

# 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.

---

Revision #1

Created 9 July 2025 21:32:19 by RISA

Updated 9 July 2025 21:33:41 by RISA