements and scope the use case

A.1.1. What are you planning to achieve?

* This question focuses on the primary objectives of implementing blockchain in your country.

A.1.2. For whom is it intended?

- * Identifying stakeholders and end users is critical to the success of blockchain implementation.
- A.1.3. What is needed to achieve your goals?
- * This question aims to identify resources and infrastructure requirements.

A.2. Speed, sovereignty and security factors

- A.2.1. Did you consider speed, sovereignty and security factors?
- * These factors are vital for a sustainable blockchain framework.

A.2.2. What storage is needed?

* Understanding storage requirements is key to blockchain scalability.

A.2.3. Did you compare existing options?

* This ensures the selection of the most appropriate blockchain solution.

A.3. Design and implement the architecture

A.3.1. Did you establish risk management procedures?

* Risk management is crucial for mitigating blockchain adoption challenges.

Source: Deloitte. Blockchain risk management, n.d.

A.3.2. Did you set the level of authority of network participants?

* Defines governance models for blockchain networks.

A.3.3. Do you have the skills required for blockchain adoption?

* Skills assessment ensures readiness for blockchain adoption.

A.3.4. Are you planning to collaborate with the private sector?

* Public-private collaboration enhances blockchain adoption.

A.4. Testing

A.4.1. Did you ensure unit testing, performance and load testing?

* Testing ensures that blockchain operates under expected and peak conditions.

A.4.2. Are authorized economic operators, traders and other agencies involved in the key testing steps?

* Involvement of stakeholders in testing guarantees system effectiveness.

A.4.3. Did you set up real-world scenarios for testing?

* Real-world testing ensures system readiness for deployment.

A.4.4. Did you consider the six key technical testing processes (security, performance, functionality, integration, unit and retest/regression testing)? * Comprehensive testing ensures robust blockchain performance.

Source: Blockchain testing guides from the Institute of Electrical and Electronic Engineers.

A.5. Develop smart contracts

A.5.1. What logic do you want to achieve behind smart contracts?

* Smart contract logic defines their purpose and functionality.

Source: Ethereum. Ethereum developer documentation, 2023.

A.5.2. What is the process that you want to include?

* Process inclusion ensures that blockchain functionality aligns with goals.

Source: Hyperledger Fabric. Process and Data Design, 2020.

A.6. Deploy the blockchain

A.6.1. Have all necessary servers/nodes been set up and synchronized for the network?

* Proper set-up ensures blockchain operational readiness.

Source: Amazon Web Services (AWS). Blockchain node deployment on AWS: A comprehensive guide, 2024.

A.6.2. Has a simple majority of computational units (servers or nodes) been achieved to establish a common agreement on the state of network records?

* This asks if more than half of the network's nodes agree on the current state of records, ensuring consensus and accuracy in the system.

A.6.3. Is the genesis block successfully up, running and producing further blocks?

* The genesis block is the first block of a blockchain, and its creation marks the start of the blockchain network. If the genesis block is successfully created, the blockchain should be operational.

A.6.4. Which provider will host the network?

* Hosting decisions impact blockchain performance and sovereignty.

Source: Gartner Peer Insights. Blockchain platforms reviews and ratings, n.d.

A.6.5. Are there cost-benefit analyses supporting this choice?

* Financial evaluations ensure cost-effectiveness.

A.6.6. Are there considerations for autonomy and sovereignty in this option?

* Sovereignty ensures national control over blockchain systems.

Source: European Parliament. Digital sovereignty for Europe, 2020.

A.7. Design security protocols

A.7.1. What measures are in place to detect and prevent unauthorized intrusions and data tampering?

* This question asks about security measures like firewalls, encryption and intrusion detection systems to prevent unauthorized access and data tampering.

A.7.2. Has a network reorganization plan been developed for scenarios requiring record correction?

* This question assesses whether there is a plan in place to reorganize a blockchain network in cases where errors in records need to be corrected.

A.7.3. Have robust data encryption mechanisms been implemented to protect blockchain data?

Source: Open Worldwide Application Security Project (OWASP). Cryptographic Storage Cheat Sheet, n.d.

A.7.4. Have comprehensive access control measures been established to restrict unauthorized entry?

* This question asks if systems have measures such as multifactor authentication, permissions and monitoring in place to prevent unauthorized access.

Source: Kisi. <u>Blockchain for Physical Access Control</u>, n.d.

A.8. Design and integrate portals and user interfaces

A.8.1. Is the interface aligned with the blockchain application's business logic and process flow?

* The interface should integrate seamlessly with business logic.

A.8.2. Does it cater to the average user's needs without requiring deep technical knowledge?

* Accessibility is key for the average user to access the interface without it being overcomplicated.

A.8.3. Is the development team skilled in user interface (UI) and user experience (UX) design?

* Skilled design teams enhance user satisfaction.

A.9. Integrate with existing infrastructure

A.9.1. Has a road map been established to integrate blockchain with existing systems?

* A road map outlines the strategic plan for incorporating blockchain into existing digital systems. It should clearly define goals, timelines and the specific use cases of blockchain within the organization.

Source: European Commission. EU Blockchain Observatory and Forum, n.d.

A.9.2. Are there gaps in current systems that blockchain can effectively address?

* This question assesses whether current systems have weaknesses or inefficiencies that blockchain technology can help mitigate, such as security, transparency or operational efficiency.

A.10. Monitor, evaluate and maintain the blockchain and digital infrastructure

A.10.1. Are there processes in place to proactively identify and address security vulnerabilities?

* A proactive approach to security ensures that vulnerabilities are detected and fixed before they are exploited. This question examines the presence of a vulnerability management process.

A.10.2. Is there a system to continuously monitor activity logs for potential network attacks or unauthorized access?

* Continuous monitoring is crucial for identifying potential security breaches.

A.10.3. Are access control measures regularly reviewed and updated to enhance network security?

* Access controls determine who can interact with system resources. This question ensures that these measures are continually assessed and adjusted to mitigate emerging threats.

Source: ISMS.online. ISO 27001 - Annex A.9: Access Control, 2023.

A.10.4. Are software updates and network upgrades scheduled and implemented routinely?

* Regular updates and upgrades help mitigate security risks by fixing vulnerabilities and improving system performance.

A.10.5. Are stakeholders and users regularly informed about best practices for maintaining digital hygiene?

* Digital hygiene refers to practices that reduce the risk of cyber threats. This question evaluates if users are educated on how to protect themselves and the system.

A.10.6. Is there a feedback mechanism to gather input from users for system improvements?

* Feedback mechanisms allow users to share their experiences, identify pain points and suggest improvements, ensuring that systems remain user-friendly and effective.

12

3 Policy guidelines

A. Policy steps for successful stakeholder engagement

A.1. Identify key stakeholders and define key roles

A.1.1. Have all relevant governmental agencies and stakeholders been identified and included in coordination efforts?

* This question ensures that all parties with an interest or role in the blockchain implementation are considered and engaged in the coordination process.

A.1.2. Is there a clear plan to address the technical needs for implementing blockchain across the sector?

* A clear plan should outline the technical resources, infrastructure and skills required for blockchain implementation in the sector.

A.1.3. Is there a shared platform for agencies to collaborate and communicate effectively for inter-agency coordination?

* This question assesses whether there is a centralized platform where agencies can communicate, share information and coordinate efforts for the blockchain implementation.

A.1.4. Are there specialized subcommittees within the national committee on trade facilitation addressing specific challenges related to blockchain deployment?

* Specialized subcommittees can focus on particular challenges related to blockchain implementation, ensuring targeted solutions.

Source: The United Nations Conference on Trade and Development (UNCTAD) Trade Facilitation Guidelines highlight the role of specialized committees in traderelated initiatives.

A.1.5. Have individuals with relevant knowledge and expertise been identified for the blockchain implementation process? * Identifying experts ensures that the blockchain implementation is informed and supported by those with the necessary technical and industry knowledge.

A.1.6. Are the selected individuals equipped with the authority necessary to make decisions and drive implementation efforts? * Having authority ensures that the identified experts can make decisions, allocate resources and lead the blockchain implementation efforts.

A.1.7. Has a core implementation team been established to oversee the operational and functional aspects of blockchain deployment?
* This team will be responsible for managing the day-to-day operations of blockchain deployment, ensuring its smooth execution.

A.1.8. Are key institutions such as customs, ports, standards and revenue authorities represented within the team?

* Key institutions must be represented to ensure that blockchain implementation aligns with regulatory and operational requirements.

Source: World Bank Group. National Trade Facilitation Committee Roadmaps and Translating Commitment into Effective Action, n.d.

A.1.9. Does the implementation process include oversight and leadership from multi-stakeholder bodies such as national trade facilitation committees? * Multi-stakeholder bodies can provide oversight, ensuring transparency, coordination and consensus throughout the blockchain implementation process.

A.2. Understand stakeholder needs and communicate the benefits of the blockchain tools

A.2.1. Are each stakeholder group's specific trade facilitation needs, concerns and expectations understood?

* Understanding the specific needs and concerns of each stakeholder group helps tailor the blockchain solution to meet diverse expectations.

Source: United Nations Economic and Social Commission for Asia and the Pacific (ESCAP). Trade facilitation in the Asia-Pacific region: a bright outlook, 2014.

A.2.2. Are engagement strategies tailored to address each stakeholder group's specific concerns and expectations?

* Tailored engagement strategies ensure that each group's concerns are addressed and that they feel invested in the blockchain initiative.

A.2.3. Are stakeholders informed about how blockchain benefits align with their needs, such as transparency, security and efficiency?

* Keeping stakeholders informed helps gain their support and encourages active participation.

A.2.4. Are multi-user needs from various stakeholders incorporated into the blockchain design process?

* Blockchain systems should be designed to meet the diverse needs of multiple stakeholders, ensuring broad adoption and effectiveness.

A.2.5. Is the input of relevant agencies incorporated into the design of blockchain technical solutions?

* Input from relevant agencies ensures that blockchain solutions are practical, comply with regulations and fit within existing systems.

A.3. Ascertain stakeholder readiness and preparedness for the technology

A.3.1. Have the main concerns of stakeholders regarding blockchain implementation (e.g. cost, complexity, user protection and security risks) been identified?

* Identifying and addressing stakeholder concerns early on can mitigate resistance and smooth the implementation process.

Source: Manuel Pedro, and others. Blockchain and the Public Sector, 2021.

A.3.2. Is there a clear understanding of how stakeholder interest aligns with the goals of blockchain implementation?

* Understanding the alignment between stakeholder interests and implementation goals ensures that the project delivers value to all involved parties.

A.3.3. Are feedback tools such as surveys or questionnaires utilized to gauge stakeholder expectations and readiness for blockchain technology? * Feedback tools help measure stakeholder readiness and gather valuable input for refining the implementation process.

Source: Joe Wynne. Stakeholder Analysis, n.d. The Project Management.

A.3.4. Has a formal blockchain readiness assessment been conducted to evaluate the preparedness of stakeholders for the new technology?

* A readiness assessment gauges the preparedness of stakeholders to adopt blockchain technology, highlighting gaps and areas for support.

A.4. Develop a stakeholder engagement implementation plan

A.4.1. Has a clear stakeholder engagement implementation plan been developed?

* A well-defined plan outlines how stakeholders will be engaged throughout the blockchain implementation process, ensuring consistent communication and alignment.

A.4.2. Does the plan outline specific objectives, timelines, resource allocations and expected outcomes for stakeholder engagement? * Clear objectives, timelines and resource allocations ensure that stakeholder engagement is organized and efficient.

A.4.3. Has the plan been designed inclusively, involving a national committee on trade facilitation or similar multi-stakeholder group? *Including a national committee on trade facilitation or other similar body ensures that stakeholder engagement is comprehensive and representative of all interests.

Source: UNCTAD. Inclusivity in trade facilitation: the role of National Trade Facilitation Committees, 2024.

A.4.4. Are there provisions in the plan to accommodate feedback and adapt to prevailing conditions?

* The ability to adapt the plan based on ongoing feedback ensures its relevance and effectiveness as conditions evolve.

A.5. Organize key stakeholders before starting the blockchain implementation process

A.5.1. Have stakeholder coordination meetings and workshops been organized before starting implementation? * Coordination meetings ensure that stakeholders are aligned and prepared for the implementation process.

A.5.2. Have multi-agency engagement sessions been planned to align the stakeholders' perspectives and expectations?

* This evaluates whether steps have been taken to bring together different agencies and stakeholders for discussions aimed at harmonizing their objectives, resolving differences and ensuring a shared understanding of the project's direction.

A.5.3. Have any role conflations, gaps or overlaps been identified and addressed?

* Identifying and addressing role conflations, gaps or overlaps ensures clear responsibilities and effective collaboration among stakeholders.

A.6. Set up training, education, research and support for stakeholders

A.6.1. Have training sessions been planned to help stakeholders understand the key benefits and utility of the technology?

* Training sessions ensure that stakeholders understand how blockchain will benefit them and the broader system.

A.6.2. Is there a process for conducting periodic research to assess and improve how the technology meets stakeholder needs?

* This checks if a structured approach is in place to regularly evaluate the technology's performance and gather insights for refining it to better address stakeholder requirements.

A.6.3. Are stakeholders provided with continuous support to ensure effective and sustainable technology use?

* Continuous support ensures that stakeholders can effectively use blockchain and adapt to its evolving nature.

A.7. Implement stakeholder feedback loops, monitoring and evaluation

A.7.1. Is there a system to monitor and evaluate stakeholder dynamics regularly during implementation?

* Monitoring and evaluating stakeholder dynamics ensures that any concerns or changes in perspective are addressed promptly.

A.7.2. Are any areas for improvement identified during the evaluation process, and are there clear steps for addressing these issues promptly? * Evaluation allows for identifying weaknesses or areas for improvement and for taking timely corrective action.

Readiness assessment road map: impact if not implemented

The absence of a reliable technical and digital infrastructure, including Internet, electricity and secure data centres, would hinder blockchain accessibility, scalability and security.

Weak legislative and regulatory frameworks create legal uncertainty, limit enforceability of digital transactions, and expose users to financial and security risks. A lack of skilled professionals and institutional readiness slows adoption, while insufficient cybersecurity measures increase vulnerability to fraud and hacking.

Without a clear national strategy, funding and interoperability standards, blockchain innovation remains fragmented, reducing investment confidence and limiting economic benefits.

Poor environmental considerations and exclusion of SMEs and marginalized groups further restrict equitable access. Additionally, weak international cooperation isolates the country from global blockchain advancements, reducing competitiveness and cross-border integration.

Lack of proper planning and organization causes role conflicts, inefficiencies and delays. Without continuous training, feedback loops and evaluations, the implementation may stagnate, and potential improvements will be missed.

Not implementing a structured blockchain approach can cause inefficiencies, security vulnerabilities and project failure.

Insufficient testing and weak smart contract logic lead to operational failures and losses. Security gaps result in breaches, while poor user interfaces hinder adoption.

Failing to integrate with existing systems reduces efficiency, and without continuous monitoring, threats go unaddressed, causing long-term degradation and disengagement.

Lack of clear goals and requirements wastes resources, while poor protocol and architecture choices expose the system to risks.

Without understanding stakeholder needs and expectations, the system may fail to meet their requirements, causing low adoption and inefficiency. Ignoring stakeholder readiness can lead to difficulties in technology adoption, costly mistakes and project failure.

Not implementing stakeholder coordination and engagement leads to misalignment, confusion and resistance. Failing to identify and include all relevant agencies results in fragmented efforts, delays and ineffective blockchain deployment.



Readiness assessment road map: recommendations

1. Pre-implementation phase

To foster blockchain adoption and maximize its potential, invest in critical infrastructure such as reliable Internet, resilient energy solutions and secure data centres to ensure stable operations.

Strengthen the legal framework with clear laws on electronic transactions, data protection and electronic contracts to support blockchain integration.

Encourage collaboration among stakeholders, including academia and the private sector, to develop a skilled workforce and create innovative solutions.

Implement robust cybersecurity measures, promote energy-efficient consensus mechanisms, and align with global standards to ensure security, scalability and sustainability.

Develop a national blockchain strategy, fund research and pilot projects, and support international partnerships to drive adoption and enhance competitiveness.

Prioritize inclusivity by addressing the needs of SMEs and marginalized groups while ensuring equitable access.



2. Technical guidelines

To avoid inefficiencies, security risks and project failure, it is essential to implement a structured blockchain framework with clear objectives and requirements.

Careful selection of blockchain protocols is critical for ensuring speed, security and adequate storage.

A robust architecture design is necessary to mitigate governance and operational risks, while thorough testing must be conducted to ensure functionality, prevent system failures and maintain regulatory compliance.

Developing and deploying smart contracts is vital to leverage automation and reduce manual errors.

Strong security protocols should be in place to safeguard against unauthorized access and data breaches. User-friendly interfaces are essential for adoption, and proper integration with existing systems boosts operational efficiency.

Continuous monitoring, maintenance and feedback loops are necessary to identify emerging threats, maintain performance and ensure long-term project success.



3. Policy guidelines

20

To ensure successful blockchain deployment, it is crucial to enhance stakeholder coordination through clear communication platforms, involving all relevant agencies and defining their roles early on in the process.

Understanding stakeholder needs through surveys and assessments helps tailor solutions for higher adoption.

A well-defined engagement plan with clear objectives, timelines and feedback mechanisms is essential, along with pre-implementation workshops to align expectations.

Continuous training, research and support programmes will aid stakeholders in adapting to the technology, while ongoing feedback and evaluation ensure that the system evolves and improves over time. This approach mitigates resistance, delays and inefficiencies.



