Technical Set-Up of The CDO Unit

- The CDO Unit
- The Resources of the CDO
- The Role of the Business Analyst
- The CDO Team Organisation
- The CDO Network
- Interactions with Internal and External Stakeholders
- Collaboration with other government agencies
- The collaboration between CDOs and DPs and Civil Society
- The Collaboration with own Sector’s Institutions
- The importance of Academia and research institutions

The CDO Unit

The CDO: Definition and Role

The Chief Digital Officer (CDO) is responsible for developing and deploying an overall digital Strategy, implementing and monitoring digital projects within government departments, and implementing the government's vision for the digitisation of citizen services.
More specifically, the CDO oversees the overall IT Strategy of the Sector and oversees the IT Team under his/her supervision.
In other words, the Chief Digital Officer (CDO) is an executive that oversees the digital transformation needs of the entire Sector (Ministry and all the affiliated institutions or institutions with similar mandate) to ensure that they support the entire Sector's vision and goals. Therefore, he/she is responsible for planning, implementing and managing the overall use of information technologies, streamlining operations by implementing relevant technologies, developing technological systems that will improve customer satisfaction, and managing the information technology department.

The CDO is expected to be comfortable working in the fast-changing technology landscape and with the responsibility and pressure that comes with leading transformative initiatives to success in this environment.

The specific duties and responsibilities of the CDO position include (not limited):

Strategic Planning and Leadership:

- Advise the Sector Leadership in all IT related matters
- Be responsible to establish and infuse the sector's digital culture
- Strategic planning of the Sector to create business value, promote innovation, and contribute to growth objectives using technology
- Plan and oversee Sector's IT projects, develop and approve technology programs and budgets for the entire Sector
- Ensure tech systems, infrastructure and procedures lead to outcomes in line with business goals, develop strategies to improve the efficiency and efficacy of technological initiatives
- Oversee the development of customer service platforms
- Establish IT policies, strategies, and standards for the Sector (Policies, Strategies, IT Enterprise Architecture, digital literacy development, digital infrastructure, tools and content, sector-specific digital advancement, and innovations)

Team Management and Development:

- Manage IT and development team personnel for the department and coaching the members of the IT teams.
- Set, measure, and report IT department's KPIs on a regular basis

Enterprise IT Governance and Risk Management:

- Develop, operate and maintain the Enterprise IT architecture and adoption of innovation.
- Oversee IT risk management and align it with enterprise-wide risk management.
- Ensure the Sector's data remains secure by keeping up to date on the latest cyber security threats and finding ways to guard against them on an organization-wide scale as well as ensuring good Data Governance.

Vendor Management and Financial Oversight:

- Review and approve department purchases, vendor proposals, negotiate contracts with vendors, and service providers in accordance with the proper guidelines from relevant institutions including MINECOFIN, MINICT, and RISA
- Prepare cost-benefit analyses for every change.

Communication and Collaboration:

Communicate with other executive members, employees and end-users to make sure all parts of the Sector use technology in the best ways possible.

The Resources of the CDO

The Chief Digital Officer is provided with essential resources crucial for accomplishing their responsibilities, including:

- Human resources
- Financial resources
- Tools and technologies

Human resources:

The Chief Digital Officer is supported by various IT specialists. The CDO of a sector has a team composed of Business Analysts, Senior software developers, Network specialist, System Administration Specialist, developers, Database Administration Specialist, IT Help Desk Officer. The provision of the different profiles in terms of number largely depends on the needs, the size and the organisation of the particular sector. Also, there is a need to add specific IT talents such as cyber security experts, data engineers, devOps and data scientists. Such new positions can be hired as contractual, outsourced, or directly added to the existing structure in the future.

Financial resources:

Each sector's IT department has two distinct types of budgets available, tailored to the sector's priorities and budget constraints:

1. Operational Budget: This budget is allocated for acquiring, maintaining, and updating the IT infrastructure within the sector. It covers expenses related to hardware, software, networking, and ongoing maintenance to ensure smooth and efficient IT operations.
2. Development Projects Budget: This budget is designated for digital transformation initiatives aimed at enhancing and modernizing the sector through digital solutions. It funds projects that drive innovation, improve digital capabilities, and support the sector's strategic objectives.

The Chief Digital Officer (CDO) is responsible for the entire budgeting process. This includes:

1. Budget Planning: The CDO meticulously plans both the operational and development projects budgets, aligning them with the sector’s strategic priorities and goals.
2. Submission: The CDO submits the detailed budget proposals to both the sector leadership and the Rwanda Information Society Authority (RISA) for review and approval.
3. Management: Once the budgets are approved, the CDO oversees the allocation and expenditure of funds, ensuring that the budget is used efficiently and effectively to achieve the intended outcomes.

By managing these budgets, the CDO ensures that each sector can maintain its IT infrastructure while also pursuing transformative digital projects that enhance its performance and service delivery.

Tools and technologies:

In terms of tools, some tools are developed or acquired by RISA and made available to IT teams in the public sector.
The reader can refer to the Standards, Methodologies, tools and technologies in the section 4 of this Handbook to learn more about this topic.

The Role of the Business Analyst

The Business Analyst's main role is to work with all entities within their respective Sector to help them improve their processes and systems using Digital Technologies. She/he conducts research and extensive analysis to come up with solutions to business problems and helps in introducing the systems to end-users and customers. She/he acts as a link between core businesses and IT teams. The Business Analyst will engage with business leaders (sector management board) and users to understand how data-driven changes to process, products, services, software, and hardware can improve efficiencies and add value.

The Business Analyst is expected to have a natural analytical way of thinking and be able to explain difficult concepts to non-technical users as he/she is expected to work closely with developers, stakeholders, system architects and various subject matter experts.

The specific duties and responsibilities of the Business Analyst position include (not limited):

The specific duties and responsibilities of the Business Analysts for the position include:

Business Analysis and Requirements Gathering:

- Elicits, analyses, specifies, documents, and validates the business needs of the Sector, stakeholders, including customers and end users by outlining problems, opportunities, and solutions.
- Prioritises requests and needs from different entities/business units of the Sector and consolidates them into implementable projects.
- Conducts interviews and gathers customer requirements through various methods such as workshops, questionnaires, surveys, site visits, etc.
- Researches, reviews, and analyses the effectiveness and efficiency of existing requirements-gathering processes and develops strategies for enhancing or leveraging these processes.
- Analyses and verifies requirements for completeness, consistency, comprehensibility, feasibility, and conformity to standards.
- Translates conceptual customer requirements into functional requirements in a clear manner that is comprehensible to developers/project teams.
- Develops and utilises standard templates for writing accurate and concise requirement specifications and provides basic training for template utilisation.

Documentation and Process Modelling:

- Creates process models, specifications, diagrams, and charts to provide direction to developers and/or the project team.
- Develops and conducts peer reviews of the business requirements to ensure that requirement specifications are correctly interpreted.

Stakeholder Collaboration and Communication:

- Collaborates with project sponsors to determine project scope, vision, and stakeholders.
- Assists with the interpretation of customer requirements into feasible options and communicates these back to the business stakeholders.
- Communicates changes, enhancements, and modifications of business requirements to project managers, sponsors, and other stakeholders so that issues and solutions are understood.

Requirement Management and Quality Assurance:

- Manages and tracks the status of requirements throughout the project lifecycle, assessing competing resources and priorities to enforce and redefine as deemed necessary.
- Participates in the Quality Assurance of purchased solutions to ensure features and functions have been enabled and optimised.

Tools and Processes Optimization:

Participates in the selection of requirements documentation software solutions that the organisation may opt to use, considering emerging technologies and future trends.

The CDO Team Organisation

First and foremost, at Sector level, an IT Team is provided at the organisation structure of the leading Ministry and it covers the IT functions for the entire Sector. Thus, the IT function is headed by a Chief Digital Officer (CDO) for the harmonious coordination of IT Strategy. In Sectors without CDO, the IT function is headed by a Business Analyst. The Chief Digital Officer (CDO)/Business Analyst (BA) is an employee placed within the sector (line Ministry) but under the supervision of RISA as said before.

The BA and IT Team under the supervision of the sector's CDO is attached to the Sector's line Ministry as their reporting line and primary location. Based on proper planning and workload evaluation, the CDO/BA dispatches the allocated IT Team within the Sector to ensure full support and optimum utilisation of resources including staff and IT systems. Staff under the CDO/BA's office are allocated to the leading Ministry and serve dynamically the institutions under the Sector to ensure the smooth operation.

The team is directly attached to the lead Ministry and dispatched across the sector's institutions to address emerging IT needs. The Digital Office has also a direct reporting line to RISA as supervising authority.

Each CDO organises its team as needed, depending on the Ministry organisation and the size of the team. However, each CDO team is composed of:

i. At the leadership and management level

The CDO or BA is the leader of the whole team and the rest of the team works under his/her supervision.

They organise the team around the vision and specific objectives and projects of the sector they are in charge of.

ii. The IT technical team

1. **Senior Software Developer**: As a key team member, the Senior software developer is responsible for development, design and implementation of new software solutions or modification and upgrade of the existing ones, providing quality assurance and technical evaluation of new and legacy systems and software products in the sector. The Senior Developer will lead Developers to ensure the application of best practices and professional software development methodologies, relevant tool suites and technologies, creativity and innovation in all software development projects of the sector.
2. **Network Specialist**: the network specialist is responsible to maintain reliable, secure and efficient data communications networks in the Sector (Ministry, Lead Institution, Affiliated institutions).
3. **System Administrator Specialist**: The System administrator Specialist is responsible for the installation, maintenance, configuration, and reliable operation of computer

systems and servers in the Sector (Ministry, Lead Institution, Affiliated institutions). The System Administrator Specialist will actively resolve problems and issues with computer and server systems to limit work disruptions within the Ministry.

4. **Software Developers**: In support of the Senior Software Developer and under the supervision of the CDO and Business Analyst, the Developers (Software Developers) are responsible of the development, design and implementation of new software solutions or modification and upgrade of the existing ones, toward digitization of the institutions and sector's services. The developer is expected to work closely with other developers, Business analysts, UX and UI designers, database experts, Software architects and projects managers from RISA and the sector to ensure he/she develops solutions that meet requirements and standards.
5. **Database Administration Specialist**: The responsibility of the database administration specialist is to create, ensure and maintain the performance, integrity and security and disaster recovery of databases. He/ she is involved in the planning and development of the database, as well as in troubleshooting any issues on behalf of the users.
6. **IT Help Desk Officer:** under the supervision of CDO/BA, the IT Help desk officer s upports personnel, and acts as focal point when end-users face hardware, software, or system issues, Administers desktop computers, printers, IP telephony, servers and related equipment (monitor, hard drive, keyboard, etc..), software deployment, security updates and patches, Keep inventory of all equipment, software, and licences, Monitor and work on responding quickly to incoming requests related to IT issues.

Some key objectives should guide the CDO in his/her team's composition and organisation:

Find the right balances

- **Between the technical vision and the functional vision**: a CDO office is no longer an IT support service, supposed to maintain applications and network; it is about introducing the most efficient solutions for the administration to deliver its mission. Therefore you would need to recruit staff able to understand the sector and the missions of the ministry as well as translate users' needs into digital services.
- **Between build and run:** while some digital services need to be maintained and monitored, you need to have sufficient available staff to launch new ones. It implies having a clear view on ongoing projects/services and future needs, as well as recruiting people who can proactively identify and design new projects and services.

Articulate recruitment with the ways of working and mid-term challenges:

- Because of the switch towards product and agile methodologies, RISA will tend to recruit people with adapted hard and soft skills. It implies looking for profiles such as UX/UI designers and user researchers, product owners and managers, product ops, dev ops, business developer, community facilitator, communications officer;
- As digital transformation in the public sector faces new challenges - cybersecurity, data, privacy, etc. – there will be a need to integrate cutting edge profiles: data-scientists, data-engineers, API manager, cybersecurity specialists, and not to mention the need to have

profiles mastering the legal framework of digital and data..

Build a delivery-centred organisational and managerial structure: in order to break silos and make sure the CDO can build and operate services safely and efficiently, it could be useful to transform the organisational structure. For instance, rather than having a tech-focused organisation (software service, architecture service, ...), the CDO can structure the teams by the projects they are running/operating, and have some transversal divisions linked.

The CDO Network

CDO Network overview

The **establishment of the CDO Network** aims at ensuring that all digital initiatives are aligned with their respective organisation’s goals and objectives, as well as bring alignment with RISA’s vision and mission.
The CDO Network gathers all the CDO officers from different sectors. They are organised in this way to coordinate the work of the CDOs, oversee the collective work of all CDOs across diverse administrations and share internal best practices developed within sectors. They can also work on cross-cutting projects to address specific challenges that they all have.

CDO Network Areas of Focus

The CDO Network has key areas of focus for its activities.

Discuss Digital Transformation Agenda

The CDO Network addresses various challenges associated with digital transformation. The Network can conduct discussions on:

- **Deployment of the nationwide digital strategies**: Ensuring that the nationwide strategies such as Smart Rwanda Master Plan, NSTs are well deployed by the CDOs Network in the Rwandan administrations.
- **Cultural Shift**: Overcoming resistance to change and fostering a digital-first mindset across public administrations.
- **Citizens Experience**: Enhancing citizens engagement through digital channels and personalised experiences.
- **Scalability and Flexibility**: Ensuring that digital solutions are scalable and adaptable to changing business needs.

Address Cross-Cutting Challenges

The CDO Network meets to raise and address Cross-cutting challenges that affect multiple aspects of digital transformation and that require collaborative solutions.

The Network can discuss together how to address:

- **Governance scheme:** The Governance of the sector, the top-down and bottom-up approach of the Governance in the digital transformation ecosystem
- **Regulatory framework:** Navigating complex regulatory environments and ensuring compliance with data protection laws.
- **Interoperability:** Ensuring that different systems and technologies can work together seamlessly.

- **Innovation Management:** Encouraging innovation while managing the risks associated with new technologies.
- **Procurement and Vendor Management:** The procurement process in the public sector and its challenges, Vendor Management, the interactions between the CDOs and the suppliers etc…
- **Framework Contracts and their management**
- **Talents' availability**
- **Contractors' management and management of the outsourcing process**

Share Knowledge and Practices

The CDO Network facilitates the sharing of knowledge and best practices among members:

- Use cases and best practices: Presenting successful digital transformation initiatives and lessons learned.
- Research and Reports: Disseminating the latest research findings and industry reports relevant to digital transformation.

Share Communications among the Network

The Network strives to ensure that all Chief Digital Officers (CDOs) are aligned on key communications. During meetings, essential communications are shared, and CDOs are expected to both understand and implement them. Additionally, feedback on the current communications implementation is discussed to facilitate continuous improvement.

Publication of new policy, new regulations, new framework contracts, conferences, an event to attend…

Resource Sharing Among CDOs

Resource sharing enables the Network to leverage collective expertise and assets:

- Tools and technologies: Sharing digital transformation toolkits, frameworks, and templates. The best tools can be shared among the Network as well as feedback on their usage to enhance the tools deployment.
- Expertise: Facilitating the exchange of expertise through secondments and collaborative projects.

Sharing Best Practices

Identifying and promoting best practices helps standardise successful approaches across the network not limited):

- **Best practices in Project Management:** management style, methodologies and tools used are shared.
- **Best practices in Software Development:** lessons learned and practices that can be useful to the Network.

- **Best practices in Third parties' management:** How the suppliers and contractors are managed by the CDOs and successful stories to share.

Establishing Communities of Practice

The CDO Network, composed of CDOs with similar profiles in their Office, have the opportunity to establish Communities of Practice in order to bring together members with common interests and expertise.

The Network can establish a community for each type of practice in their teams: community of developers, Database Administration specialists' community, Help Desk specialists community, Network specialists community…
In addition, certain groups can be created, focused on specific areas such as AI, IoT, data analytics, data protection, Cybersecurity, etc…

A Peer Learning system can be developed to encourage peer-to-peer learning and mentorship within these communities.

Develop Common Projects

The network can develop Collaborative Projects that leverage the collective knowledge and skills of the community. Collaborative projects drive innovation and shared learning:

- Pilot Programs: Launching pilot programs to test new digital solutions and approaches.
- Research Initiatives: Conducting joint research initiatives to explore emerging trends and technologies.
- Innovation Labs: Establishing innovation labs for co-creating and prototyping new digital solutions.
- Sharing common tasks/ supporting a project from one sector as other sectors can be stakeholders

Increase Awareness and Host Events

Raising awareness and hosting events foster engagement and visibility:

- **Conferences and Summits:** Organizing large-scale events to bring together thought leaders and practitioners.
- **Publications and Media:** Publishing articles, white papers, and case studies to highlight the network's achievements and insights.

Interactions with Internal and External Stakeholders

Interactions within the MINICT ecosystem

Interactions between the Ministry of ICT & Innovation (MINICT) and the CDO:

In the digital transformation landscape, the Chief Digital Officer (CDO) operates as a pivotal figure within the structure, positioned under the Rwanda Information Society Authority (RISA) and, ultimately, the Ministry of ICT. This placement fosters interactions between the CDO and both institutional bodies.

Within MINICT, the primary point of contact for a Chief Digital Officer (CDO) or Business Analyst is the Permanent Secretary. This official serves as the main liaison or interlocutor for matters concerning digital Strategy, technology initiatives, business analysis or IT projects implementation in general in the Ministry or sector.

As a key digital transformation value chain actor, the CDO placed under RISA which is placed under the MINICT has interactions with both institutions. CDOs are invited each year to define their own goals that will be discussed with RISA and the PS of MINICT. Once the goals are validated; they are considered as Ministry's IT Goals.

The initiation of the goals is then the responsibility of the CDO who must carry it with great attention. Not only must they serve the Ministry priorities, but also be aligned with Smart Rwanda guidance, MINICT and RISA guidance as well.

Once the goals are initiated and validated, they become the goals of the CDO who has to achieve them as he/she will be evaluated on them by RISA and MINICT. In that sense, CDO reports to MINICT through the PS. The frequency of reports can vary from a year to another, but once in minimum.

In addition to these duties, a CDO has the prerogative to engage directly with MINICT to address specific topics pertinent to his/her role. This could encompass discussions on the implementation of sector-specific guidelines or initiatives crucial to the ongoing projects.

Within the Ministry of ICT (MINICT), the Permanent Secretary occupies a pivotal role as the main intermediary or point of contact for Chief Digital Officers (CDOs) and Business Analysts. This individual acts as a central figure responsible for overseeing and managing various aspects related to digital transformation, technological strategies, and analytical endeavours within the Ministry.

The collaboration between the Permanent Secretary and CDOs involves a dynamic exchange of information, guidance, and decision-making. CDOs and Business Analysts often interact with the Permanent Secretary to communicate their insights, proposals, and initiatives regarding digital initiatives, technological advancements, data analysis, and other relevant matters within the

Ministry's purview.

This interaction signifies a vital communication channel wherein the expertise, recommendations, and strategic plans of CDOs and Business Analysts are relayed, discussed, and often implemented under the oversight or guidance of the Permanent Secretary. The Permanent Secretary's role involves providing direction, support, and leadership to ensure the alignment of CDOs' efforts with the overarching goals and strategies set forth by MINICT.

Finally, MINICT has the authority to extend invitations to Chief Digital Officers (CDOs), Business Analysts, and their respective teams for participation in specific activities deemed essential by the Ministry. These activities can vary widely, encompassing diverse formats such as working sessions, seminars, orientation sessions, and more. These invitations signify MINICT's recognition of the expertise and contributions that CDOs and Business Analysts, along with their teams, can bring to the table. They serve as opportunities for collaborative engagements, aimed at fostering a deeper understanding, sharing knowledge, and collectively addressing critical topics or initiatives aligned with the Ministry's objectives.

Working sessions often involve focused, hands-on collaborative efforts where professionals collaborate intensively on specific projects, strategies, or problem-solving tasks. Seminars offer a platform for knowledge exchange, where experts can present insights, trends, or best practices relevant to the Ministry's technological landscape.

Orientation sessions may serve as introductions to new policies, frameworks, or technologies, allowing participants to gain a comprehensive understanding of their implementation within the Ministry's context. These sessions can aid in aligning strategies, refining approaches, and enhancing the overall efficiency and effectiveness of digital initiatives.

By inviting CDOs, Business Analysts, and their teams to these activities, MINICT leverages their expertise, fosters collaboration, and ensures alignment with the Ministry's goals. It reflects a commitment to a collaborative and inclusive approach, harnessing collective knowledge and skills for the advancement of digital innovation within the Ministry.

Interactions between Rwanda Information Society Authority (RISA) management and the CDOs

Objectives Definition:

Annually, CDOs are tasked with formulating forthcoming year objectives, which they submit to RISA and MINICT, as detailed in the previous interactions with MINICT. These objectives necessitate a SMART approach, aligning with the broader Smart Rwanda Strategy while also eliciting commitment from the CDO.

Annual goals refer to specific, measurable, achievable, relevant, and time-bound objectives set by individuals or organisations to be accomplished within a year's time frame. These goals serve as a roadmap, outlining key priorities, targets, and milestones to be achieved within the designated period. They are typically aligned with broader strategies, vision, or organisational objectives and are used as a benchmark for evaluating progress and success at the end of the year.

Ultimately, at year-end, the CDO's performance evaluation hinges upon the achievement of these established goals.

The evaluation process of CDOs is based on KPIs that can be found on the dedicated part of this Handbook and in the annex.

Vision guidance, advice, and communication sessions:

CDOs may be invited to specific and strategic sessions with the RISA in the framework of their work. Although the frequency of these meetings is not fixed, it should be noted that participation is compulsory for CDOs. It can also be working sessions with the RISA, on dedicated topics, or seminars and workshops where CDOs and BAs must attend.

Reports and Follow-up:

In its capacity as the overseeing body for CDO operations, RISA ought to receive project reports, performance updates, and team management insights as integral components of the CDO's responsibilities. Communication channels, including reporting, meetings, and monitoring, between the CDO and RISA can take on either formal or informal structures but must be maintained for the duration required.

Recruitment needs:

As a supervisor of the IT team, the CDO addresses the recruitment needs to RISA, the supervisory authority. RISA launches the recruitment procedure, advertising and pre-selecting candidates after checking that the position is listed in the organisation chart.

In accordance with the Ministry of Public Servants and Labour’s guidelines, in the realm of IT job vacancies within public institutions, when a position becomes available, the CDO shares a roster of these openings with RISA for a comprehensive recruitment Strategy. RISA takes charge of all recruitment procedures for IT roles within streamlined public institutions. Upon successful completion, candidates are assigned to the institutions with open positions, aligning with their exam performance and prioritising requests based on the sequence of submissions from public institutions (following a "first come, first served" approach).

Other types of interactions:

RISA can involve a CDO in collaborative projects, such as the CDO Network collaborative projects. Additionally, RISA can arrange sessions focused on sharing experiences and Ministry-level best practices among CDOs.

The collaboration between National Cyber Security Authority (NCSA) and the CDO

As the primary Cyber Security Authority at the national level, the National Cyber Security Authority (NCSA) assumes a critical role in assisting CDOs in fulfilling their cybersecurity responsibilities. These interactions are multifaceted and can be initiated by either the NCSA or the CDO,

establishing a collaborative framework essential for effective cybersecurity management within organisations.

When the NCSA initiates interactions, their focus revolves around imparting crucial guidance and setting standards pertaining to cybersecurity. This guidance serves as a fundamental compass for IT teams, ensuring adherence to recognized cybersecurity protocols. Furthermore, the NCSA conducts comprehensive training sessions dedicated to enhancing the proficiency of IT teams in handling cybersecurity issues. Their cybersecurity awareness platform stands as a reservoir of invaluable resources, offering training modules and guidance that prove instrumental for both CDOs and IT teams in navigating the complex realm of cybersecurity.

In addition to guidance and training, the NCSA shoulders the responsibility of providing cybersecurity solutions, ensuring robust protection against cyber threats. Moreover, they manage the licences associated with these cybersecurity solutions, fortifying the cybersecurity infrastructure and safeguarding digital assets within departments.

On the other hand, interactions instigated by the CDO typically occur when potential or real cybersecurity threats are identified. In these instances, the CDO promptly engages the NCSA, seeking immediate intervention and resolution. Throughout this process, the CDO remains actively involved, collaborating closely with the NCSA to ensure a swift and effective response to the identified cybersecurity issue.

To further enhance and streamline these interactions, there's an ongoing project aimed at formalising and structuring the engagement between CDOs and the NCSA. This structured approach entails subjecting each interaction to a ticketing process, establishing a systematic means of tracking and documenting the resolution of cybersecurity incidents. Moreover, the CDOs will have the opportunity to provide instantaneous feedback on the NCSA's interventions, contributing to a culture of continuous improvement in cybersecurity practices. This initiative aims to strengthen communication channels, optimise response mechanisms, and elevate cybersecurity resilience across departments, fostering a more secure digital environment. Part of the project also involves integrating an SLA process and establishing specific KPIs to be followed. The interactions follow-up will be handled by RISA.

Collaboration with other government agencies

The collaboration between Rwanda Governance Board (RGB) and the CDO

The Rwanda Governance Board is the Authority in charge of promoting good governance, ensuring accountability, and supporting the development and implementation of governance policies and strategies in Rwanda. It plays a crucial role in promoting and sustaining good governance practices, fostering accountability, transparency, and effective leadership across different sectors of the Rwandan society. Below are key responsibilities of RGB:

- **Policy Formulation**: RGB is responsible for formulating policies, frameworks, and strategies related to good governance and national development. It works in collaboration with various government entities to develop policies that promote transparency, accountability, and effective governance practices.
- **Capacity Building and Training**: RGB conducts training programs, workshops, and seminars aimed at enhancing the capacity of public institutions, civil society organisations , and individuals in matters related to governance, leadership, and accountability.
- **Monitoring and Evaluation**: It oversees the implementation of governance-related policies and programs across various sectors. This involves monitoring the performance of institutions and assessing their adherence to governance standards.
- **Promoting Accountability and Transparency**: RGB advocates for and supports initiatives that promote accountability, transparency, and ethical conduct in both public and private sectors. It encourages organisations to adopt best practices in governance to improve service delivery and foster public trust.
- **Advisory Role**: RGB provides advisory services to government institutions, offering guidance on governance-related matters and assisting in the development of action plans to enhance governance practices.
- **Research and Advocacy**: It conducts research and studies on governance issues to identify challenges and opportunities for improvement. RGB uses this research to advocate for policy changes and reforms that strengthen governance structures. It also explore citizens' perception with service delivery and disseminate the findings;
- **Collaboration and Partnerships**: RGB collaborates with various stakeholders, including government agencies, civil society organisations, and international partners, to foster partnerships aimed at advancing good governance practices and achieving national development goals.

The Rwanda Governance Board (RGB) actively engages with various Ministries to facilitate and promote good governance practices across the Country. This engagement involves working collaboratively with Ministries to develop, implement, and enhance policies and strategies that foster transparency, accountability, and effective service delivery.

As part of its functions, the RGB manages the citizen's scorecard—a tool used to assess citizens' perceptions of public service delivery and the transparency of governmental operations. This scorecard serves as a feedback mechanism, allowing citizens to voice their opinions on the quality of services provided by different government agencies and the transparency maintained in these processes.

When it comes to interactions with the RGB, these engagements can be particularly valuable for gaining insights into the perception of citizens regarding specific digitization efforts managed by a Chief Digital Officer (CDO). For a CDO leading digital transformation initiatives within a public service sector, understanding citizens' perspectives becomes crucial. Insights gathered through the RGB's citizen scorecard can provide valuable feedback, offering a glimpse into how citizens perceive the digital services being implemented.

This insight isn't solely beneficial in ensuring a citizen-centric approach; it also plays a vital role in managing project performance and outputs. By incorporating citizens' perceptions and feedback into the project evaluation process, the CDO can effectively gauge the success of digitization initiatives. This feedback loop aids in refining strategies, optimising service delivery, and ensuring that the digital services align closely with the needs and expectations of the citizens they serve. Ultimately, leveraging RGB interactions and citizen feedback enhances the overall effectiveness and success of public service digitization efforts overseen by a CDO.

The Collaboration between CDOs and Regulations Authorities

Effective collaboration between Chief Digital Officers and ICT regulation authorities is essential for achieving a balance between innovation and regulatory compliance in the evolving digital landscape. This collaboration ensures that digital strategies contribute to economic growth, societal benefits, and regulatory adherence. In Rwanda, RURA is responsible for regulating the ICT sector which oversees the regulatory and standardisation aspects to be observed by both consumers and network/service providers. The CDO network can play a key role in providing consolidated and common inputs to RURA for the sector regulation.

Below are some areas of collaboration:

Policy Alignment and regulatory compliance:

CDOs and CDO Network and ICT regulation authorities should collaborate to ensure that digital strategies align with existing and emerging regulations. This involves understanding regulatory frameworks and incorporating them into digital transformation initiatives. CDOs need to work closely with ICT regulation authorities to ensure that digital initiatives comply with relevant laws, standards, and regulations. This includes data protection, privacy, cybersecurity, and other regulatory aspects.

Dialogue and Consultation:

There can be some ongoing dialogue and consultation channels between CDOs and CDOs Network and ICT regulation authorities. This process will involve regular communication to address challenges and identify opportunities for improvement.

Risk Management:

CDOs and CDOs Network and regulation authorities should collaborate on risk assessments related to digital initiatives. This includes identifying and managing risks associated with technology adoption, data governance, and cybersecurity.

Innovation Promotion:

Collaborative efforts can be directed toward promoting innovation within the bounds of regulations. ICT regulation authorities can create frameworks that encourage responsible experimentation and the adoption of emerging technologies.

Standards Development:

CDOs and CDOs Network can contribute to the development of industry standards by actively participating in standardisation processes. This ensures that digital innovations adhere to established norms and facilitate interoperability.

Data Governance and Privacy:

Given the importance of data in digital initiatives, collaboration is vital in establishing robust data governance and privacy frameworks. CDOs should work with ICT regulation authorities to define guidelines for responsible data management.

In order to enhance collaboration between CDOs and regulation authorities, there is a strategic and proactive approach to run. Here are some keys to foster effective collaboration:

Key 1: Establish Regular Communication Channels and Promote Trust and Transparency:

Set up regular meetings, forums, or workshops for ongoing communication between CDOs and ICT regulation authorities. These platforms provide opportunities for dialogue, information exchange, and addressing emerging issues.

Define clear communication protocols to streamline the exchange of information between CDOs and regulation authorities. This includes processes for submitting feedback, addressing queries, and collaborating on regulatory compliance.

Foster a culture of trust and transparency between CDOs and regulation authorities. Open communication and transparency build confidence and facilitate collaborative problem-solving.

Key 2: Participate in Regulatory Consultations:

CDOs should actively participate in consultations organised by ICT regulation authorities. This involvement allows them to provide insights, share industry perspectives, and contribute to the development of regulations that align with technological advancements.

Key 3: Create a Joint Task Force or Working Group:

Establish a joint task force or working group that includes representatives from both CDOs and regulation authorities. This collaborative team can focus on specific issues, share expertise, and work together on regulatory challenges.

Key 4: Educate and Build Awareness:

CDOs should actively engage in educating regulation authorities about the digital landscape, emerging technologies, and industry trends. Building awareness helps regulators understand the complexities of digital innovation and formulate regulations that are informed and practical.

Key 5: Involve CDOs in the Regulatory Development Process:

Invite CDOs to contribute to the development of ICT regulations. This involvement ensures that regulatory frameworks consider the practical implications of digital initiatives and encourage responsible innovation. Encourage the adoption of industry standards and best practices in regulatory frameworks. CDOs can provide valuable insights into global standards, ensuring that regulations align with international norms.

Key 6: Joint Capacity-Building Initiatives:

Collaborate on capacity-building initiatives, such as training programs and workshops, that enhance the understanding of digital technologies, cybersecurity, and data governance among both CDOs and regulation authorities.

Key 7: Collaborate on Incident Response Planning:

Work collaboratively on incident response planning and cybersecurity measures. Establish protocols for information sharing in the event of cybersecurity threats or incidents that may impact both private and public interests.

Key 8: Establish a Feedback Loop:

Create a feedback loop where CDOs can provide constructive feedback on the effectiveness and practicality of existing regulations. This iterative process helps refine regulations based on real-world experiences. Create feedback mechanisms where CDOs can provide insights to regulation authorities on the practical implications of regulations. This helps in refining policies based on real-world experiences.

Enhancing collaboration between CDOs and ICT regulation authorities is essential for creating a regulatory environment that supports innovation while ensuring compliance and responsible digital practices. By fostering strong partnerships, both parties can contribute to the development of a dynamic and effective regulatory framework.

The collaboration between CDOs and Service Providers

In their daily work, CDOs may interact with other institutions apart from those mentioned above, mainly internet and other resources providers.

The collaboration between Connectivity Providers and the CDO

Frequent communication channels are established between CDOs and the connectivity providers companies, primarily centred around resolving internet access issues. These issues could range from minor glitches to more complex challenges disrupting connectivity. The norm involves resolving these issues remotely, leveraging technology and expertise to troubleshoot and rectify problems without physically being present at the location.

However, for specific and critical issues that demand hands-on attention or intricate on-site diagnosis, the partner team is engaged for on-premise interventions. This direct, in-person approach allows for a more comprehensive understanding of the issue and facilitates tailored solutions to rectify the problems swiftly and effectively.

The collaboration between CDOs and Connectivity providers reflects a responsive and proactive approach to maintaining an efficient and secure digital ecosystem. It signifies a commitment to ensuring uninterrupted connectivity while reinforcing the robustness of the network infrastructure. Through a combination of remote problem-solving and targeted on-site interventions, both parties work synergistically to address challenges and uphold the reliability and efficacy of the digital systems.

CDOs must consult the guidelines that are published by RISA for network connectivity, service providers management guidelines while dealing with these partners.

The collaboration between National Data Center and the CDOs

The National Data Center is responsible for hosting all government data. The entity in charge of managing the national data centre works with the CDOs by offering them hosting and security services. It also manages the network and security systems, implementing regular updates and providing technical assistance to the CDOs.

While interactions with these partners lack a structured framework currently, upcoming projects aim to establish clear service follow-up methods to streamline operations and improve service quality. These methods may include implementing ticketing systems, Service Level Agreements (SLAs), and Key Performance Indicators (KPIs) focused on customer satisfaction.

CDOs must consult the guidelines that are published by RISA on data centres and cloud.

The collaboration between E-service provider and the CDO

The E-Service provider entity collaborates with CDOs to work together on government services digitalization. This collaboration should extend to seeking inputs or guidance from the CDO's team for expertise or advice. Conversely, CDOs should also require inputs, expertise, or specialised services from the partner to bolster their initiatives aimed at improving public services.

Guidelines on Suppliers management published by RISA are applicable here as well.

Collaboration with Software development companies

Software development companies collaborate with government agencies, companies, and organisations to create outstanding user experiences, secure solutions, and support and maintenance across the product/solution lifecycle.

The interactions between the CDOs and these companies are various. CDOs may engage with them given their expertise in web and mobile application development, information security consultancy, and network security services.

The collaboration between CDOs and DPs and Civil Society

Primary development partners help Rwanda in its development vision. CDOs can therefore apply for funding individually or through the supervisory administration (sector/Ministry, MINICT or RISA), in collaboration with development partners. Whether they are investors, sponsors, or supporters, development partners play a pivotal role in providing financial and strategic support. Here are some strategies to enhance collaboration with development partners:

Clearly define Goals and Expectations:

Establish clear and transparent goals for the collaboration. Clearly articulate what you aim to achieve and discuss expectations from both parties. This clarity helps in aligning efforts and avoiding misunderstandings.

Regular Communication:

Foster open and regular communication with development partners. Provide them with updates on the progress of the project, key milestones, and any challenges faced. Regular communication builds trust and keeps backers engaged.

Create a Collaborative Culture:

Cultivate a culture of collaboration where feedback and input from development partners are valued. Encourage an open dialogue where they feel comfortable sharing their thoughts and ideas.

Actively seek input and feedback from development partners on various aspects of the project. Their insights can be valuable in refining strategies, improving products, or addressing challenges.

Involve development partners in Decision-Making:

Include development partners in important decision-making processes. Seek their input on key strategic decisions, service development, or other critical aspects of the project. Involving them enhances their sense of ownership.

Transparency in Finances:

Maintain transparency in financial matters. Clearly communicate how funds are being utilized and provide financial reports. Transparency builds trust and confidence in the way resources are managed.

Showcase Impact and Results:

Demonstrate the impact of development partners' contributions by showcasing tangible results. Whether it's service releases, business growth, or social impact, highlighting achievements helps development partners see the real-world outcomes of their support. The impact and results presentation must be orientated to the centres of interest of the development partners (UN sustainable development Goals, social inclusion, poverty reduction, gender equality, environmental issues…).

Acknowledge and Appreciate:

Acknowledge the contributions of development partners and express genuine appreciation for their support. Publicly recognize their involvement through social media, newsletters, or other platforms. Feeling appreciated strengthens the relationship.

Provide Regular Updates:

Keep development partners informed with regular updates through newsletters, emails, or dedicated communication channels. Highlight progress, share success stories, and address any setbacks transparently.

Organise development partners' events:

Arrange events or webinars specifically for development partners. This creates an opportunity for direct interaction, allowing backers to ask questions, share their thoughts, and feel more connected to the project.

Offer Collaborative Opportunities:

Explore collaborative opportunities where development partners can actively contribute to the project beyond financial support. This could involve partnerships, mentorship programs, or other ways to leverage their expertise.

Secondly, collaboration between CDOs and civil society is essential for building trust, promoting social good, and ensuring that data is used responsibly for the benefit of communities and society at large. It requires a commitment to inclusivity, transparency, and the shared goal of using data for positive social impact.

Civil Society can be involved in these ways:

Open Dialogue and Engagement:

- *Objective*: Foster open communication and engagement between CDOs and civil society organizations.
- *Activities*: Organize regular meetings, forums, or workshops to facilitate discussions on data policies, initiatives, and concerns. Create channels for feedback and input from civil society.

Data Accessibility and Transparency:

- *Objective*: Ensure that data is made accessible to civil society organisations in a transparent and usable format.
- *Activities:* Collaborate on initiatives to publish relevant datasets, adhere to open data standards, and provide user-friendly interfaces. Seek input from civil society on data priorities. The management of the open data set must be under the management of RISA.

Capacity Building:

- *Objective*: Enhance the data literacy and analytical skills of civil society organisations.
- *Activities:* Provide training sessions, workshops, or resources to help civil society understand and effectively use data. Collaborate on educational initiatives to build capacity within the civil society sector.

Joint Advocacy and Awareness Campaigns:

- *Objective:* Work together on advocacy efforts and awareness campaigns related to data rights, privacy, and responsible data use.
- *Activities:* Collaborate on public awareness campaigns, jointly advocate for policies that protect data rights, and address concerns related to data privacy and security.

Project Collaboration:

- *Objective:* Undertake joint projects that leverage the expertise and resources of both the CDO's organisation and civil society.
- *Activities:* Identify areas where collaboration can lead to positive social impact. Develop and implement projects that address social challenges using data-driven approaches.

Inclusive Decision-Making:

- *Objective:* Include civil society representatives in decision-making processes related to data governance and policies.
- *Activities:* Establish advisory committees or forums that include representatives from civil society to provide input on data-related policies, initiatives, and projects.

Feedback Mechanisms:

- *Objective*: Establish mechanisms for civil society to provide feedback on data-related initiatives and policies.
- *Activities:* Implement channels for receiving and addressing concerns, suggestions, and feedback from civil society. Regularly assess and respond to the needs and priorities identified by civil society organisations.

Participatory Data Collection:

- *Objective:* Engage civil society in participatory data collection efforts.
- *Activities:* Collaborate on projects that involve the collection of community-based data, ensuring that civil society is actively involved in the process. This can enhance the

relevance and accuracy of the data collected.

An example of collaboration with civil society can be:

Set a first users community: The concept means gathering a population of volunteers who will test Government services in advance, before they go online for the general public, and give feedback on the service to the CDOs before they start implementing the services.

The concept can be extended to build a platform to collect ideas from civil society on new government services to develop, suggestions of improvement areas on specific e-services…

The Collaboration with own Sector’s Institutions

As per the Ministry's directive, staff members within the CDO or BA's office are specifically assigned to the primary Ministry. Their role is not confined solely to the leading Ministry, instead, they are tasked with dynamically supporting various affiliated institutions or agencies. This indicates a flexible and multifaceted responsibility, catering to the diverse needs of institutions within the Sector.

While the CDO often acts as the primary contact point, the entire team is actively engaged with these sector institutions. Their involvement extends beyond mere interaction, as team members are mobilised and involved in specific projects or tasks crucial to supporting the functions of these institutions.

Given this mandate, the CDO assumes the responsibility of strategically organising the team to ensure optimal resource deployment. This includes the strategic distribution of team members among institutions or dedicating specialised support by assigning Business Analysts to specific groups of institutions. Additionally, the CDO plays a pivotal role in overseeing and coordinating the support rendered to all these institutions.

The overarching goal of this organisational Strategy is to align the team's efforts with the broader interests and goals of the Ministry. By deploying resources effectively and coordinating support across multiple institutions, the CDO ensures that the Ministry's objectives are efficiently met, enhancing digital services and operations within the Sector.

This approach allows the CDO's office to operate in a versatile and responsive manner, strategically deploying its resources to address the varying needs of institutions within the Sector. Through this concerted effort, the CDO contributes significantly to the enhancement of digital services and operational efficiency across multiple institutions, thereby contributing to the Sector's overall advancement and development.

The importance of Academia and research institutions

Academia and research institutions are vital contributors to the ongoing evolution of ICT. They play a crucial role in fostering ICT innovation. Their role encompasses knowledge creation, talent development, collaboration with industry, and addressing societal challenges, collectively shaping the trajectory of ICT innovation.

Knowledge Generation and Dissemination:

Academia conducts cutting-edge research, leading to the creation of new knowledge and insights in the field of ICT. Research institutions contribute to the dissemination of knowledge through publications, conferences, and collaborations, ensuring the broader community has access to the latest developments.

Talent Development:

Universities and research institutions are pivotal in educating the next generation of ICT professionals and researchers. They provide training, academic programs, and hands-on experiences that equip students with the skills needed for innovation in the ICT sector.

Collaboration with Industry:

Collaboration between academia and industry facilitates the transfer of research findings into practical applications. Joint projects and partnerships enable the integration of academic knowledge with industry needs, fostering innovation that is both theoretical and applicable.

Innovation Ecosystem:

Academic institutions contribute to the creation of a vibrant innovation ecosystem by nurturing an environment that encourages creativity, experimentation, and entrepreneurship. Incubators, technology transfer offices, and research centres within academia support the translation of research ideas into tangible products and services.

Applied Research and Development:

Research institutions engage in applied research, addressing real-world challenges and developing solutions with practical applications.

This applied research orientation ensures that innovations are relevant and have the potential to address current issues in the ICT sector.

Technological Breakthroughs:

Academia often leads in the exploration of new frontiers in technology, pushing the boundaries of what is possible in ICT. Breakthroughs in areas such as artificial intelligence, cybersecurity, and data science often originate from research conducted within academic institutions.

Policy and Regulation Guidance:

Academic research contributes valuable insights into the formulation of policies and regulations related to ICT. Researchers provide evidence-based recommendations that help shape policies, ensuring a balanced approach to innovation, ethics, and societal impact.

Global Competitiveness:

Countries with strong academic and research institutions in ICT tend to be more competitive on the global stage. A robust ICT innovation ecosystem enhances a nation's capacity to stay at the forefront of technological advancements and maintain a competitive edge in the global market.

Social Impact:

Academia plays a role in addressing societal challenges through ICT innovations that can improve healthcare, education, accessibility, and other aspects of daily life. Research institutions contribute to the ethical considerations and responsible development of technology with a focus on positive societal impact.

The CDO Network can work closely with Academia and research institutions, as well as common activities under the coordination of RISA. In addition, RISA and MINICT can play a role in creating strong partnerships with academia and research institutions. RISA and MINICT can initiate contact, provide a framework for interaction and open up various possibilities for collaboration that CDOs will explore with the academia and research institutions. Successful collaboration requires ongoing commitment, flexibility, and a shared understanding of the objectives. By fostering strong partnerships with academia and research institutions, sectors can tap into a wealth of knowledge and contribute to advancements in their respective fields as well as fostering innovation. Below are some best practices in a collaboration with Academia and research institutions.

Stage 1: Identify Common Goals and Objectives:

Clearly define the goals and objectives of the collaboration. Understand what both parties aim to achieve and ensure alignment with each other's missions and objectives.

Stage 2: Establish Clear Communication Channels:

Establish effective communication channels to facilitate the exchange of ideas, progress updates, and feedback. Regular meetings, emails, and collaborative platforms can enhance communication.

Stage 3: Build Relationships:

Develop relationships with key faculty members, researchers, and decision-makers within academia. Attend conferences, seminars, and networking events to establish connections.

Stage 4: Engage in Joint Research Projects:

Collaborate on joint research projects that align with the interests and expertise of both parties. This can lead to the generation of new knowledge and innovative solutions.

Stage 5: Provide Access to Resources:

Offer access to resources that academia may not have readily available, such as industry data, technologies, or real-world scenarios. This can enhance the practical relevance of research projects.

Stage 6: Participate in Advisory Boards:

Join advisory boards or committees within academic institutions. Your industry expertise can contribute valuable insights to curriculum development, research agendas, and overall strategic planning.

Stage 7: Facilitate Workshops and Training Programs:

Offer workshops, training programs (internship opportunities and work experience for students), or guest lectures to share industry insights, trends, and practical experiences with students and faculty members.

Stage 8: Promote Technology Transfer:

Explore opportunities for technology transfer, where innovations developed within academic settings can be applied commercially. This can lead to the development of new products, services, or processes.

Stage 9: Collaborate on Conferences and Events:

Sponsor or participate in conferences, symposiums, or industry events organised by academia. This provides exposure to cutting-edge research and facilitates networking opportunities.

Stage 10: Understand Intellectual Property (IP) Agreements:

Clearly define intellectual property ownership and rights in collaboration agreements. Establish agreements that protect the interests of both parties regarding the use and commercialization of research outcomes.

Stage 11: Evaluate the Impact:

Regularly assess the impact of the collaboration on both the organisation and academia. Measure outcomes, share success stories, and identify areas for improvement.

Stage 12: Promote Diversity and Inclusion:

Encourage diverse participation in collaborative initiatives. Embrace inclusivity in research teams and ensure that different perspectives contribute to innovative solutions.