CDOs Key Functions and Roles

- Strategic Leadership
- Digital Culture and Innovation
- Ensuring a Quality Data Governance
- Ensuring a Quality Cybersecurity
- Quality Management System
- Sector Digital Maturity Assessment and Action Plan
- IT Operations
- Risk Management
- Internal Audit
- Financial Responsibilities
- Procurement and Vendor Management

Strategic Leadership

Aligning digital strategies with national strategies

Aligning sector digital Strategy with national strategies is crucial for cohesive and effective development. As a CDO evolves in an advanced digital context, it is mandatory to align sector Strategy to nationwide strategies. Please refer to the part on National strategies to learn about national digital strategies that are in place in Rwanda.

Please refer to the Sector Blueprint definition guidelines to see how to develop sector digital transformation strategy in the alignment of national strategies.

Setting KPIs for performance measurement

A specific document on the KPIs that should be monitored by a CDO is available at RISA. Please refer to the dedicated document on the KPIs set and implement them.

Digital Culture and Innovation

Establishing a sector-wide digital culture

The CDOs mandate and ambition is to achieve a level where a sector-wide digital culture takes root in the sector, set-up an environment where innovation, digital adoption, and adaptation become ingrained in the sector's DNA.

Establishing a sector-wide digital culture has many advantages:

- It enables staff to acquire a good digital culture which will be a catalyst for the administration's digital transformation.
- It improves the acceptability of the staff of the digital changes implemented by CDOs.
- It accelerates digital transformation through the involvement of all stakeholders.
- It improves collaboration and innovation because sector staff are involved in the process.

Establishing a sector-wide digital culture involves a concerted effort to foster an environment where digital innovation, adoption, and adaptation are embraced at all levels.

Here are some steps to establish a sector-wide digital culture:

Leadership Buy-In: The CDO has to start at the top. Leaders must champion digital transformation, demonstrating its importance and integrating it into the sector's vision and Strategy. Without the sector leadership support, it is more difficult to achieve a digitally rooted environment in sectors.

Communication and awareness campaigns: It is necessary for the CDO to identify and educate stakeholders about the benefits and necessity of digital transformation. This involves regular communication about the sector's digital vision once defined and demonstrates that each individual role is crucial. Various tools can be used to do so: tutorial, internal communication campaign, webinar, guides... These communications must be precise, and the objective must be clear, information simplified, and the benefits highlighted.

Training and Upskilling: Investing in training programs to equip employees with digital skills is necessary. This could include workshops, courses, or certifications relevant to the sector's needs. A common program can be set-up at RISA’s level for all Ministries, but all CDOs can adapt it to his/her sector. Here, specific domains can be targeted and be topics of training: cybersecurity, paperless Strategy, efficiency through technology, etc...

Encourage Innovation: The CDO can create an environment that encourages experimentation and innovation within the sector’s leading Ministry and affiliated agencies. He/she should support initiatives that explore new digital technologies and methodologies.

Collaboration and Cross-Functional Teams: Foster collaboration among different departments and encourage the formation of cross-functional teams to work on digital projects. This breaks

down silos and encourages knowledge sharing. This encompasses activities to gather employees from all over the sector (leading Ministry and affiliated agencies) to work on a specific project.

Agile and Adaptive Approach: Embrace an agile mindset that allows for quick adaptation to changing technologies and market needs. Encourage iterative processes and learning from failures.

Provide Resources and Support: Ensure that the necessary resources, tools, and infrastructure are available to support digital initiatives. This includes both technological resources and managerial support.

Recognition and Incentives: Recognize and reward individuals and teams that contribute significantly to the sector's digital goals. Incentivise innovative ideas and successful digital implementations.

Data-Driven Decision Making: Promote a culture of using data to drive decisions. Encourage the collection and analysis of data to derive insights and inform strategies.

Regular Assessment and Adaptation: Continuously assess the progress of the digital culture initiatives. Adapt strategies based on feedback and changing needs to ensure sustained improvement.

Promoting Digital Literacy

Promoting digital literacy directly engages the employees all over the sector. CDO simply must conduct basic activities to enhance the digital literacy of the leading Ministry and affiliated agencies staff. The overall goal is to enhance digital literacy among employees, empowering them to leverage technology effectively in their roles and improve overall operational efficiency.

The first step in building digital literacy is to assess the sector current workforce’s digital skills and determine which skills are necessary to make the digital transformation roadmap a reality.

Take stock of existing skills in the public sector: understand the transformations that all job families will undergo and identify gaps and specific areas where training is needed.

Professions within public administration are undergoing transformations due

The following table describes common government job functions and the transformations they are experiencing in a digital transformation. All positions are impacted, from management to legal services, hence the importance of extending digital literacy across government.

Profession type	Transformations
Purchasing in the digital sector	From acquiring equipments and network to purchasing cloud, infrastructure, software and intellectual services

Cybersecurity/Cybercrime	Enhance capacity to respond to new threats and respect standards
Stats/Data	From producing statistics to analysing raw data and making them available from public-decision making
Management & steering leadership	Adopt new ways of working: agile, remote, distributed governance
Development	Generalisation of the DevOps approach, new standards on eco conception, accessibility (design), use (and production) of open source softwares
Legal	Compliance (data privacy and new regulations), legal design
Infrastructures	From a “static” (IT architecture) to a dynamic vision (Ops, data circulation)
User support	Enhance relations to digital services users, measure impact
Project/Product Management	New methods to develop digital services for public policies
Communication	From institutional communication to community management

Set-up tailored Training Programs: Develop training programs that cater to various skill levels and job roles. Offer a mix of basic digital literacy courses covering fundamental skills like using software, email, and the internet, as well as more advanced courses for specific tools or technologies relevant to their roles and depending on their prerequisites.

Hands-On Workshops and Webinars: Conduct interactive workshops and webinars where employees can practise using digital tools in real-time. Encourage participation and provide opportunities for Q&A sessions.

- *Organise training and awareness campaigns on the digital issues*: IT Tools, collaborative tools. This encompasses organisation of training programs to upskill employees on new technologies, ensuring they can effectively use and leverage these tools.
- *Organise regular follow-up and workshops sessions on the IT ongoing projects* in the sector, in order to involve employees in the transformation projects.

Digital Resources and Support: Offer access to digital resources such as online tutorials, guides, and FAQs. Provide ongoing support through help desks or designated digital literacy mentors. Realise some demo and tutorial on IT tools usage, IT key topics for the sector’s staff. These

resources should be included on a dedicated webpage of the Ministry or on other specific webpage easily accessible to the employees.

Encourage Continuous Learning: Foster a culture of continuous learning by promoting online courses, certifications. Encourage employees to stay updated with technological advancements relevant to their roles.

Internal Knowledge Sharing: Facilitate knowledge sharing sessions where employees can share their expertise or experiences with digital tools. This could be through presentations, team meetings, or internal forums.

Pilot Projects and Sandbox Environments: Encourage employees to experiment with digital tools in a safe environment. Implement pilot projects where they can apply newly learned skills without the fear of failure.

Measurement and Feedback: Implement measures to assess the effectiveness of training programs. Gather feedback from employees to understand their experience and areas that need improvement. Reward the most involved employees/agents

Incorporate Digital Literacy into Policies: Embed digital literacy requirements into job descriptions, performance evaluations, and promotion criteria, emphasising its importance in the administration.

Various mechanisms must be put in place to build up digital literacy among all civil servants:

- **Digital academies:** set up an in-house digital academy to assess and develop current civil servants digital skills
- **Formal training:** Include formal training opportunities as part of your compensation package for civil servants and ensure that digital skills are available in course catalogues.
- **Informal training:** Encouraging civil servants to join a community of practice, giving opportunities for internal mobility and developing a culture of collaboration can all offer informal training opportunities for staff.

Digital Campus: An emerging cross-department resource centre to offer customised training to teams and individuals. It is made up of dedicated teams in charge of:

- Guiding HR offices & business managers to build trainings for teams:

- Identification of needs
- Conception of learning path (usually upskilling)
- Implementation
- Evaluation

- Building & Providing a training catalogue on every aspects of digital transformation

- Online / Presential
- In house / provided by external providers

- Possibility to obtain funding to build new learning approaches

- Possibility for civil servants to become teachers.

Digital Academy: An Academy which aims at teaching public servants the digital skills, approaches, and mindset needed to transform public services in today's digital age.

As part of its activities, the Academy must bring together partners from different spheres, including Government, Academia and the Private Sector, with the focus on Collaboration and the sharing of knowledge and experience. The Academy will offer both general and more specialised learning opportunities, in the classroom and online, for public servants at all levels.

Another good practice is also to **let civil servants find their own training courses** based on their interests and skills. This means potentially financing online courses given in other countries or about topics not yet included in the initial training catalogue. This promotes talent retention and gives staff maximum flexibility to advance their careers as they see fit.

Fostering Innovation and Growth

Fostering innovation and growth entails establishing an environment that champions creativity, experimentation, and ongoing enhancement. Innovation stands as a linchpin, and CDOs must cultivate it within their sector.

This endeavour begins by **nurturing a culture of innovation** within the team. The CDO plays a pivotal role in fostering a mindset that appreciates fresh ideas and solutions, fostering an environment where employees feel empowered to share their thoughts without fear of judgement. Embracing failure as a learning opportunity is integral—encourage experimentation and acknowledge that not all ideas will yield success.

Cultivating an innovation culture also entails **promoting diverse collaboration**. Encouraging teamwork among individuals with varied backgrounds, skills, and experiences often leads to novel and inventive ideas.

Furthering this culture means **embracing failure as a stepping stone to success**. Create a safe space where unsuccessful attempts are seen as opportunities for growth. Discuss lessons learned from setbacks and apply these insights to future endeavours.

Having dedicated resources—be it budget, teams, or platforms—is crucial. Allocate specific resources to innovation projects, empowering teams with the necessary time, finances, and personnel. Establish **platforms for idea sharing and encourage cross-functional collaboration** among different departments or areas of expertise, fostering the exchange of unique ideas that lead to innovative solutions.

Learning serves as the bedrock of an innovative culture by fostering adaptability, continuous improvement, and knowledge sharing. It encourages individuals to refine processes and seek better solutions, driving efficiency and effectiveness. CDOs should work with RISA core team to

design the training catalog and invest in **ongoing learning programs** to keep employees updated with the latest trends and technologies.

Conducting innovation improvement activities is essential to nurture an innovation culture. These activities may include brainstorming sessions, problem-solving challenges, workshops, and collaborative events to ignite creativity and teamwork within the team.

- **Brainstorming Sessions**: Encourage open brainstorming sessions where team members freely share ideas without judgement. Focus on quantity over quality initially to generate a wide range of ideas.
- **Problem-Solving Challenges**: Present the team with real or hypothetical challenges and ask them to come up with innovative solutions. Encourage creative thinking and unconventional approaches.
- **Cross-Training and Skill Sharing**: Organise sessions where team members share their expertise or teach skills to others. This promotes a diverse skill set within the team and encourages learning from each other.
- **Innovation Workshops**: Host workshops specifically aimed at fostering innovation. Use exercises, case studies, or role-playing activities to stimulate creative thinking and problem-solving.
- **Hackathons or Innovation Days**: Set aside dedicated time for the team to work on innovative projects or ideas. Encourage them to collaborate across departments and generate prototypes or new concepts. These activities may involve external partners: innovators, private sector, academia, start-ups, researches…
- **Mind Mapping or Visualization**: Use visual tools like mind mapping to help team members organise their thoughts and explore connections between different ideas or concepts.
- **Field Trips or External Insights**: Arrange visits to other innovative companies or industries. Exposure to different environments often sparks new ideas and perspectives.
- **Design Thinking Exercises**: Introduce the team to design thinking methodologies, allowing them to empathise with users, define problems, ideate solutions, prototype, and test ideas.
- **Storytelling Sessions**: Allow team members to share success stories, innovative ideas, or lessons learned from challenges. This fosters a culture of sharing and inspires others to think creatively.
- **Gamification of Learning**: Incorporate games or challenges that encourage creative thinking, problem-solving, and teamwork. This adds an element of fun while promoting innovation.

The CDO can also **conduct reward innovation activities**. The aim is to recognize and reward employees who contribute innovative ideas or solutions. Incentivize creativity through rewards, bonuses (co-defined with RISA and MIFOTRA), or recognition programs.

Regular **evaluation and feedback mechanism** is mandatory. Establish mechanisms to regularly evaluate innovation initiatives. Gather feedback from employees and stakeholders to understand what works and what needs improvement.

Ensuring a Quality Data Governance

Data Governance is one of the strategic tasks that the CDO and his/her team must manage. The Standards obliges the CDOs to host their data in the cloud by collaborating with the partner in charge of data hosting and cloud for the Government.

However, apart from dealing with the National Data Center for hosting the data of the Ministries, the CDO has a strategic role to play in the data governance issue. Indeed, ensuring robust data governance involves establishing policies, processes, and practices to manage data effectively, securely, and in alignment with organisational goals. Here are key steps to achieve this:

- **Define Clear Objectives**: Establish clear data governance objectives aligned with the sector's overall Strategy. The various ICT laws (Data protection, security and cybersecurity, data privacy..) should be considered. Define what "good data governance" means for your specific context—whether it's data quality, security, compliance, or accessibility.
- **Leadership and Accountability**: Assign ownership of data governance to a dedicated team or team member. Ensure there's strong leadership support to drive data governance initiatives and establish accountability for data-related decisions.
- **Develop Policies and Standards**: Create comprehensive data governance policies, standards, and guidelines. These should cover data quality, security protocols, access controls, data lifecycle management, and compliance requirements.
- **Data Inventory and Classification**: Conduct a thorough inventory of all data assets, categorise them based on sensitivity and importance, and establish clear classification protocols. This ensures appropriate handling and protection of different types of data.
- **Data Quality Management**: Implement measures to maintain and improve data quality. Establish procedures for data cleansing, validation, and regular quality checks to ensure accuracy and reliability.
- **Data Security and Privacy**: Institute robust security measures to safeguard data from breaches or unauthorised access. Implement encryption, access controls, user authentication, and regular security audits. Ensure compliance with relevant data privacy regulations.
- **Data Lifecycle Management**: Define processes for data creation, storage, usage, archiving, and deletion. Establish clear guidelines for how long data should be retained based on legal, business, or regulatory requirements.
- **Data Governance Framework and Processes**: Develop a structured framework for decision-making, change management, and communication regarding data governance initiatives. Ensure that data-related processes are documented and communicated across the organisation.
- **Training and Awareness**: Conduct training programs (organising, or hosting trainings from institutions like MINICT, RISA) to educate employees on data governance policies, procedures, and best practices. Encourage a culture of data awareness and responsibility across the departments.

- **Continuous Monitoring and Improvement**: Regularly monitor compliance with data governance policies and standards. Gather feedback, conduct audits, and refine processes to adapt to changing business needs and technological advancements.

Ensuring a Quality Cybersecurity

In terms of Cybersecurity, the CDOs have the responsibility to follow the guidelines and standards provided by the NCSA and RISA. These guidelines are published on their respective websites or communicated directly to the CDOs.

CDOs also have to contact the appropriate authorities to intervene in case threats are detected, or to come to implement some cybersecurity guidelines. The CDOs responsibility covers the compliance with Regulations in terms of cybersecurity. He/she has to ensure that the department complies with relevant cybersecurity regulations and standards applicable.

Thus, the CDO must conduct regular Risk Assessment and Management. It involves conducting regular risk assessments to identify potential vulnerabilities and threats and develop a risk management plan to prioritise and mitigate these risks effectively.

The CDO also must conduct team members training and awareness by educating all department members about cybersecurity best practices. The CDO must conduct regular training sessions to raise awareness about phishing, social engineering, and other common cyber threats.

Another key action is the access control and authentication. It covers the implementation of strong access controls and authentication mechanisms. It enforces the principle of least privilege, ensuring users have access only to the data and systems necessary for their roles.

Some Regular Updates and Patch Management are necessary. The CDO must keep all software, operating systems, and security tools up to date with the latest patches and updates as vulnerabilities often arise from outdated software versions.

The CDO and his/her team must secure Network Infrastructure by implementing firewalls, intrusion detection systems, and encryption protocols to protect the department's network. Regularly monitor network traffic for unusual activities are necessary.

In addition, there are some key actions that are necessary to assure a good cybersecurity in the departments:

- **Data Encryption**: Encrypt sensitive data both at rest and in transit to prevent unauthorised access in case of a breach.
- **Incident Response Plan**: Develop a clear and tested incident response plan to handle cybersecurity incidents effectively. This includes steps for containment, investigation, recovery, and communication.
- **Regular Security Audits and Assessments**: Conduct periodic security audits and assessments to evaluate the effectiveness of existing security measures and identify areas for improvement.
- **Vendor and Third-Party Risk Management**: Assess the cybersecurity measures of third-party vendors and contractors. Ensure that they comply with your department's security standards.

- **Continuous Monitoring and Improvement**: Implement systems for continuous monitoring of cybersecurity measures. Stay updated on emerging threats and adapt security strategies accordingly.

Quality Management System

A **Quality Management System** (**QMS**) is a structured framework implemented by organisations to ensure they meet and maintain certain standards of quality in their products, services, processes, and overall operations. It's a systematic approach designed to enhance efficiency, consistency, and customer satisfaction while continuously improving the organisation's performance.

A QMS is a comprehensive approach that involves all levels and functions within an organisation, aiming to embed a culture of quality, continuous improvement, and customer satisfaction. Here are some **key components and aspects typically associated with a QMS**:

Quality Policies: These are overarching statements or guidelines set by the organisation's management, outlining its commitment to quality standards and objectives. These policies often reflect the organisation's values and goals.

Processes and Procedures: QMS involves defining and documenting specific processes and procedures for various aspects of operations. This includes everything from product development, service delivery, to internal audits and corrective actions. The aim is to ensure standardised and consistent methods are followed throughout the organisation.

Quality Planning: This involves setting quality objectives, defining processes to achieve them, and allocating necessary resources. It includes risk assessment and mitigation strategies to anticipate and address potential issues.

Quality Control: This encompasses the measures put in place to monitor and verify that products or services meet predefined quality criteria. This can involve inspections, testing, and checks at various stages of production or service delivery.

Continuous Improvement: A fundamental aspect of a QMS is the commitment to ongoing enhancement. This involves collecting and analysing data, feedback, and performance metrics to identify areas for improvement and implementing changes to enhance overall quality.

Training and Education: Ensuring that employees are well-trained and equipped with the necessary skills and knowledge is crucial. Training programs are often an integral part of a QMS to ensure that everyone understands and complies with quality standards.

Customer Focus: A QMS often emphasises understanding and meeting customer needs and expectations. Feedback mechanisms and customer satisfaction surveys are commonly used to gauge and improve customer experiences.

Certification and Standards: Many organisations adopt internationally recognized standards (such as ISO 9001) to guide the development and implementation of their QMS. Achieving certification against these standards can signal to stakeholders and customers that the organisation adheres to certain quality benchmarks.

The QMS should be managed at RISA level and deployed by CDOs in their respective ministries. Please refer to RISA, NCSA and MINICT guidelines on the Quality Management System.

In order to establish a successful and robust Quality Management System (QMS), several steps must be initiated. Here are key steps to guide the CDO in its willingness to establish QMS within his/her Ministry.

Understand Organisational Needs and Objectives:

Identify your organisation's quality objectives, customer expectations, and regulatory requirements. Ensure alignment between these factors and the QMS you plan to implement.

Leadership Commitment:

Obtain commitment and support from top management. Leadership involvement is crucial for implementing and sustaining a QMS throughout the organisation.

Formulate a Quality Policy:

Develop a clear quality policy that outlines your organisation's commitment to quality, its objectives, and the principles that guide the QMS.

Define Processes and Procedures:

Document existing processes and procedures or develop new ones to achieve quality objectives. Ensure these are standardised, understood, and followed across the organisation.

Training and Awareness:

Provide adequate training to employees regarding the QMS, their roles, and how they contribute to maintaining quality. Ensure awareness and understanding at all levels.

Implement Quality Control Measures:

Put in place mechanisms for quality control, including inspections, testing, and checkpoints throughout the production or service delivery process.

Establish Quality Assurance Practices:

Implement systems to ensure compliance with quality standards. This includes regular audits, reviews, and corrective actions to maintain consistency and adherence to standards.

Continuous Improvement:

Foster a culture of continuous improvement by collecting and analysing data, feedback, and performance metrics. Encourage innovation and the implementation of improvements.

Customer Feedback and Satisfaction:

Establish channels for gathering customer feedback and use it to drive improvements. Ensure that customer needs and expectations are consistently met or exceeded.

Monitoring and Review:

Regularly monitor and review the QMS to assess its effectiveness. Use internal audits and management reviews to identify areas for improvement.

Seek Certification and Compliance:

QMS should be aligned with recognized standards such as ISO 9001 and work towards certification to demonstrate adherence to quality benchmarks.

Adaptation and Evolution:

Continuously adapt the QMS to changing organisational needs, industry standards, and technological advancements.

The CDO must keep in mind that the key to a successful QMS lies not only in its implementation but also in its continual maintenance and improvement. It should be an integral part of the organisation's culture and operations, driven by a commitment to delivering quality products or services.

Sector Digital Maturity Assessment and Action Plan

Within the responsibility of infusing and enhancing the sector's digital culture, the CDO also must enhance the digital maturity of the sector.

Sector digital maturity refers to the **level of advancement and sophistication in the adoption, integration, and utilisation of digital technologies within a particular ministry or sector**.

Maturity models are widely used tools, typically **employed for self-assessment**, to help organisations gauge their current capabilities in specific functional, strategic, or organisational areas. By self-assessing and discussing various maturity levels and descriptors, organisations can develop a shared understanding of the changes needed to advance to higher maturity levels over time.

It encompasses various dimensions, including **Governance** in the digital landscape, the extent to which digital **processes and tools** are embedded in the sector's operations and strategies, the **employees digital literacy** and IT readiness and the **change management** in digital field relevance.

Assessing digital maturity involves evaluating how effectively a sector leverages digital innovations to enhance efficiency, service delivery and citizen engagement.

A tool is designed to help CDOs to conduct the digital maturity assessment in the Rwandan context. Structured into **4 pillars**, each **pillar is structured into axis and sub-axis**. Each sub-axis is made of **several questions with 5 options**. The CDO must **choose the option that is the most suited to the current sector's current situation**. Based on the option selected, the tool will give a score for each axis and pillar.

The Pillars of the Digital Maturity Model:

1. **Governance:** Assesses strategic alignment, leadership commitment, digital policies and reporting routines regarding digital
2. **Tools, Processes, and Methodologies**: Reviews the sophistication, automation, standards, and integration of digital tools and technologies in the Business.
3. **People and Resources:** Evaluates workforce skills, training programs, teams' composition and size, and the collaborative culture supporting digital transformation.
4. **Change Management**: Analyses communication strategies, change adaptability and internal collaboration to improve innovation.

The levels of the maturity grid are:

1. **Initial stage:** describes sectors that have not yet defined their digital path and are still relying on legacy and traditional processing methods.
2. **Emerging stage:** describes those sectors that have undertaken or are undertaking digitization reforms as part of their progress towards the medium level of digital maturity.
3. **Operational stage:** describes sectors that have reached a certain level of maturity thanks to structured actions undertaken in the past. The sector is beginning to be rewarded in terms of digital integration, the alignment of digital with business objectives.
4. **Advanced stage:** describes sectors that have developed in terms of digital maturity. They serve as a benchmark for other sectors, use digital to drive innovation, are well shared across the organisation and are continually improving to stay at the forefront of digital trends.
5. **Leading:** This level is intended to represent the leading edge of what is generally possible today, with some collaboration with stakeholders. Sectors here are looking at what might be possible in the longer term, moving towards more transparent and increasingly demanding industry standards.

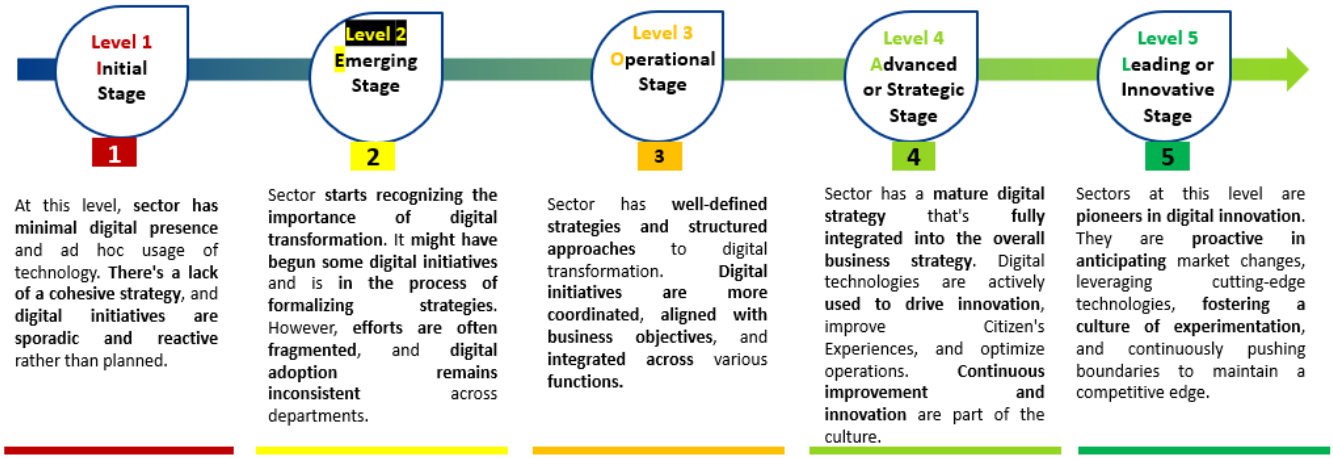

Figure 10: Digital Maturity Model levels

On each axis, several questions are designed to be completed by RISAs because the axes and sub-axes analysed are managed at RISA or central level. These areas should be monitored by RISAs, although CDOs may still make recommendations.

When filling in the Maturity Model, CDOs should gather some prerequisites:

Plan the assessment in advance: planning the assessment means finding the relevant resources to participate in the assessment. A referent can be designated per axis regarding the nature of each talent work in a team. For example, the one in charge of Cybersecurity in the team is well placed to conduct the assessment on the Cybersecurity axis.

Find enough time to conduct the assessment: The assessment can be done pillar per pillar and not necessarily the whole grid at one time. The depth demanded by each question requires time to be devoted to the exercise, and CDOs need to ensure that this is the case.

Use the KPIs set developed in the framework of the grid prior to the assessment in order to reduce subjectivity. Please refer to RISA to get the KPIs set associated with the Digital Maturity Model.

Be honest in your self-assessment: don't forget to fill in the column on justification so that you can check the option you have chosen.

Include a party from outside the Ministry in the evaluation: For example, a CDO from another ministry/sector could take part in the evaluation, act as referee/moderator to settle any differences of opinion and provide an outside perspective.

Continue to monitor progress from one year or assessment period to the next.

Provide feedback to RISA when applying the tool in order to enhance.

The **step after the completion of the Digital Maturity Model** is to **draw an action plan** to **reach the next level of maturity**. To draw the action plan, CDOs can rely on the description of each step in the digital maturity through the options. For example, selecting option 2, means that to reach the next level, the sector should complete the following statement or option.

The action plan should then be sent to RISA for validation before implementation.

Pillar	Axis/subaxis	Current Maturity level	Target for next 6 months	Digital Maturity improvement actions	
	Axis 1: Sectoral legal Framework	Initial Stage		**Actions**	**Accountable**
	Sectoral legal framework				
	Axis 2: Organization and Culture	Emerging Stage		**Actions**	**Accountable**
	Structure of the organization				
	Knowledge management				
	Axis 3: Mission and vision (Sector level)	Operational Stage		**Actions**	**Accountable**
	Mission and vision statement orientation				
	Horizon of goals for digital				
	Axis 4: Digital policies	Advanced Stage		**Actions**	**Accountable**
	Digital policies				
	Axis 5: Leadership and governance	Leading Stage		**Actions**	**Accountable**
	Leadership commitment into Digital				
	Governance structure established for digital monitoring				

Figure 11: Extract of the action plan to enhance sector's digital maturity

After having identified the actions and having defined them in the Action Plan table, CDOs should share the Action Plan with the Accountable persons identified for agreement and follow-up. Regular follow-up meetings must be scheduled to monitor the implementation of the action plan.

IT Operations

Daily tasks management of the Chief Digital Officer

The role of a Chief Digital Officer (CDO) as a supervisor of the IT Department can be multifaceted, blending both operational and strategic responsibilities. **Operational tasks, like ensuring systems run smoothly, data governance, and daily management, are crucial for the organisation's efficiency**. However, without proper planning and delegation, these tasks can consume a significant portion of the CDO's time, **potentially hindering strategic initiatives**.

Effective planning and organisation are indeed vital. Delegating operational tasks to competent team members, such as business analysts, can allow the CDO to focus on strategic projects. This Strategy optimises the use of resources and expertise within the department, ensuring that both day-to-day operations and forward-looking projects receive adequate attention.

It's essential to assess the team's size and capabilities to properly delegate tasks. Larger teams should allow for more specialised roles, whereas smaller teams should require more flexible task allocation. A well-structured plan can ensure that both operational and strategic aspects receive the necessary attention without overwhelming any team member, including the CDO.

Below is a **list of operational tasks** which are under the responsibilities of a CDO (or Business Analyst), not restrictive:

- **Systems Maintenance**: Overseeing the maintenance and functionality of hardware, software, and network systems to ensure they run smoothly and securely.
- **Data Governance**: Implementing and enforcing data governance policies to maintain data quality, security, and compliance with regulations.
- **Cybersecurity Management**: Directing efforts to protect the organisation's IT infrastructure from cyber threats, including managing security protocols, incident response, and risk assessment.
- **IT Infrastructure Management**: Planning and managing the organisation's IT infrastructure, including servers, databases, cloud services, and other critical technology resources.
- **IT Support and Helpdesk Management**: Ensuring efficient and responsive IT support services for employees, troubleshooting issues, and overseeing help desk operations.
- **Service providers and vendor management**

Alongside these responsibilities, some **general tasks are listed** (not restricted) as follows:

- **Budgeting and Resource Allocation**: Developing and managing budgets for IT initiatives, including allocating resources effectively across various projects and departments.
- **Vendor and Stakeholder Management**: Collaborating with external vendors for software/hardware procurement and managing collaborations with stakeholders across the organisation.

- **Policy Development**: Developing and updating IT policies and procedures to align with organisational goals and industry best practices.
- **Project Oversight**: Supervising ongoing IT projects, ensuring they stay on track, meet deadlines, and align with strategic objectives.
- **Performance Monitoring and Reporting**: Tracking IT performance metrics, analysing data, and presenting reports to management to evaluate IT effectiveness and propose improvements.

These tasks require a balance between day-to-day operations and long-term strategic planning to ensure the smooth functioning of the organisation's IT landscape.

Strategic projects on which CDO or Business Analyst can be involved daily are various:

- **Sector Digital Transformation Strategy and IT Roadmap Development**: Creating long-term plans that align IT initiatives with the Ministry or sector’s goals, considering technology trends and potential impact. It is also about developing and implementing strategies to leverage emerging technologies (like AI, IoT, or cloud computing) to enhance processes and outcomes. It covers the implementation of the Rwandan National Digital Transformation Plan-Smart Rwanda Master Plan
- **Citizen’s Experience Enhancement**: Identifying opportunities to use technology to improve citizen experiences, potentially through better user interfaces, personalised services, etc.
- **Innovation management**: Leading efforts to explore new technologies, conducting research and development activities to identify opportunities for innovation within the organisation.
- **Strategic Partnerships**: Identifying and fostering partnerships with tech vendors, startups, or research institutions to bring innovative solutions and stay ahead in the industry.
- **Change Management**: Overseeing change management processes related to technology adoption, ensuring smooth transitions and buy-in from stakeholders.
- **Data Strategy and Analytics**: Developing a comprehensive data Strategy, including data governance, analytics capabilities, and leveraging data insights for informed decision-making. On this task, close collaboration with the National Data Center is key.
- **Cybersecurity Strategy**: Creating and implementing robust cybersecurity strategies to safeguard the organization against evolving threats and ensuring compliance with regulations. On this task, collaboration with the NCSA is key.
- **IT Talent Management and Development**: Developing strategies for retaining IT talent to maintain a skilled and motivated workforce. As the recruitment and training parts are under the management of RISA, the CDO should focus on the retention of talent.

These strategic tasks involve vision, planning, and alignment of technology with the organisation's overall objectives to drive innovation, efficiency, and competitive advantage.

Technical department structure (IT resources)

The CDO as a Head of the IT Department works in a structure defined according to the size of the Ministry's ICT team. Components of the structure are:

- **IT Project Management**: Oversees and coordinates the planning, execution, and completion of IT projects within the department. This component is managed in many cases by the CDO and the Business Analyst (s).
- **Software Development/Engineering**: Engages in creating, maintaining, and enhancing software applications critical to the organisation's operations. It includes the development, design and implementation of new software solutions or modification and upgrade of the existing ones, provides quality assurance and technical evaluation of new and legacy systems and software products in the sector. The Senior Developer oversees this role and is supported by a team of developers.
- **Network Operations**: Responsible for maintaining and managing the organisation's network infrastructure, ensuring connectivity, security, and reliability. The network specialists are in charge of that.
- **Systems Administration**: Manages and supports servers, operating systems, and related software to ensure smooth operations and security across the organisation. The System Administration Specialist is in charge of the system Administration.
- **Database Management**: Handles the design, implementation, and maintenance of databases vital for storing and retrieving organisational data. The Database Administration Specialist is in charge of this role.
- **Help Desk/Technical Support**: Provides frontline support to users, troubleshooting technical issues, and offering guidance on IT-related problems. The IT Help Desk Officer is in charge of this role within the CDO team.

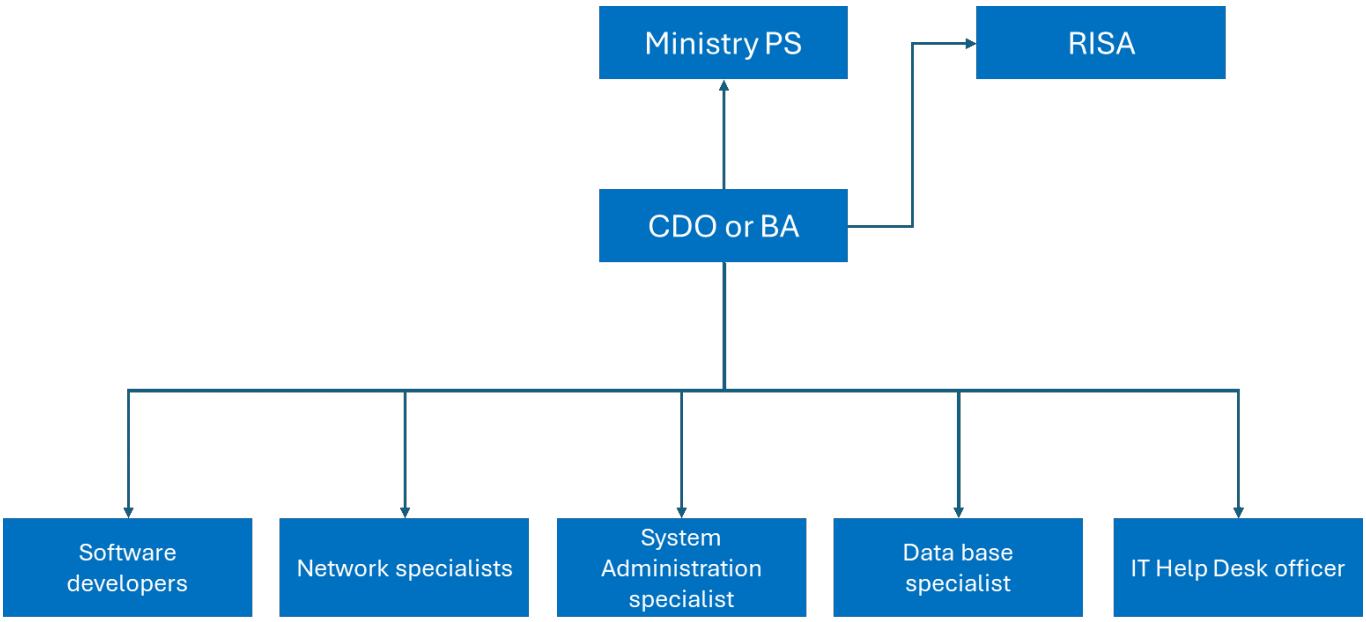

Figure 12: CDO Office Structure

ICT related Logistics and ICT Assets Management

An ITSM tool with built-in asset management functionalities becomes essential for enhanced asset management across various sectors within the Ministry.

The Chief Digital Officer (CDO) holds responsibility for acquisition, maintenance, and disposal of ICT assets within his/her or her Ministry. In this regard, collaborating closely with the Logistics Office of the Ministry is key.

The responsibility for managing the database of IT assets typically falls under the purview of the IT Support staff, who collaborate with the Logistics Office of the Ministry. Together, they ensure accurate and up-to-date records of IT assets are maintained, covering acquisition, maintenance schedules, and disposal processes.

At the national level, the Ministry of Finance utilises a budget management tool that incorporates a module dedicated to asset management. This tool likely assists in tracking, managing, and accounting for ICT assets within the Ministry. CDOs are required to fill in this tool the Asset of their Ministries.

RISA has a system requiring all government institutions to register their ICT assets. This centralised system aims to create a comprehensive inventory of ICT assets across government entities.

Some individual Ministries have their own independent asset management systems or processes apart from the Ministry of Finance or RISA systems. These additional systems could cater to specific needs or provide supplementary tracking mechanisms for assets within those institutions.

The collaborative efforts between the CDO and Logistics Office of the Ministry highlight **the importance of a coordinated approach to asset management**. The goal is to maintain accurate records, streamline acquisition processes, ensure efficient maintenance, and manage proper disposal of IT assets across government institutions. An ITSM tool can be implemented to manage ICT assets and harmonise the practices in all government institutions.

Risk Management

IT risk refers to the likelihood of an unforeseen and unfavourable business outcome resulting from the exploitation of vulnerabilities within an information system by a specific threat or malicious actor. This risk spectrum encompasses scenarios such as human error, equipment malfunction, cyberattacks, and natural disasters.

The practice of IT risk management entails applying established risk management methodologies to address IT threats effectively. This process encompasses the use of procedures, policies, and tools to systematically identify and assess potential threats and vulnerabilities within the IT infrastructure.

For more details, users can refer to the IT Risk Management Guidelines that are published by RISA.

Below are some best practices in terms of IT Risk Management. There are some steps to deploy to perform good risk management.

Step 1: Formulate a robust risk management Strategy:

The initiation of effective risk management involves the identification and assessment of potential vulnerabilities within an IT environment. Examples of these vulnerabilities include weak system passwords, unpatched systems, and downloads of malicious software. However, the manual process of identification and assessment can be both costly and resource-intensive. To streamline this process, organisations are encouraged to utilise automated tools, such as help desk or service desk software, which come equipped with risk management capabilities. These tools automatically detect and assess risks, promptly alerting security teams to potential issues.

Step 2: Conduct ICT asset management:

To mitigate technology risks effectively, maintain a continuous vigil over IT assets, including routers and servers. Employ reliable asset life cycle management software for automated, centralised network inventory, offering comprehensive insights into asset performance, security, and licensing concerns. Utilise this software to continuously monitor software licence expiration dates and receive automated alerts.

Step 3: Enhance cybersecurity:

Establishing and sustaining a secure IT infrastructure is pivotal in preventing cybersecurity risks. Employ appropriate security tools, policies, and procedures to thwart various threats. In addition to traditional measures like firewalls and antivirus software, integrate advanced security tools such as security information and event management (SIEM) software to bolster security controls. SIEM software, being automated, maintains a detailed log of security events, correlating data for swift threat identification. It facilitates automated responses to security incidents, such as blocking IP addresses linked to unauthorized activities. Leverage built-in templates for generating security and compliance reports.

Step 4: Ensure transparent communication:

Develop robust internal and external communication strategies to convey risk details to relevant parties. Clear communication expedites a coordinated response against evident threats in the IT environment, aiding faster risk mitigation, assessment, and monitoring. When devising your risk communication and management Strategy, seek input from all key stakeholders to comprehend various aspects of a given risk, including affected parties, significant challenges, and potential recovery costs.

Step 5: Implement access control:

Mitigate data security risks by instituting stringent authentication and authorization procedures within your organisation. Modern access management software assists in ensuring that only authorised users access sensitive parts of the network, thereby minimising the risk of insider threats. These tools continuously monitor file system changes to detect unauthorised alterations and generate compliance reports detailing user permissions and activities. Utilise such tools to proactively track privileged users' accounts for unusual activities, enhancing preparedness against advanced threats.

By implementing a comprehensive risk management approach, sectors can better protect their ICT assets and systems from potential threats and vulnerabilities. Regular reviews and updates to the risk management plan ensure that it remains effective in addressing emerging risks.

Internal Audit

The approach to auditing within an IT environment differs based on whether the goal is a financial, performance, or IT audit. There are mainly three common approaches for running internal audits in best practices.

Approaches	Focus	Example
System-Oriented Approach	This approach concentrates on the examination of management systems to ensure their proper functioning	In financial management systems, auditors should assess the effectiveness and efficiency of financial controls, budgeting processes, and overall financial management practices
Result-Oriented Approach	This approach assesses whether the intended outcomes or outputs of programs and services have been achieved as planned	Auditors should evaluate the success of a government program by examining whether it has achieved its goals and produced the desired results. This could involve analysing performance indicators and comparing actual outcomes to planned objectives.
Problem-Oriented Approach	This approach involves examining, verifying, and analysing the causes of specific problems or deviations from established criteria	If there are discrepancies or issues identified in a particular area, such as a project not meeting deadlines or exceeding budgets, auditors using a problem-oriented approach would investigate the root causes of these problems

Table 2: Internal Audit approaches

Each approach serves a distinct purpose and may be chosen based on the specific objectives of the audit and the context in which it is conducted. Performance auditing aims to enhance transparency, accountability, and effectiveness in organisations by providing insights into how well systems and processes are functioning and whether desired outcomes are being achieved.

Audit always divided to four main steps:

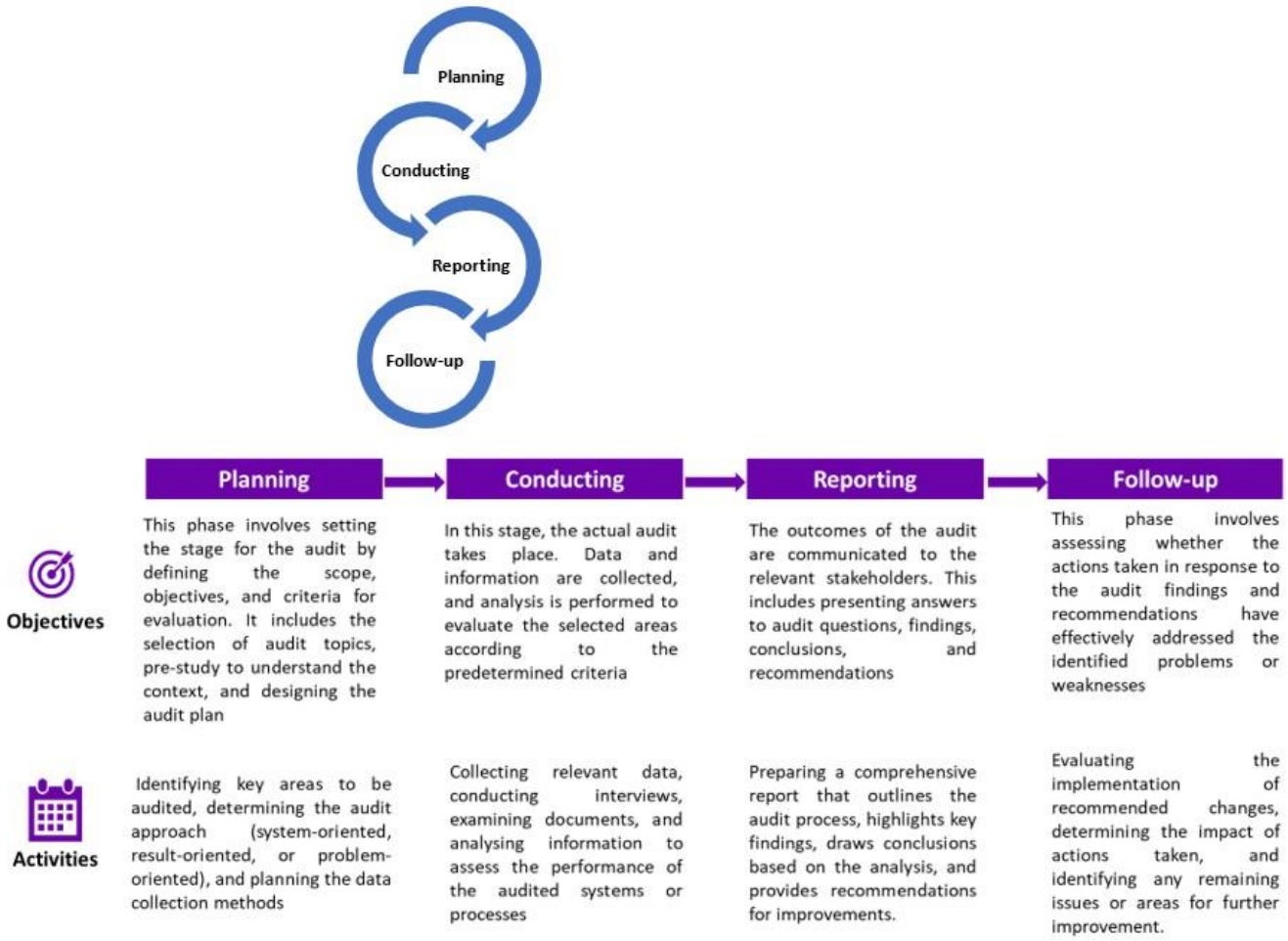

Figure 12: Detailed steps for an internal audit activity

The process is indeed iterative, as new insights gained during the conduct phase may lead to adjustments in the audit plan. Additionally, the reporting stage may involve ongoing discussions and feedback with stakeholders, and the follow-up process ensures that the audit's impact is sustained over time.

That said, it is worth checking the list of items to be audited by the CDO teams. The list provided below is the one used by external auditors for Audit procedure and should be followed by the sector IT structure. The categories of audit checklist are mentioned in the table below, and detailed audit questions are presented in the annex of this Handbook.

N	CONTROL	Content
A	**ACCESS CONTROL POLICY AND PROCEDURES**	Access control policy, procedures for account registration and follow-up, user access privileges reviewing, strong password enforcement, sessions automatically log off after a period, remote access limitations, authentication to access the network, risk assessment performed before allowing mobile devices on the organisation system...

B	**SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES**	Existence of information security awareness program at the organisation level, security training to all information system users
C	**AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES**	Auditable events clearly defined with an audit frequency and audits records
D	**SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES**	documented/shared Information security policy in place, periodic security assessment conducted and reports available, critical infrastructures and their protection plan in place
E	**CONFIGURATION MANAGEMENT POLICY AND PROCEDURES**	Baseline configuration of the information system as well as change management procedure existence, definition of a list of prohibited or restricted functions, ports, protocols and/ or services
F	**BUSINESS CONTINUITY PLANNING POLICY AND PROCEDURES**	Business continuity plan in place and periodically tested, periodic information backup to support the recovery time, back-up routine
G	**INCIDENT RESPONSE POLICY AND PROCEDURES**	appropriate incident handling procedures in place and known by all the staff
H	**SYSTEM MAINTENANCE POLICY AND PROCEDURES**	written standard for system maintenance, maintenance support process ensure confidentiality of information, maintenance services provided by licensed/certified people/firm
I	**MEDIA PROTECTION POLICY AND PROCEDURES**	electronic media disposal Policy, secure store for electronics and physical media within a physically secure or controlled area

J	**PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES**	physical access restricted to selected employees, control all items brought into or taken out of the computer/server room, sensitive application servers/ systems located in a physically restricted area
K	**PERSONNEL SECURITY POLICY AND PROCEDURES**	procedures address personnel screening and records of screened personnel, personnel termination/transfer; records of personnel termination/transfer actions
L	**SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES**	information security and information security risk management integrated into the system development life cycle, include and consider security requirements in acquisition contracts, use software in accordance with contract agreements and copyright laws?
M	**SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES**	separate application for users and managers/admin, mechanism to prevent unauthorised and unintended information transfer via shared system resources, information system that protects and prevents DoS, continuous monitoring Strategy and reporting of the security status of the information system
N	**SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES**	antivirus software and endpoint security installed in the systems, all staff been advised of the virus prevention procedures, centrally manage antivirus software and endpoint security, receiving security alerts, advisories, and directives from designated external institutions
O	**DISASTER RECOVERY**	contingency plan provide for recovery and extended processing of critical applications in the event of catastrophic disaster, recovery plans approved and regularly tested, disaster recovery teams established to support disaster recovery plan, responsibilities of individuals within disaster recovery team defined and time allocated for completion of their task, recovery plan ensure, in the event of failure that no loss of data received but not processed, no reprocessing of data already processed

Table 3: Internal Audit check

The above list is provided by RISA and is subject to change. Please refer to the Internal IT Audit Guidelines from RISA for the latest available checklist.

Financial Responsibilities

As a department head, the CDO has financial responsibilities. The Chief Digital Officer (CDO) carries significant financial responsibilities, including budget planning for the upcoming year.

Budgeting responsibilities:

In the process of defining the next year's budget in October of the previous year, the CDO needs to consider various aspects:

Budget Planning: Assessing the IT department's needs, including operational expenses, new projects, upgrades, software/hardware requirements, cybersecurity measures, staff training, and other relevant expenses.

Forecasting: Predicting and estimating the costs based on past expenses, expected growth, technological advancements, and any upcoming projects or initiatives.

Allocating Resources: Determining the allocation of financial resources to different areas within the IT department, prioritising strategic initiatives while also ensuring operational efficiency.

Regarding the budget submission and integration into the overall Ministry budget, there should be variations in how it's accounted for, depending on the Ministry’s organisation.

Some Ministries prefer a specific line item in the **budget dedicated solely to IT projects**. This delineates the funds explicitly allocated for IT operations, projects, and maintenance.

In other cases, the IT budget **should be integrated into a more general expense category**. This could include various administrative or operational costs beyond IT, making it part of the broader operational expenditure.

The decision to place the IT budget in a dedicated line or within general fees should depend on the organisational structure, accounting practices, and the Ministry's preferences for budget categorization.

The budgeting process depends on whether it is an ordinary budget (provided by MINECOFIN) or it is through the Development Partners.

Ordinary budget: from MINECOFIN

Figure 13: Budget planning procedure for government funding

In addition, CDOs plan how to spend the budget and report on how the budget is spent.

Via DPs

Figure 14: Budget planning procedure for DPs funding

**Either reimbursement against invoice or reimbursement after disbursement, or disbursement directly by the donor to the Ministry.*

Following the annual budget approval, the CDO oversees the implementation of IT projects' budget allocation. Occasionally, funds may need to be redirected to address urgent Ministry needs. In such instances, the CDO restructures IT project priorities to reallocate resources accordingly.

Additionally, the CDO holds the responsibility of greenlighting IT expenditures before payments are made to providers.

For as long as a project falls within the remit of its ministerial department, the CDO is responsible for planning, implementing and reporting on the use of funds.

Procurement and Vendor Management

Needs identification and procurement plan

Before any procurement activities take place, it's essential to have a clear plan in place. This plan outlines what needs to be purchased, when it needs to be acquired, and how it aligns with the organisation's goals and budget.

Before creating the procurement plan, there's a phase of identifying what exactly should be included in it. This involves a thorough assessment of the organisation's needs, considering factors such as operational requirements, budget constraints, and any regulatory or compliance considerations.

Reviewing and approving department purchases

The CDO and his/her team are responsible for ensuring that the Ministry or sector receives the necessary resources on time. This involves not only identifying the needs but also coordinating with vendors or suppliers to facilitate timely delivery and implementation.

The expenditures typically fall into two categories: development project budgets and operational budgets.

The development project budget encompasses expenses associated with project deployment. For instance, these could involve prototyping and Proof of Concept, consulting or Professional Services, Software Development, System Integration…

On the other hand, the operational budget includes expenses tied to the day-to-day functioning of the IT department. This incorporates purchases such as IT Consumables, Hardware and Software Maintenance, IT Security Expenses...

The national procurement laws and guidelines must be applied for managing the procurements.

It is incumbent upon CDOs to meticulously review and validate these expenses before they are processed for payment by the sector's financial department. This duty **necessitates the establishment of an expenses follow-up tool**. The tool will serve to compare budget consumption against the allocated budgeted amount, mitigating the risk of surpassing the budget limit by the end of the fiscal year. CDOs are advised to leverage tools already in place for budget management and expenses follow up.

By implementing an effective expense monitoring system, the CDO ensures prudent financial oversight, preventing potential over budget situations and maintaining financial discipline within the IT department. This meticulous approach not only ensures efficient resource allocation but also contributes to the overall fiscal health and strategic planning of the sector.

Management of Framework Contracts

RISA holds framework contracts that encompass a significant portion of the necessary purchases for CDOs across their respective sectors. RISA is in charge of negotiating and signing these framework contracts. However, consulting with the CDO and their teams before considering and negotiating each framework enhances decision-making and promotes alignment with public administrations needs and goals. It reflects a strategic approach to procurement and contract management that prioritises public administrations effectiveness.

CDOs are tasked with providing feedback to RISA regarding any purchases not covered within the existing frameworks.

This process mandates that when a CDO requires a purchase, the initial step involves reviewing RISA's framework contracts before exploring alternative procurement options. Should the specific need not be covered by an existing framework contract, it must be forwarded to RISA for approval, alongside the sector's management. Further details regarding this scenario will be outlined in the subsequent section titled "Negotiating contracts with vendors and service providers."

Framework contracts denote agreements directly negotiated between RISA and providers, possessing both commencement and expiration dates. Prior to the contract's expiration and the decision on renewal, CDOs are approached to provide feedback to RISA based on their prior experiences with the providers. This feedback is strongly encouraged and must be submitted to RISA on a quarterly basis as per compliance requirements.

Moreover, enhancing the management of framework contracts necessitates the incorporation of best practices in contract management. Some examples are listed below:

Satisfaction KPIs: Introducing KPIs specifically focused on satisfaction metrics allows for the quantification and assessment of customer contentment with the suppliers. These metrics should encompass feedback mechanisms, surveys, or ratings that gauge the satisfaction levels of CDOs and other stakeholders with suppliers' services. These KPIs must be about:

- **Satisfaction Levels**: Gauge the contentment of CDOs, teams, or sector employees with the supplier, considering aspects like responsiveness, support quality, and overall satisfaction.
- **Service Efficiency**: Evaluate the efficiency and effectiveness of the services rendered by the provider in meeting established goals and requirements.
- **Timeliness Comparison**: Measure the average service delivery time against market practices to assess whether the provider meets or exceeds industry benchmarks.
- **Innovation in Service**: Assess the provider's innovative approaches or unique solutions offered during service delivery, showcasing adaptability and progressive strategies.
- **Provider Availability**: Evaluate the provider's accessibility and availability for support or inquiries within specified working hours or agreed-upon schedules.
- **Response and Intervention Times**: Monitor the average time taken by the provider to respond to queries or issues raised and the time taken for intervention or problem resolution.
- **Emergency Service Quality**: Analyse the quality and effectiveness of the alternative solutions or temporary services provided in emergency situations, ensuring they meet

required standards and mitigate disruptions effectively.
- **Service after sales satisfaction**: It measures the degree to which CDOs are satisfied with the support, assistance, or resolution provided after they've received a service or a product from a supplier: quality of Support, Follow-Up Communication…

The process must involve **each CDO providing input or feedback** regarding the suppliers/service provider's performance through these designated KPIs. Once the CDOs have completed and submitted their assessments, RISA consolidates this data promptly. This allows for an ongoing compilation of Key Performance Indicators, enabling RISA to continuously monitor the service provider's performance throughout the contract duration.

RISA needs to establish a feedback template or portal to allow the CDO team to provide feedback on specific contracts. The establishment of a feedback template or portal for feedback on each contract by the CDO team is a proactive step towards enhancing communication, streamlining processes, improving contract evaluation, fostering continuous improvement, and promoting accountability in procurement and contract management practices.

By regularly **gathering and aggregating these KPIs, RISA gains timely insights into the supplier’s performance** at various stages of the contract. This proactive approach enables RISA to make more informed and well-grounded decisions, especially when approaching the contract's conclusion or when contemplating renewal or modifications to the existing agreement.

The prompt compilation and review of these KPIs empower RISA to assess the service provider's effectiveness, address any identified issues or areas for improvement, and make strategic decisions based on comprehensive data and evaluations provided by the CDOs.

There also must be **Service Level Agreements (SLAs)** in the contract signed with the suppliers. The implementation of SLAs establishes clear expectations between RISA and the service suppliers. These agreements outline agreed-upon response times, resolution deadlines, and quality benchmarks, ensuring that services align with predefined standards. RISA must be responsible for forcing suppliers to comply with these SLAs. In the event of non-compliance, penalties must be applied, up to and including termination of the service contract.

A framework for **monitoring and reporting performance against SLAs and satisfaction KPIs** should be put in place. Regular assessments and reports will provide insights into service delivery effectiveness, enabling continuous improvement and informed decision-making.

Ticketing Systems: A ticketing system will be introduced to manage and track service requests and issue resolution. This systematic approach ensures that every reported issue or service request is documented, assigned, and tracked through to resolution, promoting accountability and efficient service delivery.

Negotiating Contracts with vendors and service providers

As mentioned in the section on negotiating framework contracts, purchases not covered under the framework contract may entail direct negotiations between the CDO and suppliers. Nonetheless, adherence to the Rwandan Public Administration procurement procedure is mandatory for

guidance on the purchasing process. Please, refer to guidelines for acquisition and upgrade of IT systems.

Specifically, for CDOs, obtaining RISA's approval is essential before releasing the terms of references for any purchase. Moreover, when multiple approvals are granted and CDOs are poised to engage in vendor contract negotiations, it's crucial to implement recommended best practices.

Effective contract negotiation involves **strategic planning, communication, and a focus on achieving mutually beneficial outcomes**. Effective contract negotiation also involves a **balance of assertiveness and collaboration to achieve favourable outcomes for both parties**. Being **well-prepared**, **maintaining a constructive dialogue**, and **seeking mutually beneficial solutions** are crucial aspects of successful contract negotiations.

Here are some best practices:

Preparation is Key: Thoroughly research and understand all aspects of the contract, including terms, conditions, goals, and potential risks. Clarify your organisation's needs, priorities, and desired outcomes before negotiations begin.

Set Clear Objectives: Define clear and realistic objectives for the negotiation process. Establish what you aim to achieve, whether it's cost savings, service enhancements, or specific deliverables.

Build Collaborations: Foster a positive and collaborative collaboration with the other party. Focus on mutual respect, transparency, and open communication to create a conducive negotiation environment.

Understand Alternatives and Leverage: Know your alternatives and leverage points. Understand what alternatives exist if the negotiation doesn't yield the desired outcome and use these as negotiating leverage.

Flexibility and Creativity: Be flexible and open to creative solutions. Explore various options beyond just price, such as performance-based incentives or long-term partnerships that benefit both parties.

Listen Actively: Actively listen to the other party's concerns, needs, and perspectives. Understanding their goals can help identify areas of agreement and compromise.

Negotiate Incrementally: Break down the negotiation into smaller, manageable components. Negotiate each aspect separately, allowing for compromises and concessions on less critical points.

Be Patient and Respectful: Negotiations can take time, so exercise patience. Remain respectful and professional throughout the process, even during challenging discussions.

Document Agreements: Ensure all agreements, concessions, and terms discussed during negotiations are documented in writing. This helps prevent misunderstandings and serves as a reference for both parties.

Seek Legal Advice: Involve legal experts or contract specialists to review and provide guidance on the terms and conditions. They can ensure legal compliance and protect your organisation's interests.

Review and Follow-Up: Review the negotiated terms thoroughly before finalising. Ensure that both parties understand and agree on the finalised terms. Follow up with regular reviews to ensure compliance.

There also must be **Service Level Agreements (SLAs)** in the contract signed with the suppliers. The implementation of SLAs establishes clear expectations between the CDO and the service suppliers. These agreements outline agreed-upon response times, resolution deadlines, and quality benchmarks, ensuring that services align with predefined standards.

The CDO must define a framework for **monitoring and reporting performance against SLAs and satisfaction KPIs**. Regular assessments and reports will provide insights into service delivery effectiveness, enabling continuous improvement and informed decision-making.

Vendors Management

Successful vendor management allows key benefits. By effectively managing vendors, CDOs can foster strong partnerships, optimise performance, mitigate risks, and ensure that vendor collaborations contribute positively to overall business objectives. Some benefits are:

- Improve vendor selection
- Harness cost savings
- Speed up vendor onboarding
- Reduce the risk of supply chain disruption
- Strengthen supplier collaborations
- Negotiate better rates

Managing sector’ vendors involve several mandatory steps to ensure effective collaborations and optimal performance.

Vendor Onboarding: Streamline the onboarding process for new vendors. Provide necessary documentation, guidelines, and training to ensure they understand your sector's requirements and standards.

Establish Clear Expectations: Clearly communicate your sector's expectations regarding performance, quality, timelines, reporting, and communication channels.

Performance Monitoring: Implement Key Performance Indicators (KPIs) to measure vendor performance against agreed-upon benchmarks. Regularly monitor and evaluate their performance.

Regular Reviews and Meetings: Schedule periodic meetings and reviews with vendors to discuss performance, address any issues, provide feedback, and align strategies.

Communication Channels: Establish effective communication channels to facilitate ongoing dialogue, address concerns promptly, and maintain transparency.

Vendor and Third-Party Risk Management: Assess the cybersecurity measures of third-party vendors and contractors. Ensure that they comply with your department's security standards. Identify potential risks associated with vendors and develop risk mitigation strategies to manage disruptions or failures.

Compliance and Governance: Ensure vendors comply with legal, regulatory, and ethical standards. Implement governance frameworks to oversee adherence to contractual obligations.

Collaboration Building: Foster strong collaborations with vendors based on trust, collaboration, and mutual respect. Cultivate partnerships rather than transactional interactions.

Performance Improvement Plans: Collaborate with vendors to create improvement plans if performance falls short. Set achievable goals and monitor progress.

Exit Strategies: Have well-defined exit strategies in case a vendor collaboration needs to be terminated. Ensure a smooth transition to alternative suppliers without disrupting operations.

Incentives and Rewards: Offer incentives or rewards for outstanding performance to encourage vendors to exceed expectations.

Continuous Improvement: Continuously seek opportunities for improvement and innovation in vendor collaborations, processes, and outcomes.