IBRS | ANALYSIS INSIGHT JUDGEMENT

The CIO Handbook

Mastering the CIO Journey: From Novice to Sage in a Digital Age

Michael Mitchelmore

2023

Table of **Contents**

Executive Summary 2023

Enterprises that struggle with transitioning to modern digital frameworks share similar issues such as outdated systems and weak governance. This inhibits innovation, widening operational gaps that call for immediate action. The role of the CIO has never been as crucial as today in addressing these issues to identify and implement the right strategy for robust digital transformation.

As such, integrating technology, personnel, and methodologies is crucial. Their pivotal role ensures the organisation's future readiness in terms of trends, technologies, and market changes. This definitive guide offers CIOs the critical tools and insights that are imperative to lead their enterprises through best practices, skills optimisation and more aggressive innovation.

Through this handbook, IBRS offers an invaluable resource for CIOs to expand their role's impact and position their organisation in aligning technology initiatives with their business goals.

Document Objectives:

This handbook aims to provide CIOs the following:

1. ***Leadership and strategy alignment. Equip CIOs with an understanding of their multifaceted role, highlighting the importance of aligning technology with business strategy, fostering collaboration with stakeholders, and cultivating a balance between innovation and operational efficiency.***
2. ***Assessment and operational excellence. Provide CIOs with tools and guidelines to conduct comprehensive evaluations of the wider business and the ICT unit in their initial tenure, highlighting potential areas of improvement, risks, and strategies to optimise long-term ICT goals.***
3. ***Innovation and enterprise connection. Guide CIOs in developing a clear understanding of how ICT connects to enterprise functions, emphasising the role of innovation frameworks and the alignment of technology architecture with business objectives and market trends.***
4. ***Risk management and documentation. Prepare CIOs to proactively manage potential technological threats, emphasising the importance of comprehensive ICT documentation, business impact analysis, and recovery strategies, ensuring resilience in face of crises and threats.***

The Handbook:

- Guides CIOs in navigating multifaceted roles, ensuring alignment of ICT with business strategy, and fostering collaboration with stakeholders.
- Equips new CIOs with strategies for immediate impact, emphasising due diligence, efficiency optimisation, and innovation framework development.
- Advocates for comprehensive risk management, from conducting a business impact analysis for disaster recovery to proactive cyber threat mitigation and data integrity.
- Emphasises the significance of integrated ICT documentation and strategic procurement, encouraging simplicity in strategy formulation and regular review.

CIO Role at a Glance

The US Government identifies[1] that the CIO has six key responsibilities:

IT Leadership and Accountability: responsible and accountable for the effective implementation of IT management responsibilities.

IT Strategic Planning: responsible for strategic planning for all IT management functions.

IT Workforce: responsible for assessing agency IT workforce needs and developing strategies and plans for meeting those needs.

IT Budgeting: responsible for the processes for all annual and multi-year IT planning, programming, and budgeting decisions.

IT Investment Management: responsible for the processes for managing, evaluating, and assessing how well the agency is managing its IT resources.

Information Security and Privacy: responsible for establishing, implementing, and ensuring compliance with an agency-wide information security program.

In short, the CIO role and responsibilities are a challenging ask for anyone. The responsibilities above are aligned with the roles suggested by IBRS. What is missing in our view is the responsibility to manage up. Whether you have a seat at the senior leadership team (SLT) table or not, seek to understand what the SLT is looking to achieve, and keep the SLT informed on the ability of technology to assist these outcomes.

1. 'CIO Role at a Glance', U. S. Chief Information Officers' Council, 2018.

Chapter 1

CIO Responsibilities

Quick take

In this chapter, CIOs, especially those in the ANZ, India, and ASEAN market, will learn how to enhance their multifaceted roles in the organisation. Delving deep into sectors like technology, finance, and e-commerce, readers will discover strategies for innovation and operations, while ensuring technology aligns with business objectives. Through a blend of qualitative and quantitative insights, CIOs are equipped to foster robust collaborations with key stakeholders.

Chapter 1

CIO Responsibilities

To provide advice on how best to perform as a CIO, this handbook must first identify the roles and responsibilities of a nominal CIO position. IBRS suggests that a CIO role is multifaceted, and focused on four key business deliverables. These roles are:

- **Member of the Senior Leadership:** to operate as a member of the senior leadership team of the organisation, influencing strategy decisions on how best to deliver business outcomes.
- **Leading the ICT Business Unit:** to manage the ICT business, to ensure efficient and effective delivery of IT services.
- **Chief Innovation Officer:** to be an influencer for change, and drive innovation in both business and technology change and transformation programs.
- **Manage the ICT Business:** be an effective financial and human resource manager to maximise the productivity of the ICT business unit.

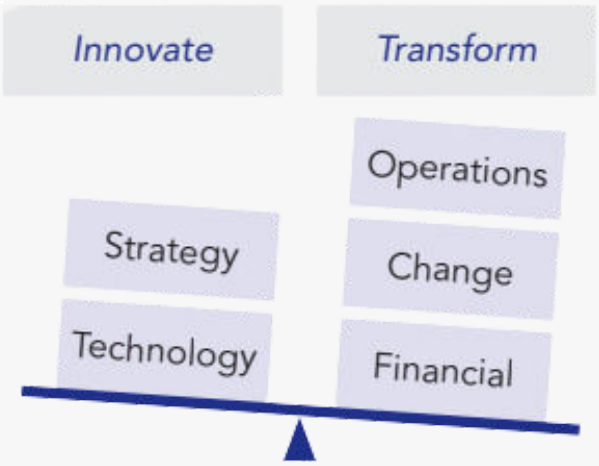


Diagram 1.1 CIO Balancing Act

The role of the CIO is therefore seen as a balancing act where the CIO must be able to innovate and transform the use of technology aligned to the business strategy. Gaining the best from technology, managing the operational delivery of ICT, whilst effectively managing change are being seen as a good financial manager.

Chapter 1

CIO Responsibilities

No one technology stream will provide the personal and professional development necessary to meet all challenges. As such, the CIO Handbook covers what the new CIO should do to deliver in the role. It will address the following:

- Situational awareness
- Alignment of business strategy and corporate plan
- Cost of operating ICT
- Technology – architecture, procurement, planning
- Critical business services underpinned by technology
- People and skills
- Driving innovation

Each advisory will address the CIO roles and responsibilities, and provide guidance to CIOs (new and experienced) on what they need to have in hand to do the job. This advisory covers what a newly appointed CIO in any organisation needs to quickly address. The focus here is the need to attain *situational awareness* of the qualitative and quantitative aspects of the environment within which you are now operating. Whilst many of the following points may seem to be motherhoods, not doing this homework will impact your ability to succeed, and ultimately the impact upon the businesses' success over time.

Qualitative

Investigate and read into:

- What is the business objective of the organisation? What is it the business is looking to achieve, and how are these outcomes currently delivered?
- Is the business subject to specific legislation, regulations, agreements, or policies that shape the approach to business?
- Who is who in the leadership team?
- Gain an understanding of the people and skills in your ICT team.
- Read the last two audit reports to determine priorities and risks that are already identified.

Chapter 1

CIO Responsibilities

Quantitative

Investigate and read into:

- What is the state of the business strategy, corporate plan, and any supporting plans like the technology plan, workforce plan, etc.?
- What are the current governance arrangements around ICT and innovation?
- What are the current pain points in the delivery of business and in the support of technology?
- What is the position of ICT documentation and processes?
- Is there a line of sight from the business strategy to the ICT architecture?
- What are the ICT KPIs and are they aligned to business criticality?
- Are the risks in delivery of ICT services defined?

The focus of your work in determining the situational awareness of the environment you are operating within is primarily business, rather than technology. This initial work will enable you to use empathy to gain the support of business colleagues and guide technology colleagues.

What's next?

Start by envisioning your communication and interaction dynamics with both the leadership and ICT teams. Then, pinpoint the misalignments between the business strategy and ICT's delivery capabilities. Based on these findings, identify the ICT's approach towards the top three risks that impact its success in supporting the business.

The next chapter will discuss how CIOs can conduct a thorough due diligence of both the wider business and the supporting ICT unit.

Chapter 2

Understanding **the Environment**

Quick take

This chapter discusses the transformative power of an intensive 90-day review. By learning how to dive deep into both business and ICT practices, identify inefficiencies, and craft robust action plans, you can effectively address associated risks, and areas for improvement within the ICT unit. This will also train CIOs to solidify their leadership position and set a clear path towards enhancing their leadership reputation and optimising the enterprise's long-term ICT goals.

Chapter 2

Understanding the Environment

The first 90 days is often spoken of as the period where the ability to affect change is most effective. To achieve effective change, the CIO needs to complete a due diligence process of both the business overall and the ICT business unit that supports it.

The due diligence checklist is designed to determine what is current practice and the risks associated with those practices. The key outcome is to determine where the ICT business unit is effectively supporting business, where efficiencies can improve effectiveness, and where waste and risk can quickly be addressed.

CIO Due Diligence Checklist

Item	What to Check	Why Check
Critical Business Function	Identify what critical business functions ICT supports and delivers.	To gain visibility of ICT from a business perspective.
Strategic Risks	Assess impact of ICT on the organisation's strategic risks.	To identify where ICT is best placed to innovate.
Organisation of the ICT Business Unit	Assess the organisational structure of the ICT business unit.	To understand the alignment of the ICT business unit org structure with support of critical business functions.

Understanding the Environment

CIO Due Diligence Checklist		
Item	**What to Check**	**Why Check**
ICT Business Unit CAPEX and Annual OPEX budget	Costs of ICT to business.	To identify potential areas where the budget may appear excessive or inadequate.
Organisations Annual Expenditure	Costs of running the business as a whole.	To identify potential areas where ICT investment may improve productivity or reduce costs.
SLA's, OLA's, and Underpinning Contracts	Review existence, tracking and suitability.	To understand if ICT is communicating its performance and value.
Technology and Digitisation	What technology choices have been made in recent times.	Identify any technology debt and effectiveness of digitisation approach.
Process Management i.e., ITIL, Procurement, Project Management, Recruitment	What processes are in place?	Identify the maturity of the ICT business unit and the business as a whole.
People (permanent)	What skills are permanent and are there any single person dependancies?	What skills are in place and what is missing?

Understanding the Environment

CIO Due Diligence Checklist

Item	What to Check	Why Check
People (labour hire)	What, why and at what cost does labour hire play a role?	Is the mix of labour hire and permanent employees acceptable? Is the ICT business unit paying a reasonable price?
Contingency Planning	BCP, DR, cyber response, major incident.	What is the readiness of the ICT business unit to address emergencies?
Governance	Where is oversight provided?	Are ICT risks and issues appropriately understood by the business?
Architecture, HLD Documentation, and SOPs	What documentation is in place?	To identify any key person risks where you are reliant on people to explain the reasons why.
Sourcing Model and Service Contracts	What is under contract, and at what cost?	How long has it been since the contracts were market tested – is the business paying a fair price for services?

Understanding the Environment

CIO Due Diligence Checklist		
Item	**What to Check**	**Why Check**
Software Assets	Software asset management register.	Does the ICT business unit have a list of software? At what cost, legacy versus future state, supportability, and security?
Hardware Asset	Assets stocktake.	Is it accurate, is it in line with strategy and architecture, what cost, legacy versus future state, supportability, and security?
Support Agreements	Second and third level support of the ICT environment.	Are they in place, necessary, what cost, is there effective mitigation of risk?

Chapter 2

Understanding **the Environment**

Once you have completed this due diligence, it is important that you quickly identify and document areas of concern, and develop an action plan and roadmap to rectify those areas of concern and reinforce those areas of merit. The first 90 days are a real opportunity to initiate actions that allow the CIO to shape the agenda. Where there is waste and risk associated with ongoing practices that have been allowed to operate in the shadows, the use of the due diligence checklist will provide the new CIO with data on which to base decisions.

In the experience of IBRS, many ICT business units have evolved over time and there will be many enclaves where people and providers have grown ineffective over time. CIOs who focus on the ineffective areas (and know why they are doing so) will quickly develop a reputation with their team for leadership, and with the business for getting things done. The focus is to deliver a more effective ICT business unit and reduce the risk (and costs) to the business in the longer term.

What's next?

Begin by completing the due diligence checklist immediately upon your appointment. If you're an existing CIO, let this checklist shape your forward-thinking. From there, transition into formulating your actionable strategy.

The next chapter will look into how CIOs can assess ICT costs, identify potential improvements, and recognise opportunities for innovation, all to drive efficiency and innovation using organisational documents.

Chapter 3

The CIO as Part of **Senior Leadership**

Quick take

This chapter expounds on how a CIO can use executive decisions effectively by immersing themselves in foundational organisational documents. Further, depending on the ICT's maturity, CIOs will discover strategies for either elevating its stature or leveraging it for innovation and risk management.

Chapter 3

The CIO as Part of Senior Leadership

In the first chapter, we looked at the balancing act the CIO must manage to undertake the four roles of a CIO, which are:

- To operate as a member of the senior leadership team of the organisation, influencing strategy decisions on how best to deliver business outcomes.
- To manage the ICT business, to ensure efficient and effective delivery of IT services.
- To be an influencer for change, and drive innovation in both business and technology change, and transformation programs.
- Be an effective financial and human resource manager to maximise the productivity of the ICT business unit.

This chapter will focus on how to ensure you can operate as an effective member of senior leadership and be an influencer for change. The key to this is to know the business, what are the critical deliverables the business must have in play to achieve its stated goals (in the case of government and not-for-profit), or its target outcomes (profit and loss in the case of commercial organisation).

Many CIOs come from technical backgrounds and do not always have a business focus. Technology is not an end in itself; the business which the IT underpins is the end state that must be the focus. If we take the case of a bank, many technical specialists will say the critical business function of an automatic teller machine is the software that it uses to operate. In business terms, the criticality is that it can dispense withdrawals of cash and allow for deposits. It is the business perspective that allows the CIO to better understand the impact of, and need for, innovation.

Chapter 3

The CIO as Part of Senior Leadership

Within the first week of appointment, the new CIO must undertake an exercise to achieve the best possible understanding of the critical business functions that the ICT underpins. As a minimum, find, read, and comprehend:

- Legislation that impacts the authority of or operation of the organisation.
- Charters or deeds that define the organisations' purpose.
- The organisation's last two annual reports.
- The organisation's strategic plan.
- The organisation's corporate plan.
- The organisation's annual budget, and to determine the:
  - ratios of expenditure across the organisation (HR, front office, ICT, etc.), and
  - the cost of operating the business and the cost of running ICT as a proportion.

With the documented understanding of the organisation's business focus, take the opportunity to speak with and visit the organisation's shopfront (whether that be a bank, an industrial complex, or a government office) to verify your understanding. Use the CIO Checklist provided in the Chapter 2 of this handbook to gain an understanding of the pain points and where ICT can either be improved, or where ICT can improve the business processes.

Once you have completed this assessment, you are now able to review your ICT internal documentation to better understand the critical elements of ICT that underpin the critical business functions of your organisation. To complete this step, you will need to understand the maturity of ICT in the organisation to both support and help innovate the business. You will need to seek out, read and review:

The CIO as Part of Senior Leadership

- The ICT architecture diagrams, standards, and principles used by the organisation to identify where shadow IT or legacy IT is in play.
- The high-level design(s) of the in-place architecture, to quantify how the infrastructure, data, and business applications are interdependent.
- The documented IT service management (ITSM) processes used, such as service desk, change, and service agreements.
- The documented approach to program and project management, and the current approved program of work.

Here lies a potential problem if the maturity of ICT is low. Many organisations, especially organisations with limited resources and highly outsourced approaches to ICT, will have low maturity. There may also be limited documentation to review and several single-person dependencies with whom this knowledge resides. Meaning the CIO will have to make risk-based judgements and potentially not be able to join all the dots. If this is the case, your first move as the new CIO is to put a program in place to improve the maturity of ICT in these areas to better support change and innovation for the business.

If the maturity of the ICT is high, then you can now make a sound judgement on where to focus your input to the executive and the senior leadership team on:

- The current risks associated with legacy ICT and/or unnecessary complexity of the architecture that will have the potential to impact the business outcomes.
- The risks to the business associated with data loss, – either because of a need to complete a disaster recovery or through a cyber incident.
- Where current business processes can be improved with:
  - innovation using ICT, or
  - where the current ICT platform can or should be improved.

Chapter 3

The CIO as Part of Senior Leadership

Once you have completed these discovery activities, you should then look to develop a technology reference model on what you have today from a technology lens and a high-level capability model from the business lens, based on your organisation's business critical functions. This will then allow you to quickly identify:

- What is critical from a functional perspective.
- The current technology solutions that underpin each function.
- Any duplicate capability delivering similar services to differing business streams.
- Legacy services and the risk they expose to the business.

Importantly, this process of discovery into critical business functions will also allow you as a new CIO to:

- better understand how the costs of ICT have evolved,
- how the cost benefit ratio for delivery of ICT can be improved,
- where the business may benefit from process re-engineering to use the existing technology more productively, and
- where opportunities may exist for innovation, to challenge the way the services and functions can be delivered differently.

Chapter 3

The CIO as Part of **Senior Leadership**

What's next?

To ensure technology effectively supports vital business functions, begin by modelling the technology that currently underpins the capability of the business. Through this analysis, identify gaps, duplications, legacy systems, and risks that could affect critical business operations. Finally, as you build on these insights, pinpoint areas where existing processes can benefit from more efficient technological applications and recognise opportunities where innovation could enhance productivity while simultaneously reducing risk.

The next chapter discusses the value of developing an innovation framework, ensuring transparency about innovation needs and technological trends.

Chapter 4

The CIO's Role in Innovation

Quick take

In this chapter, CIOs will discover the value of understanding their ICT environment together with the business goals it serves. By developing an innovation framework, enterprises can leverage transparency and its influence on aligning innovation with strategy. The CIO's unique position as a guiding force, rather than a proprietor of innovation, will be highlighted, emphasising their pivotal role in establishing an inclusive innovation environment.

Chapter 4

The CIO's Role in Innovation

This chapter will focus on the role of the CIO as an influencer for change, driver of innovation in both business and technology change, and transformation programs.

To quote Henry Ford:

> "If you always do what you've always done, you'll always get what you've always got."

The role of the CIO as the chief innovation officer is not to own innovation, but to guide it. In guiding the innovation practice of the business, the CIO will influence the SLT on the need to establish an innovation framework and processes that both allow the SLT to control the use of innovation, and allow input from every part of the business in identifying innovation opportunities.

To be an effective leader in innovation, a CIO must create an environment where innovation thrives. A CIO must sponsor innovation and create a mindset where:

- Within the business – moving ICT from an innovation limiter to an innovation enabler.
- Within ICT – moving from an innovation blocker to an innovation enhancer.

To this end, innovation cannot be something tacked onto an existing ICT strategy or technology plan; it must be embedded in the culture of the organisation. An effective chief innovation officer will be willing to challenge the status quo at every level, identify opportunities for innovation, assess the value proposition, and embrace innovation opportunities wherever the value proposition is real.

Chapter 4

The CIO's Role in Innovation

Not all innovation will be disruptive or radical. Innovation from within an organisation using technology will normally fall into the incremental or sustaining categories. Innovation in these areas should not be underestimated as it potentially can, at minimal cost to the business, generate substantial improvements in productivity and customer satisfaction.

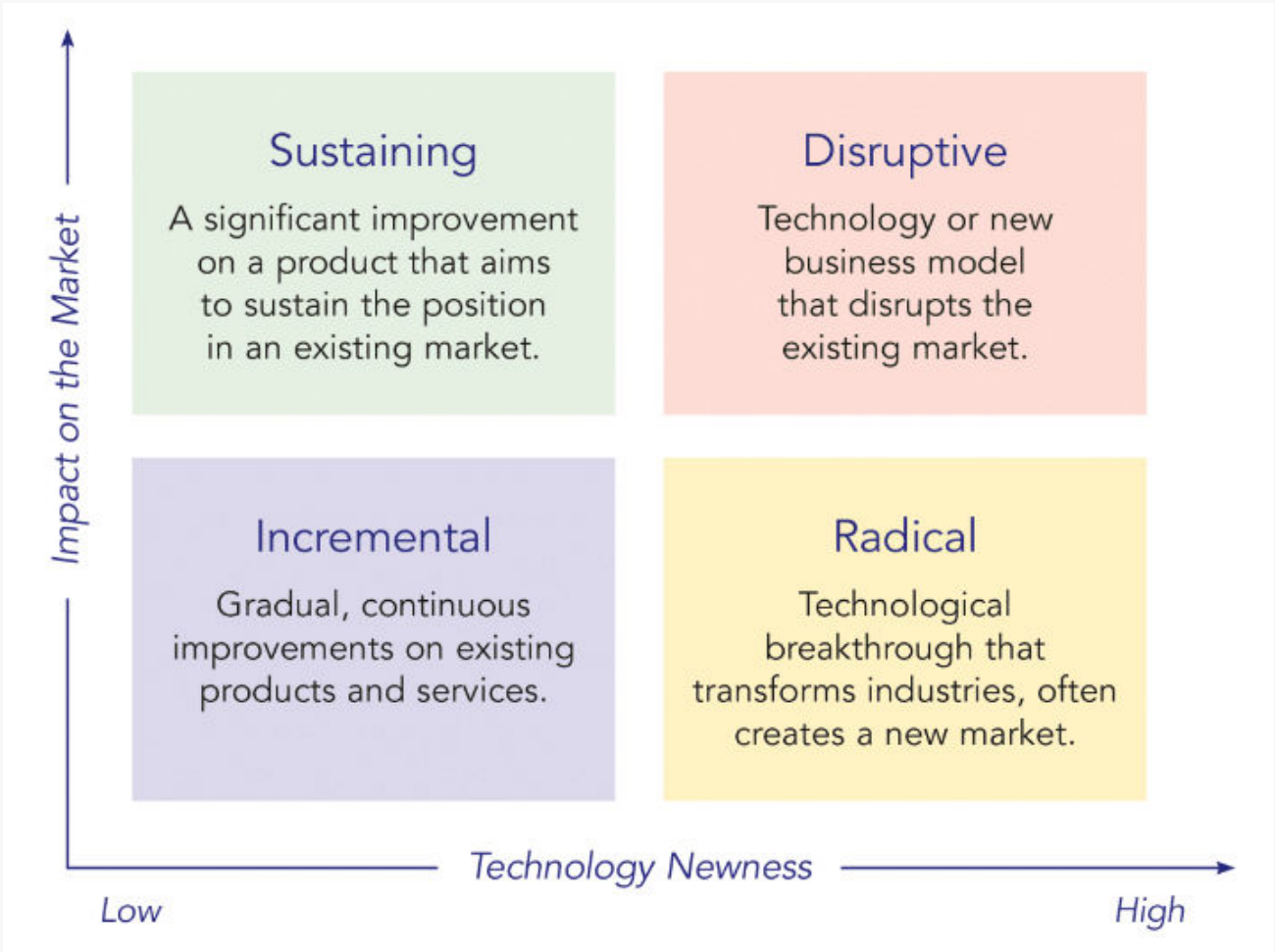


Diagram 4.1 Categories of Innovation

Chapter 4

The CIO's Role in Innovation

Significant value can be achieved where the CIO can lead adoption of radical and disruptive thinking resulting from developments in technology.

The first step in any innovation or change process is to understand the environment in which you operate. To achieve this, IBRS recommends CIOs enhance their situational awareness using the following four lenses to better understand the current state of ICT, your business focus, your people, and the art of the possible.

- **Current State ICT:** to understand the current state of your organisation's ICT environment, the CIO will have completed the due diligence checklist provided in Chapter 2.
- **Business Focus:** to understand the focus of the business, the CIO will need to be an effective member of the executive leadership.
- **People:** understanding your people is to trust their inclusion in the innovation practice. Use the knowledge of your internal teams and the customer community to better understand where innovation can deliver improvements.
- **Art of the Possible:** the CIO must be well-read and aware of not only the current trends in technology, but also the trends in technology being prosecuted by competitors. To do this effectively, the CIO should dedicate resources to reviewing and researching developments in technology, engaging with the strategic vendors of their organisation, and jointly building a technology hub to evaluate proof of concept exemplar projects.

Chapter 4
The CIO's Role in Innovation

Innovation Framework

IBRS recommends CIOs consider establishing an innovation framework based on the Deming continuous improvement cycle[2] where a preliminary step is introduced to develop an understanding of the current state. This allows the CIO to master the environment they are operating in, and think creatively on how that environment can be improved.

IBRS takes the view that to disrupt the organisation's status quo, you must understand the environment in which you need to innovate. Then, with this knowledge in mind, seek to identify the opportunities where innovative approaches will succeed. Then challenge the status quo through the development of exemplary projects to prove the value of innovation. Once proven, manage the transition program to transform the business and the ICT that supports it.

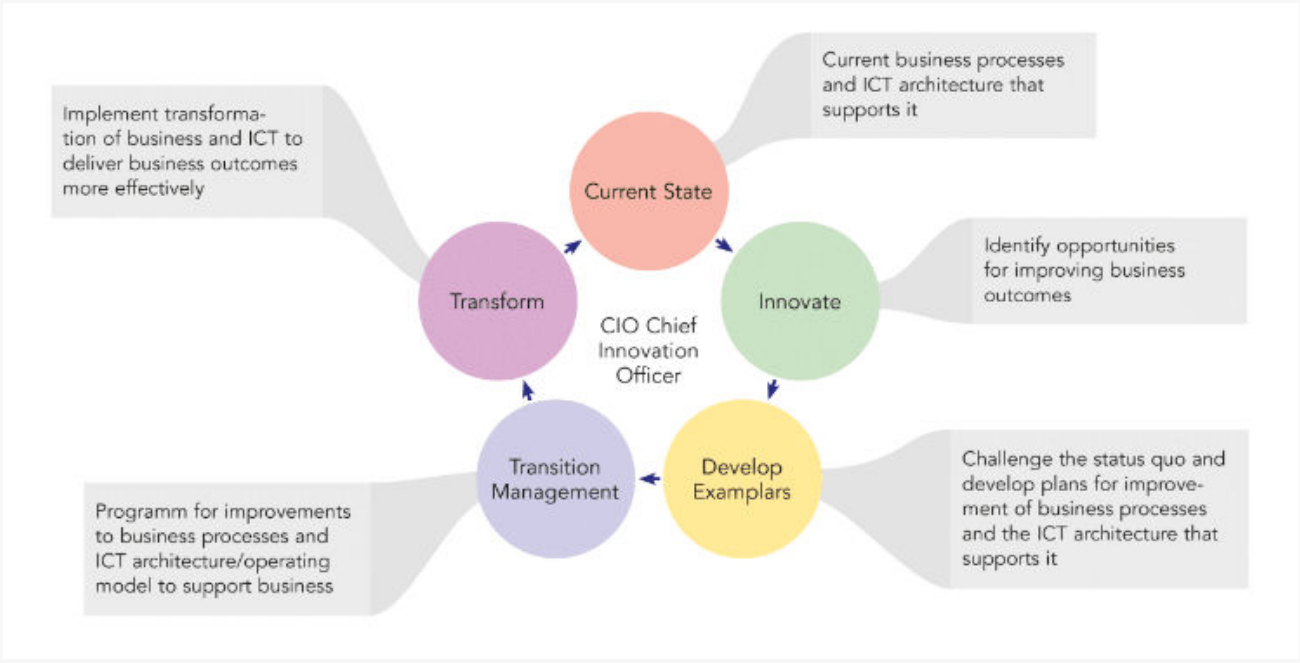


Diagram 4.2 Innovation Framework

2.'The PDSA Cycle, (Plan-Do-Study-Act)', The W. Edwards Deming Institute, 2022.

Chapter 4

The CIO's Role in Innovation

Innovation Practice

Underpinning the framework is the need to develop an innovation practice within the business processes in the same way [2]that risk and audit processes function. The CIO needs to seek wide acceptance within the SLT that real benefits will flow from applying innovative practices.

Innovation just like other practices in business needs to become normalised. IBRS recommends the CIO guide innovation through the development of innovation practice in their organisation. One way to do this is to ensure the innovation practice is established from the bottom up and from the top down. IBRS recommends the CIO should encourage the establishment of an innovation committee, to oversee innovation for the organisation, that reports to the senior leadership, providing proposals for their consideration and approval.

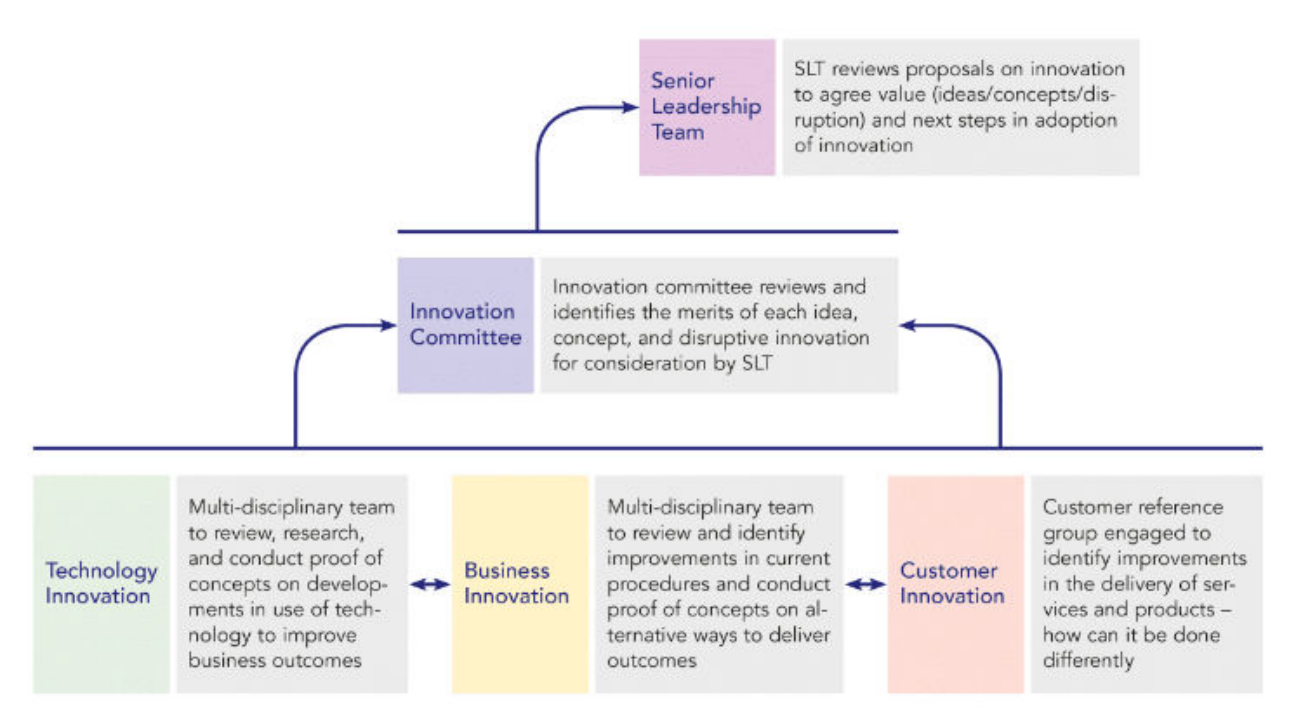


Diagram 4.3 Innovation Practice Framework

Chapter 4

The CIO's Role in Innovation

The innovation committee and SLT represent the business ownership level of innovation. This level in turn needs to be supported by a technical innovation body, a business innovation body, and a customer innovation body. These bodies will be tasked to assess where innovation in each category of incremental, sustaining, radical, and disruptive innovation can be employed to improve productivity and the customer experience.

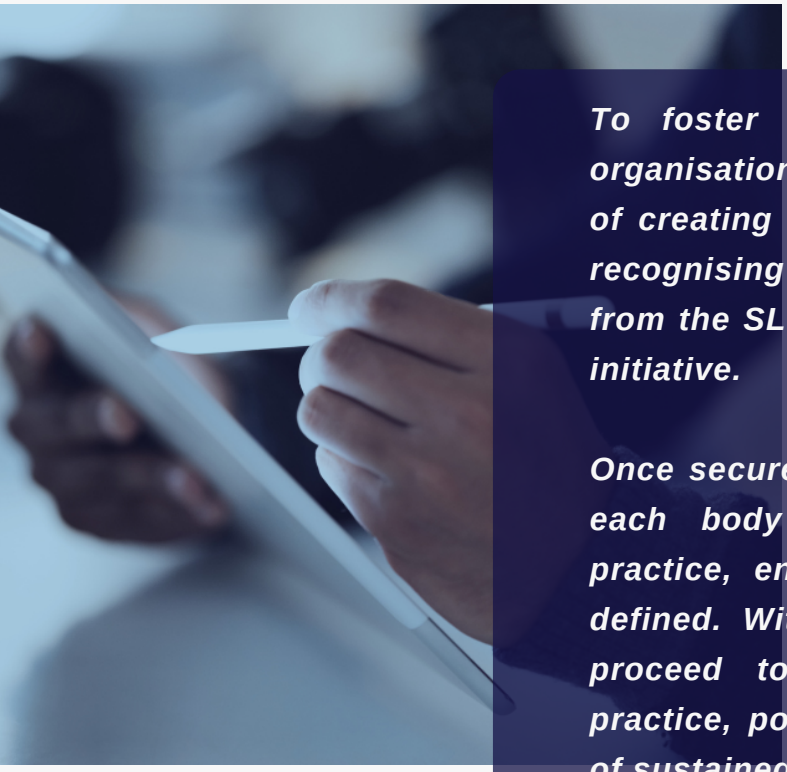
To establish an innovation practice, IBRS recommends that the CIO:

- Establish an innovation committee, akin to a risk and audit committee, tasked to review innovative proposals for SLT consideration.
- Establish a customer reference group to assist the organisation in seeing the services and products the organisation delivers from the customer lens.
- Advertise internally that the organisation has established an innovation practice and is open to considering innovative ideas to improve productivity of the organisation, and customer satisfaction.
- Establish multidisciplinary teams to assess opportunities for innovation (MDTI), such as:
    - **Technology MDTI:** led by the office of the CIO with members from ICT architecture, ICT operations teams, ICT contract and vendor management team, and a representative from the office of the chief operations officer (COO).
    - **Business MDTI:** led by the office of the COO, with members from each business unit, HR, finance, marketing, and a representative from the office of the CIO.
- Establish a working group within the technology MDTI to research and seek from vendors the potential opportunities new technology in development offers to the organisation.
- Develop an innovation hub where exemplar proof of concepts are assessed.

Chapter 4

The CIO's Role in Innovation

What's next?



To foster a culture of innovation within the organisation, start by assessing the potential value of creating a dedicated innovation practice. Upon recognising its significance, seek endorsement from the SLT to underscore the importance of this initiative.

Once secured, draft a clear terms of reference for each body within the prospective innovation practice, ensuring roles and responsibilities are defined. With these foundational steps in place, proceed to formally establish the innovation practice, positioning the organisation for a future of sustained growth and ingenuity.

The next chapter elaborates on why conducting a business impact analysis (BIA) can support CIOs in assessing potential consequences of total technology service loss and identify critical business processes and recovery needs.

Chapter 5

Business Impact Analysis

Quick take

This chapter discusses why most organisations often overlook supporting critical enterprise functions. It then introduces business impact analysis (BIA) as a solution to secure the enterprise from the effects of digital service disruptions. Through this, the enterprise can better align ICT with organisational imperatives, ensuring business continuity, and making informed, data-backed decisions even in crisis situations.

Chapter 5

Business Impact Analysis

How does each business unit respond to a total loss of services? Often, businesses will expect ICT to just work. It is important that the impact of a catastrophe is discussed with (each business unit/the business/ businesses). Any discussion must emphasise that ICT is not solely responsible for the issue. In terms of business resistance, there are several questions that need to be considered by the CIO:

- How does each business unit respond to a total loss of services?
- What is the possible impact on service?
- What are the knock-on effects to business reputation?
- What are the financial impacts in terms of lost revenue and the cost of providing limited services?

Understanding and agreeing on the business impact in the event of a catastrophic failure will allow CIO's to manage priority of restoration, and allow business units to better structure their plans while the ICT issues are resolved.

The BIA should address three critical areas:

1. **Determine Business Processes and Recovery Criticality:** business processes supported by the ICT system are identified, and the impact of a system disruption to those processes is determined, along with outage impacts and estimated downtime. The downtime should reflect the maximum that an organisation can tolerate while still maintaining the service. To achieve this, business areas should be asked to identify the duration of time that an outage can be tolerated through the use of a template. IBRS suggests the following template (Figure 5.1) be considered for use by CIOs. It is an example of a template which has been effective when used by an IBRS client. This process can then be used to score applications and services with a numerical value based on the responses, to determine the criticality and priority for restoration.

Business Impact Analysis

2.**Identify Resource Requirements:** realistic recovery efforts require a thorough evaluation of the resources required to resume business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records. The ICT area will need to develop planning for disaster recovery and cyber incident response for business executive approval based on the BIA.

3.**Identify Recovery Priorities for System Resources:** based on the results from the previous analysis, system resources can be more-clearly linked to critical business processes. Priority levels can then be established for sequencing recovery activities and resources. It is important to also assess the investments necessary to meet the identified BIA should the existing architecture be found inadequate.

Business Impact Analysis

Figure 5.1. Business Impact Analysis Matrix (BIA – Inherent Risk)				
Business Application or Service Title:				
Application/Service description:				
Associated or linked systems:				
Please indicate your assessed Impact by copying tick into appropriate box				√
Impact to Business 1 day or less	**Low**	**Medium**	**High**	**Very High**
Loss of public confidence				
Ability to conduct Business activity with clients				
Internal impact to staff				

Business Impact Analysis

Loss of Revenue (values are examples only)	$0-10k	$10-250k	$250k-1m	>$1m
Contravenes legislation				
Reason/Explanation for assessed impact: *Public facing; Revenue loss; Staff impact; Legislation; Other*				
Impact to Business 2-5 days	**Low**	**Medium**	**High**	**Very High**
Loss of public confidence				
Ability to conduct Business activity with clients				
Internal impact to staff				
Loss of Revenue	$0-10k	$10-250k	$250k-1m	>$1m
Contravenes legislation				

Business Impact Analysis

Reason/Explanation for assessed impact: *Public facing; Revenue loss; Staff impact; Legislation; Other*				
Impact to Business >5 days	**Low**	**Medium**	**High**	**Very High**
Loss of public confidence				
Ability to conduct Business activity with clients				
Internal impact to staff				
Loss of Revenue	$0-10k	$10-250k	$250k-1m	>$1m
Contravenes legislation				
Reason/Explanation for assessed impact: *Public facing; Revenue loss; Staff impact; Legislation; Other*				

Chapter 5

Business Impact Analysis

Descriptors for Loss of System or Application	
Very High Risk and Impact	Very damaging to the business, significant loss of public confidence, high loss of revenue, contravenes legislation. Needs to be restored urgently.
High Risk and Impact	Damaging to the business, likely loss of public confidence, loss of revenue, may not contravene legislation. Needs to be restored quickly.
Medium Risk and Impact	Some damage likely to the business, may have loss of public confidence, may result in loss of revenue. Manageable for a period by other routine procedures and controls.
Low Risk and Impact	Very limited damage to the business, no real loss of public confidence, no loss of revenue. Manageable by other routine procedures and controls.

By completing a thorough BIA process, the CIO will be able to justify, using data-driven decision-making, the suitability of the ICT architecture to support the business. The BIA process will provide business and ICT with a line of sight between business priorities, business continuity planning, and any underpinning plans for disaster recovery or cyber incident response.

Chapter 5

Business Impact Analysis

What's next?

To enhance the resilience and preparedness of your business, begin by conducting a BIA process. Building on the insights derived from this assessment, review and refine both disaster recovery and cyber incident response plans to ensure alignment with identified priorities. Subsequently, test these plans for efficacy against the set benchmarks. Concluding this process, evaluate any necessary investments to ensure the business's availability and survivability needs are met.

The next chapter delves into the reasons why enterprises need to align procurement governance to meet current and future enterprise requirements.

Chapter 6

How To Manage Procurement **Strategically**

Quick take

In this chapter, CIOs will deep dive into the process of aligning procurement governance with the evolving needs of the enterprise. Highlighting the significance of a strategic approach, it will explore the interplay of business, architecture, infrastructure, and contracts in procurement decisions. Through this, CIOs will gain insights into developing a forward-looking three-year procurement plan, laying the foundation for timely and impactful technology acquisitions.

Chapter 6

How To Manage Procurement **Strategically**

To complete procurement with a strategic focus, those in charge of the ICT acquisition processes need to understand and manage the factors that impact procurement, not just the planning and processes for each procurement. IBRS has identified four key factors that impact procurement:

- **Business Change:** driven by strategies for business, new capabilities, and/or increased market share.
- **Architecture Change**: where existing capabilities can be improved through the implementation of new or innovative technical solutions to support critical business functions.
- **Infrastructure Change**: to maintain existing platforms through replacement of like capability to meet performance and support requirements.
- **Contracted Services**: where contracted services are ending and require market testing to extend or replace the services provided.

To effectively manage these factors, IBRS recommends that the organisation's ICT strategy governance committee (or like committee/body) be required to review the output from the business controls to manage each of these procurement factors. These business controls are depicted in the diagram below, and require ICT to conduct analysis of each factor, prioritise, and align each procurement to meet the business need over a three-year rolling program, align the budget requirements, and present the acquisition plan for endorsement to the ICT strategy committee. Only those procurements endorsed by the ICT governance committee can then progress through the procurement processes to develop and conduct a test of the market to acquire the capability.

Chapter 6

How To Manage Procurement **Strategically**

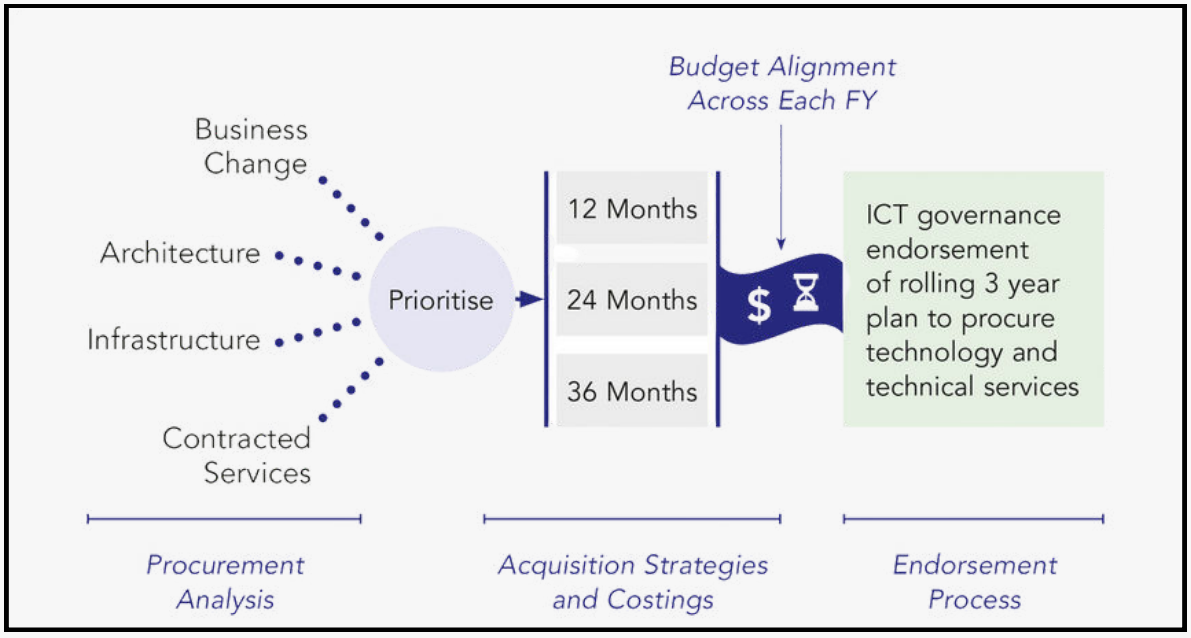


Diagram 6.1 Strategic Procurement Framework

Strategic Procurement Factors

Many organisations either have a dedicated procurement team or an office of the CIO designed to support the CIO decision processes. IBRS recommends that the procurement team or office of the CIO be designated to oversee and manage processes. The relevant body should coordinate input from the procurement factors to allow the body to prioritise procurement across a three-year acquisition plan.

Chapter 6

How To Manage Procurement **Strategically**

Business Change

To manage the procurements against the business change factor, ICT must align the business and ICT strategies. In doing so, ICT should develop a map of current technology to support existing business functions, and identify new acquisitions necessary to support proposed business functions. IBRS recommends the organisation's project/programme management offices (PMO) be tasked to develop the list of procurements needed to meet the business strategy, identifying likely options for procurement, and rough order of magnitude (RoM) cost.

Table 6.1. Example of New Capability Procurement

Technology Component	Tech	Required	Asset Value	Operations and Support	Time to Implement	Lead to Procure	Priority
e.g., Online marketplace	App CRM ERP	2025	$XX	e.g., Inhouse or outsourced	12 months	12 months	High

How To Manage Procurement **Strategically**

Architecture Change

The organisation's ICT architectural review board (ARB) and design authority should be charged to regularly review the technology solutions used to support critical business functions. With knowledge of current technology, end of supportable life, and new technology options, the ARB can advise on potential procurements where innovative options exist to replace current architectural solutions. These procurements should, where possible, be timed to be implemented at the end of supported life of the existing architecture, unless the potential gain in productivity is such that an earlier procurement can be justified. An example of the possible information to be collected is in Table 6.2 below.

Table 6.2. Example Architecture Procurement Register

Infrastructure Component Innovation	Innovation Solution	Replace	LoT	Est Cost	Benefit	Time to Replace	Lead to Procure	Priority
e.g., Network	SDLAN SDWAN	Hardware based Solution	5 Yrs	$XX	Agility	12 months	12 months	High

Chapter 6

How To Manage Procurement **Strategically**

Infrastructure

Hardware and software holdings will, by their nature, have a set lifespan, where a procurement is necessary to either upgrade or replace the technology. The operations team of the ICT group should be tasked to maintain a register of ICT infrastructure and when potential procurements should be considered for prioritisation into the rolling, three-year, acquisition planning process. IBRS recommends the register should, at a minimum, hold the following example information:

Table 6.3. Example Infrastructure Procurement Register

Infrastructure Component	Vendor	Procured	Asset Value	LoT	Ver.	Support	Time to Replace	Lead to Procure	Priority
e.g., Network LAN	Cisco	2020	$XX	5 Yrs	12.1	Support contract and cost	12 months	12 months	High

The operations team of the ICT group should be tasked to provide a revised list to the office of the CIO or the procurement office for the above information (table 6.3) for each component of the technology stack listed in the asset register. This will allow the effective prioritisation of procurements relative to existing replacements, against procurements for new capability, and those procurements where innovation may replace or improve existing technology solutions.

Chapter 6

How To Manage Procurement Strategically

Contracted Services

The procurement team of the CIO group should be charged to maintain a register of existing contracts for provision of technology services, to allow for effective planning and prioritisation of procurement decisions. The procurement office should be tasked to maintain the register of every contracted service as follows:

Table 6.4. Example Contract Services Procurement Register

Infrastructure Component	Vendor	Procured	Asset Value	Term	Time to Replace	Lead to Procure	Comments	Priority
E.g., Office 365	MS	2020	$XX	5 Yrs	3 months	12 months	E.g., SaaS with iRAP	High

Priority

The office of the CIO, or a designated element of the procurement office of your organisation, should be charged to collate the registers from the PMO, ARB, Ops team, and procurement team, such that on a quarterly basis they are to determine a rough order of priority for consideration by the ICT executive.

Chapter 6

How To Manage Procurement **Strategically**

Acquisition Strategy and Budgeting

Once priorities have been assigned, the office of the CIO, or the designated office of the procurement team, should then develop a high level acquisition strategy across a rolling, three-year plan, detailing the following

Table 6.5. Example Procurement Priority Register

Procureement	Source	Start	RoM Cost	Lead to Procure	Priority	Budget	Comments
e.g., Online Marketplace	Bus Strategy	2023	$XX	12 months	High	Yes	Required to meet business strategic outcome.
e.g., SDLAN SDWAN	ARB	2023	$XX		High	TBC	Replace end of life hardware. Will provide greater agility for business.
e.g., Office 365	Contracts	2024	$XX		High	Yes	Office automation and collaboration.

Chapter 6

How To Manage Procurement **Strategically**

Endorsement

IBRS recommends that the procurement priority register detailing the three-year, rolling procurement program be reviewed and endorsed on a quarterly basis. This will allow for the ICT executive to share with the broader business executive the key aspects of the ICT procurement plan, allowing for a strategic approach to ICT acquisitions.

What's next?

To ensure a cohesive procurement process, start by setting out a terms of reference that specifies controls for individual teams to handle each procurement element. Following this, for a more centralised approach, establish terms of reference detailing controls for the central authority to systematically collate and prioritise ICT acquisitions. Building on these foundational steps, it's essential to introduce a consistent agenda item for the ICT strategy committee, enabling them to regularly review and approve the rolling three-year ICT acquisition plan.

The next chapter teaches CIOs how to develop an ICT strategy framework that encompasses all business outcomes, communication plans, and governance structures.

Chapter 7

How To Develop An **ICT Strategy**

Quick take

This chapter introduces CIOs to the process of developing an impactful ICT strategy that aligns with broader enterprise goals. Through the lens of the 'keep it simple' principle, enterprise leaders can build the foundational elements of strategy formulation, from understanding business requirements to setting clear success benchmarks. Along these, the vital role of governance and the importance of periodic strategy reassessments will be discussed.

Chapter 7

How To Develop An ICT Strategy

The KIS (keep it simple) principle applies to strategy development. Your strategy must be easy to communicate and understandable to your target audience. The KIS principle applies throughout strategy – it must be easy to communicate by ICT, to be easily understood by its target audience, and to be easy to develop and implement. The strategy tree example below identifies four simple steps in the development of a strategy for business.

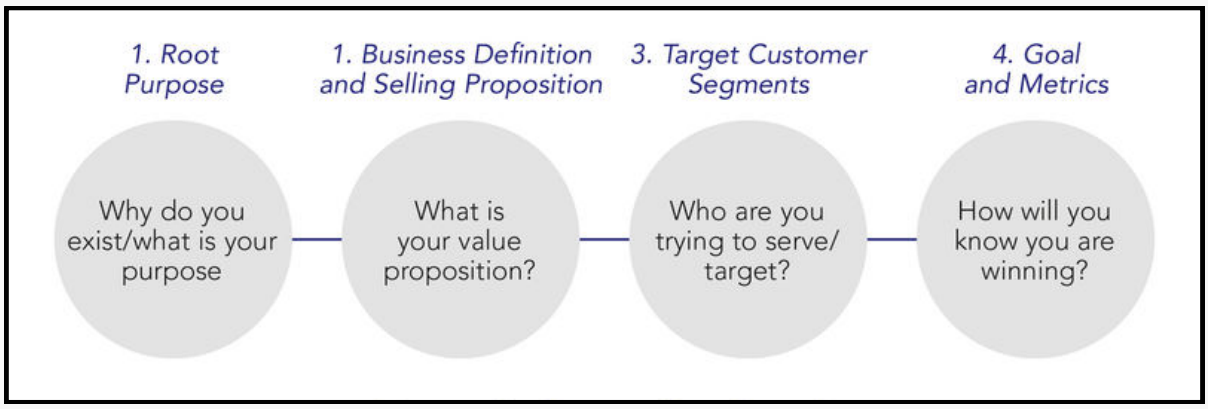


Diagram 7.1 Strategy Tree Example

In developing an ICT strategy framework from the strategy tree, the first step is the alignment of ICT to the business outcomes. CIOs can then use the IBRS strategy framework to develop the organisation's ICT vision, mission and ICT strategic plan. The IBRS strategy framework can also be used to determine the ICT approach to major change initiatives such as digital transformation, how best to adopt Cloud, or innovation in the use of ICT that drives organisational change to existing business processes.

Chapter 7
How To Develop An ICT Strategy

The development of an ICT strategy needs to be comprehensive. IBRS recommends that in developing your ICT strategy(s), you follow these six steps of the IBRS strategy framework:

1. **Analysis of the Business Needs:** identify the key aspects of the business strategy and business model the ICT strategy is required to underpin.
2. **Strategic Intent:** identify and agree on the intent of the strategy, including any known limitations or exclusions.
3. **Analysis of Technology Capability Against Need:** identify the current gap in technology capability against the future business model.
4. **Analysis of the Opportunities and/or Disruptors:** identify the potential for change that will deliver a business multiplier.
5. **Vision Horizon:** clearly articulate the outcomes of the strategy in terms of what and by when.
6. **What Needs to Happen:** identify the objectives the strategy will require to deliver and how success will be measured.

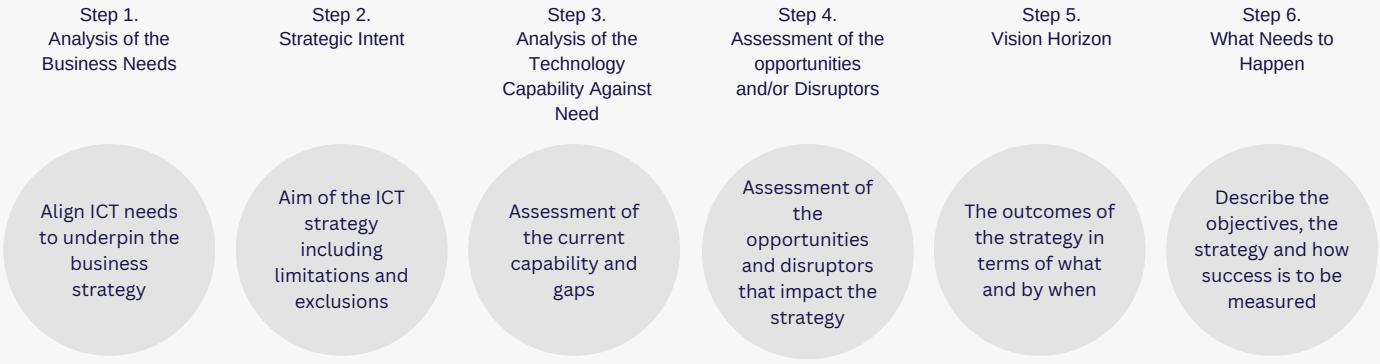


Diagram 7.2 IBRS Strategy Framework

Chapter 7

How To Develop An ICT Strategy

This planning process in the development of your ICT strategy will drive your organisation to leverage technology to best support the business strategy. But it is useful in other situations, too. The framework can be applied to strategies that support innovation or major change programs within the business.

Presentation of strategies can be: a plan on a page1, a PowerPoint pack, or in the form of a document. How it is presented will depend on your organisation's approach. It may be a good idea to touch base with the management team to confirm the form strategy presentations should take. If your organisation is one that uses a plan on a page, then the plan on a page can be the executive summary.

Whether the strategy is presented in document or PowerPoint form, IBRS suggests that a template for the structure of your strategy be as follows:

- **Executive Summary:** a plan on a page approach may be useful as the executive summary.
- **Introduction:** the introduction should explain the purpose and authority of the strategy.
- **Strategic Context:** the context is the positioning of the strategy. What are the enablers such as the business strategy objectives the strategy addresses or the disruptors/innovation it is planned to address?
- **Strategic Intent:** a clear and concise articulation of what the strategy is designed to achieve.
- **SWOT Analysis:** analysis of the approach demonstrating strengths, weaknesses, opportunities, and threats impacting the delivery of the strategy.

Chapter 7

How To Develop An ICT Strategy

- **Principles:** fundamental concepts that drive business alignment.
- **Standards:** rules for implementation of the strategy.
- **Strategy Implementation Approach:** describe each of the strategy's objectives and how each objective will be measured.
- **Governance:** description of how the strategy will be controlled.
- **Skills and Capability:** people skills and capability uplift needed to achieve the objectives of the strategy.
- **Roadmap:** high level timeline for implementation of the strategy.
- **Next Steps:** the next steps to authorise and enact the strategy.

The last two dot points can be outside the strategy document itself. Keeping them out can align to making the strategy a persistent document.

Governance

Finally, no strategy can be set and forgotten. The governance of the strategy must include regular reviews of progress and assessment of success. IBRS recommends that the best timeline horizon for an ICT strategy is three years. As a minimum, a strategy review should be set for 18 months, preferably annually, ahead of budget development, to assist in the preparation of each budget cycle.

Chapter 7

How To Develop An **ICT Strategy**

What's next?

To align stakeholders' understanding of ICT with the business strategy, leverage both internal expertise and external validation. As you craft the strategy to empower ICT to support and transform the enterprise, solicit feedback through internal and external pencil reviews of preliminary drafts.

The next chapter reveals the process of making CIOs both proactive and reactive in ensuring data integrity due to the rising cyber threats.

Chapter 8

Steps to **Data Integrity**

Quick take

This chapter looks into how CIOs can ensure data integrity amidst rising cyber threats. It will cover the importance of preventative measures, data categorisation, understanding the digital ecosystem, and developing a comprehensive recovery plan for potential breaches.

Chapter 8

Steps to Data Integrity

To best prepare for a cyber incident, IBRS recommends undertaking a two-step process to both:

- mitigate the impact of a cyber incident, and
- to then effect the recovery from a cyber incident.

When we look at data, it is often seen as a consolidation of all data. From the lens of the attacker, data has varying levels of value. If the purpose of the attack is reputation-based or denial of service, such as would be the case for a state actor, then their target will be different to that if your organisation has been selected to effect a more honest motive – to gain a profit.

To better assess how you should protect (read assure) your data integrity, organisations should look to categorise their data against four criteria of public safety (e. g., identity data), public security (e. g., transaction data such as banking details), public service (e. g., operational data supporting provision of services not addressed in safety or security), and administration (e. g., administrative records) to better understand how data should be protected.

Chapter 8

Steps to Data Integrity

Mitigation

In terms of mitigation, IBRS suggests organisations look at the following aspects against the lens of people, process, and technology to ensure the physical, personnel, and technical security around the management of data. Two primary themes of this step are:

- Effective oversight of the threat – responsive to executive governance:
  - Monitoring
  - Testing and validation
  - Skills and awareness training
- Defence in Depth:
  - Essential 8
  - Ready reaction plans (disaster recovery plan (DRP), cyber incident response plan (CIRP))
  - Immutable data storage in line with business impact analysis (BIA)
  - Encryption of data

When looking at data encryption (diagram 8.1) organisations must do so for each stage of the data life cycle, and for each type of data. The trade-off of security against performance need not always be a technical security issue. You should consider the strength of personnel security and physical security as well.

Chapter 8

Steps to Data Integrity

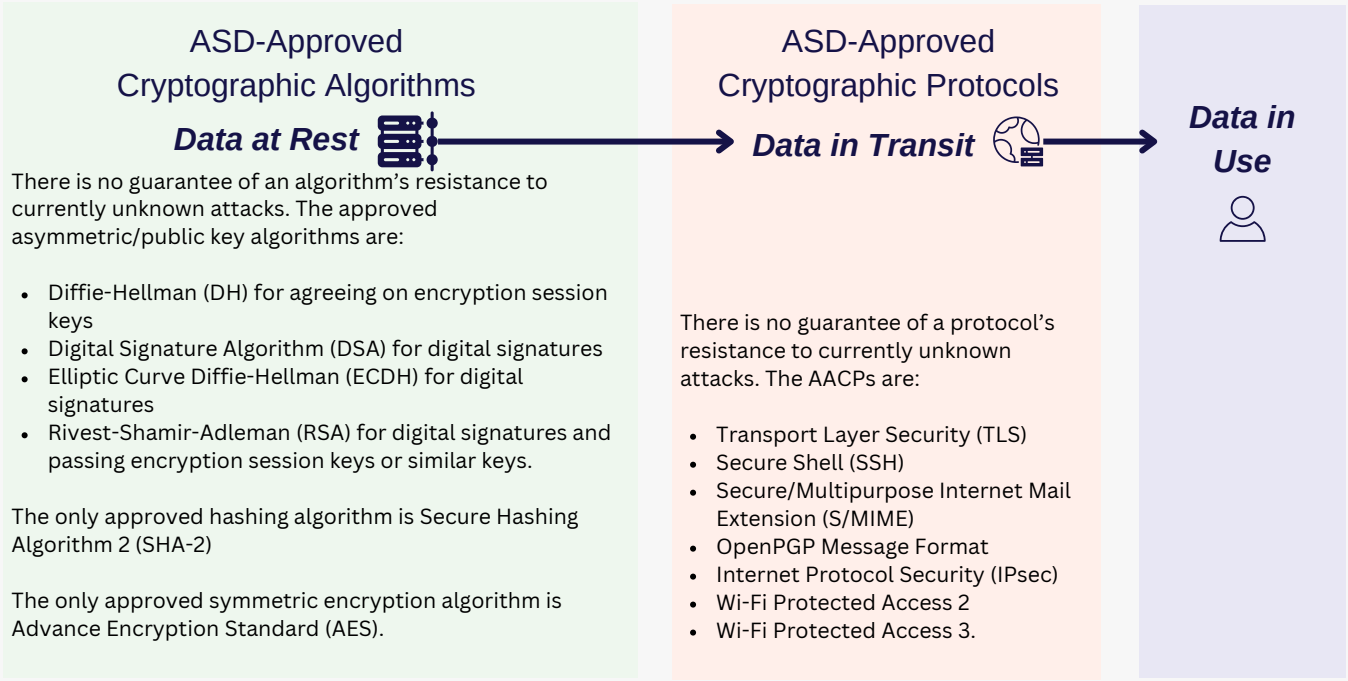


Diagram 8.1. Stages of Data and Encryption Standards: Guidelines for Cryptography | cyber.gov.au

Encryption and protection of data in flight, data at rest, and data in use, to address:

- what (if any) encryption is in place.
- where additional encryption might be of value.
- the impacts on processes and performance where encryption is in play.
- the overheads needed for key management.
- any risks associated with encryption.

Monitoring and application services can be configured to complete check sums and auditing of data. Many applications can provide audit and check-sums of data but are not turned on, most likely due to performance. IBRS recommends organisations workshop how they can activate the auditing capabilities already embedded in their platform, to ensure traceability and detection of intrusions when they occur.

Chapter 8

Steps to Data Integrity

The Australian Signals Directorate (ASD) Essential 8 (diagram 8.2) is in effect an example of good security hygiene. Every organisation should assess its maturity against the Essential 8, and have a continuous improvement plan in place to ensure complacency does not occur.

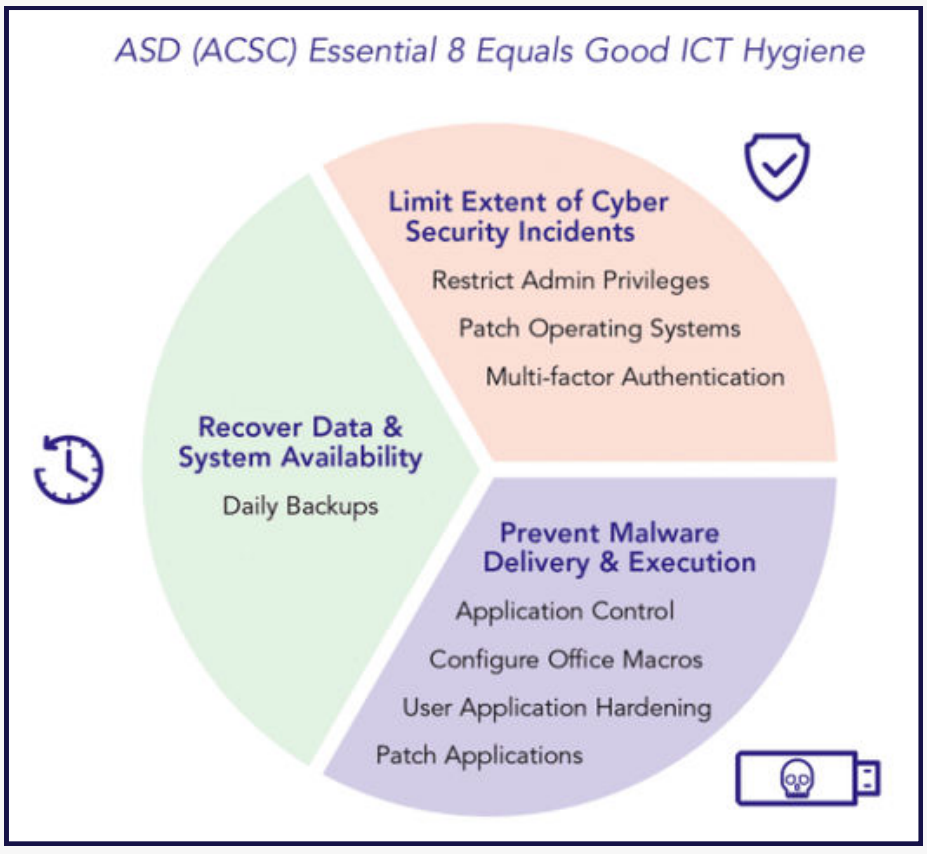


Diagram 8.2. Essential 8: Essential Eight Maturity Model | cyber.gov.au

Chapter 8

Steps to Data Integrity

You Can Outsource the Task, But Not the Risk

The impact of third parties with respect to the testing and validation and skills and awareness is also a major point of weakness for many organisations. For some organisations, there is a complicated environment where in-house, third party, and Cloud-based data repositories exist. In some cases, applications are in-house managed, Software-as-a-Service (SaaS) based, and others where only infrastructure is managed in-house and an outsourcer develops and manages the application. In such an environment, it is essential that the responsibility and risks associated with data integrity are understood. Each organisation needs to complete a mapping exercise for their executive, noting the boundaries of responsibilities. The mapping exercise should then conduct a review of the external agreements for delivery of these services, to identify the risk exposure to the organisation with respect to physical, personnel, and technical security over the data holdings.

Recovery

What then can your organisation do in advance around step 2 – recovery? The following framework is proposed for the development of your recovery plan:

- Investigate and understand the attack vector – not just what but how and when.
- Tailor the response – coordinate the response based on the actual threat.
- Adjust posture for access levels, passwords, and patching regime.
- Conduct a pen test assessment of the restored environment prior to going live.

Chapter 8

Steps to Data Integrity

First and foremost, if a cyber intrusion is detected the need to contact ASD and other legislated bodies such as Australian Federal Police (AFP) would be prudent, as an immediate reaction may result in the intrusion being escalated by the attacker. Seek guidance first!

If you have a high level of maturity in the mitigation step discussed above, then you will have read-only tapes of critical data (not necessarily all data) that were outside the immutable storage timeline. This would require both changes to process and increased holding of tapes, but as a belt and braces protection, read-only tape holding would limit the damage in the event of a ransomware attack.

Your organisation should seek advice on its approach to penetration (pen) testing, and whether a panel arrangement might be feasible for these services both in the white hat (testing inside against known vectors) and black hat (testing for weaknesses without insider knowledge) to confirm and assess risk. Ensure your data and any executables in the application that access the data are tested against the known attack vector before restoring to production.

There is no quick fix here. If your organisation is the subject of a significant cyber incident, restoration will be tracked in terms of days, not hours.

Chapter 8

Steps to Data Integrity

What's next?

Learn to prioritise data integrity by implementing robust strategies, complemented by training and monitoring. Along with this, maintain transparency with executive bodies about risk mitigation efforts. This can be accomplished through strengthening defense measures, giving special attention to third party access, and aligning with the Essential 8 Maturity Model. It is equally important to embed vulnerability assessments into recovery plans to ensure resilience against cyber incidents.

The next chapter discusses why effective ICT documentation is imperative for CIOs to develop informed decisions amidst complex on-premise and Cloud environments.

Chapter 9

Framework of ICT Documentation

Quick take

In this chapter, the significance of comprehensive ICT documentation in complex on-premise and Cloud environments is discussed. It also looks into the risks of disjointed documentation and the core elements of an effective framework. Beyond mere methodologies, the chapter focuses on the quality and integration of documentation, emphasising the need for a unified platform for efficiency and automation.

Chapter 9

Framework of ICT Documentation

Many organisations have a disjointed approach to their ICT documentation. Architecture, IT service management (ITSM), projects, contracts, and planning are more often than not loosely aligned, and are siloed in the management of the documented information they contain.

Some organisations will use Wiki-based technology, while others will use more modern technology like Sharepoint and Power BI. Key to any successful framework is the ability for it to provide line of sight for each element of the framework documentation back to the purpose for being – the business strategy.

No matter what technology your organisation uses, the key is to allow for integration of information and data across the ICT documentation framework, so that each documentation set is using the same data and information (where appropriate). To achieve this, IBRS recommends that the structure of the framework for your ICT documentation aligns with the following ICT documentation framework. The ICT documentation framework described below is structured across the four domains of strategy, operations, change, and contingency. Each domain can then be divided into four themes.

Chapter 9

Framework of ICT Documentation

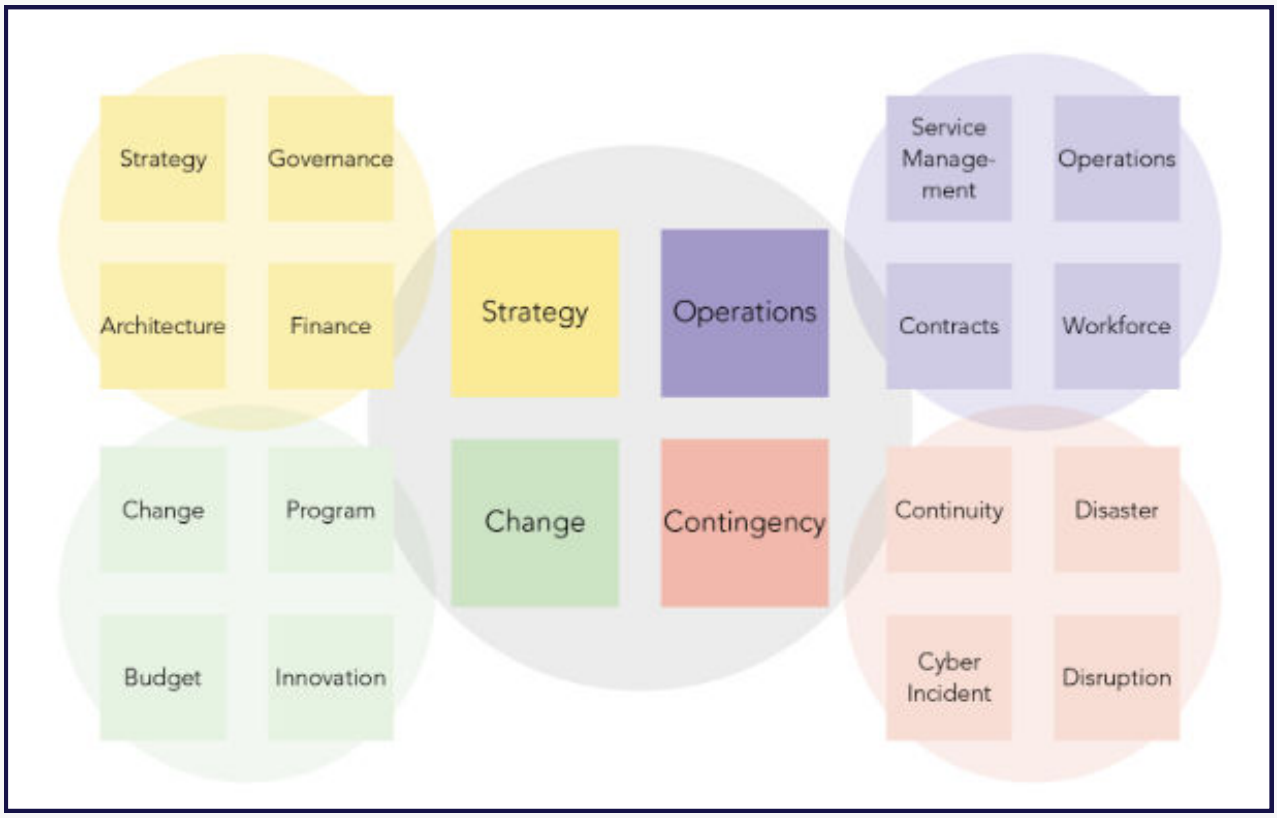


Diagram 9.1. ICT Documentation Framework

Chapter 9

Framework of ICT Documentation

Strategy Domain

The strategy component of the documentation framework should consider the following themes:

- Strategy and business planning
  - Business plan – what are the objectives of the business the ICT is supporting.
  - Technology plan – how the business is supported by technology.
  - Business cases for change under consideration – providing visibility of future change and innovation.
- Architecture, and as built diagrams
  - Business architecture – how business processes utilise technology to deliver outcomes.
  - Technical architecture – how the physical and virtual infrastructure supports the business architecture.
  - Data architecture – how data structure is designed and managed to ensure effective reuse and integration of information.
  - As built design documents – what actually exists and how it provides services.
- Governance
  - Governance model – who are the stakeholders that need to control ICT.
  - The processes for execution of effective governance – being the terms of reference for each governance body and its levels of authority.
  - Business capability mapping:
    - Business capability descriptions.
    - Critical ICT components that support each business capability.
    - Business capability owners (business owners and technology owners).
  - Risk analysis at the strategic level.
- Finance
  - Annual budgets.
  - Delegations.
  - Total cost of ownership models.
  - Financial reporting.
  - Budget planning/forecasting.

Chapter 9

Framework of ICT Documentation

Operations Domain

The operations component of the documentation framework should consider the following themes:

- Service management
  - Listing of services – the applications and services being provided both for the shopfront and inside ICT to support the shopfront.
  - Service desk SOP's.
  - Service levels – targets for acceptable delivery of applications and services to support business.
  - Performance management – how service levels are monitored and measured.
  - Knowledge database – User information, configuration management database (CMDB), and known error resolution.
  - Reporting framework – how, when, and to whom reporting is provided.
- Operational procedures
  - ICT operating model – who is responsible for what.
  - Configuration documentation – how is each service constructed and what is connected to what.
  - Service/application start-up procedures.
  - Software asset management:
    - Asset list by version and patch level.
    - Business owners.
    - Technical owners.
  - Data management:
    - Data model.
    - Back-up regime.
    - Data retention.
    - Archive.
  - Monitoring plan.
  - Risk analysis at the operational level.
  - Incident management and escalation procedures.
  - Change management procedures.
  - Release management procedures.
  - Daily hygiene procedures (e.g., checking logs, memory caches, backup completed, etc).

Framework of ICT Documentation

Operations Domain

- Contracted services
  - List of contracts and contract details:
    - Managed services.
    - Cloud services.
    - SaaS services.
    - Hardware and appliance procurement(s).
    - Software licence agreements.
    - Telecommunications services.
    - Labour hire services.
    - Consultancy services.
- Contract management procedures:
  - Contract administration processes.
  - Vendor management processes.
- Acquisition strategies for contract renewals:
  - Lead times for maintaining like for like.
  - Budget estimates for acquisitions.
  - Effects of innovation on replacement of existing solutions.
  - Effects of disruption on business outcomes and how ICT can respond.
- Workforce Planning
  - Skills mapping against the technology plan.
  - Skills gap analysis.
  - Workforce plan:
    - Workforce delivery plan:
      - Internal resources.
      - Labour hire resources.
      - Managed service resources.
      - Services resourced through product delivery (e.g., Cloud and SaaS products).
  - Workforce training plan.

Chapter 9

Framework of ICT Documentation

Change Domain

The change component of the documentation framework should consider the following themes:

- Change management
    - Baseline of business processes supported by ICT.
    - Organisational change management of business processes.
    - ICT change management processes.
    - Testing processes:
        - Unit level test scripts.
        - System level test scripts.
        - Integration level test scripts.
        - Automated testing services.
        - Business verification testing processes.
    - Patching program.
- Program management office procedures and processes
    - Project plans.
    - Schedules of in-flight projects.
    - Problem management procedures.
    - Life cycle management.
    - Software upgrade planning.
- Budget planning for change
    - Business cases for change initiatives.
    - Budget analysis.
    - Business benefit tracking and reporting.
- Innovation
    - Terms of reference for innovation working group(s).
    - Alignment processes for innovation working groups input to governance.
    - Proof of concept(s) planning, conduct, and reporting.

Chapter 9

Framework of ICT Documentation

Contingency Domain

The contingency component of the documentation framework should consider the following themes:

- Continuity
  - Business continuity plan (BCP) for ICT business unit.
  - Business impact analysis (BIA) assessment.
  - Support plans for support of business continuity.
  - Test procedures for BCP(s).
- Disaster
  - Disaster recovery (DR) plan (DRP).
  - DR workflows against DR scenario(s).
  - BIA assessments of restore time (RTO) and restore point (RPO).
  - Test plan and procedures for DRP.
- Cyber
  - Cyber incident response plan(s).
  - Test plan and procedures for CIRP.
- Disruption
  - Contingencies for elasticity of ICT in the event of disruption in the market – modelling of cost, performance, and productivity impacts if services are expanded to deal with market changes.
  - Contingencies for agility of ICT – what can be done differently?
  - Contingencies to harden cyber in the event of increased threats.

Whether you use ITIL, COBIT, Prince2, Agile, or the many other frameworks, this advisory is not about how but what should be documented. This IBRS ICT documentation framework will allow organisations to assess the value of a structure to the framework of ICT documentation. IBRS recommends that the ICT documentation your organisation considers of value be developed on a common platform to aid integration, ease of updating, and automation.

Chapter 9

Framework of ICT **Documentation**

What's next?

To secure a robust future IT talent pool, consider a long-term perspective on workforce needs. By leveraging the capabilities of younger generations, enterprises can drive better results. Concurrently, remain updated on technological innovations, fostering an environment where technically-aware users collaboratively contribute to R&D activities, ensuring the CIO remains a central figure in guiding innovation.

The final chapter looks into how CIOs can implement efficient workforce planning and optimise talent acquisition strategies.

Chapter 10

Framework for **Workforce Planning**

Quick take

The final chapter highlights workforce planning and optimising talent acquisition strategies, from traditional staffing to remote and managed services. With a focus on aligning IT needs with business objectives, IBRS offers a roadmap to building a flexible, responsive, and cost-effective ICT workforce framework to ensure your organisation can support developing the right skills for both today's challenges and tomorrow's innovations.

Chapter 10

Framework for **Workforce Planning**

IBRS previously proposed in May 2022 that the workforce problem should be defined as how best to resource the workforce to deliver and support the IT services that underpin the business.

The earlier IBRS advisory on workforce planning noted that each organisation should evaluate its approach to obtaining skills from the marketplace to establish a workforce framework based on:

- The three main time and materials (T&M) supply options of permanent staff, contract labour hire, and managed services.
- Consideration of payment based on outcomes rather than an effort to improve productivity to offset costs.
- Consideration of a remote versus hybrid or in-office workforce.
- Working under direction versus packages of work.

This chapter will provide CIOs with a method to assess their current framework and stimulate thought on how to improve their current processes. Like the ICT documentation framework, the ICT workforce planning framework can be considered against four domains, each with four themes.

Chapter 10

Framework for **Workforce Planning**

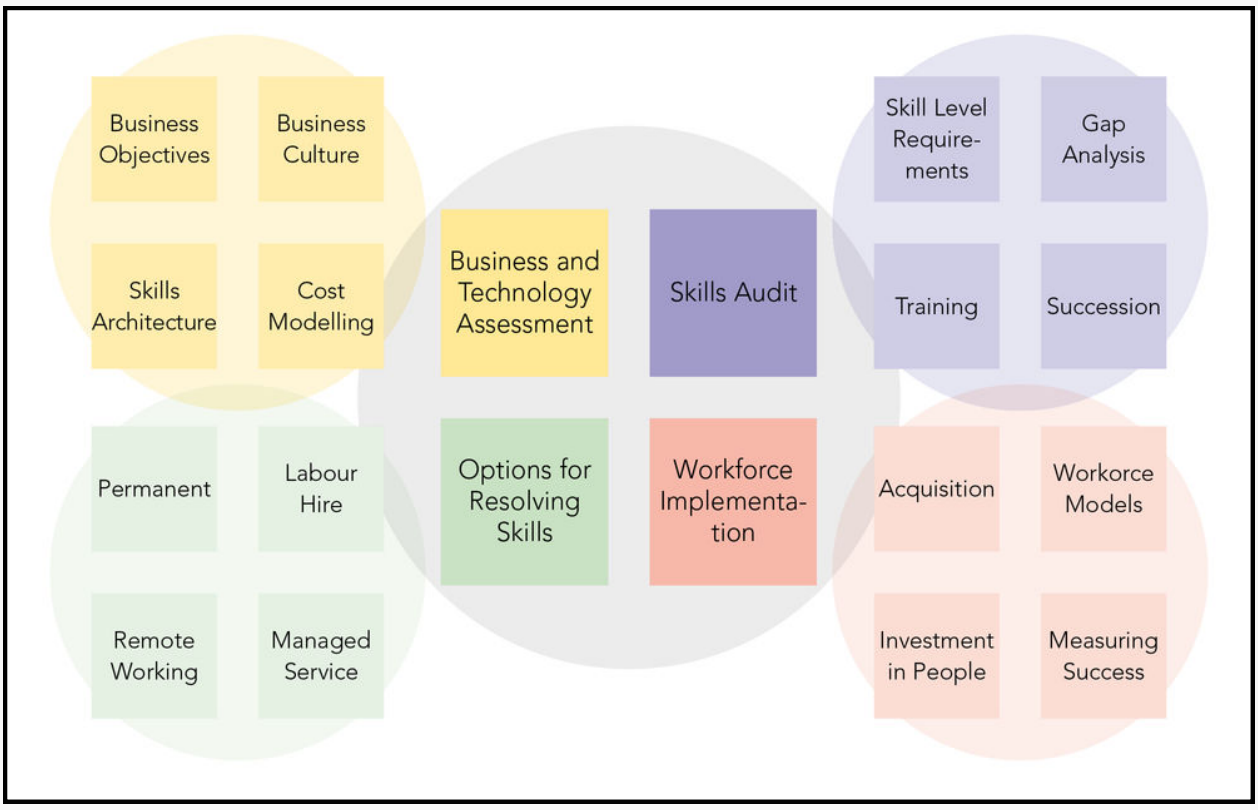


Diagram 10.1. ICT Workforce Planning Framework

Chapter 10

Framework for **Workforce Planning**

Business and Technology

This framework component is designed to conduct a thorough analysis of the skills needed to deliver success for the business under each of the following themes:

- **Business Objectives:** from the documented business and ICT strategy/plans, ascertain the business and technical skills required to deliver the agreed objectives and to achieve success. The reason for business and technology focus is that many ICT applications and services will need specific skills for administration and these will more and more be conducted within the business.
- **Skills Architecture:** assessment of the planned and as-built technical and business architectures will provide clarity of the technical and semi-technical skills needed to support the business. For example, where SaaS is used versus in-house supported services, and where is the configuration of the platform(s) expected to be managed, and are there low code or no code applications in play? This latter issue will impact how your organisation will endorse, develop, and manage the skill requirements for low code/no code applications and how they will need to be governed.
- **Business Culture:** assess the business and technology environment relative to the approach in developing the organisation's ICT workforce. Assess whether the organisation can accept a non-standard approach to the workforce, using task-based outcomes and remote workers, versus the traditional T&M approach.
- **Cost Modelling:** assess the current approach to funding the workforce. Ask how the model can be measured against business objectives and/or productivity measures rather than just skills and experience using a T&M approach? Identify from the current modelling where potential over-investment and/or under-investment can be derived. Lastly, look at alternate models that can be applied to different approaches to the workforce, such as outcome-based remote working, and outsourced outcomes.

Chapter 10

Framework for **Workforce Planning**

Skills Audit

The workforce framework will be informed by an assessment of the skills.

- **Skill Level Requirements:**
  - Business as usual (BAU) (steady state): firstly, assess the technical and data architecture against the business services they are designed to enable. When assessing the skills, include those that would support the application within the business units and the levels of support to be provided by managed services and other external SaaS providers.
  - Non BAU (major change and project management): Many organisations need additional workforce to augment BAU. Labour hire is often used to augment permanent staff to complete projects. The key in the skills audit is to gain a realistic understanding of the rate of change and the workforce options available.
  - Once the define target technology and the expected rate of change, using a defined taxonomy (like skills for the information age (SFIA)[2] where it is considered appropriate), assign the skills and experience levels needed to support the architectures.
- **Gap Analysis:** the gap analysis is designed to identify three outcomes.
  - The workforce skills shortfall to be addressed.
  - The workforce in the organisation that is in excess (needing retraining or no longer needed).
  - Market availability of the required skills. Whether the market can support permanent, labour hire, remote, or managed service. What can be trained, hired, and what needs to be considered for outsourcing.

2 Understanding Skills for the Information Age - SFIA 6 Framework', ACS, 2016.

Framework for **Workforce Planning**

- **Training:** as part of the skills audit, identify a training plan to both bring permanent staff up to the levels needed, retraining staff where appropriate.
- **Succession:** the need for succession planning is often not well executed, and is an important element of any workforce framework. No one person is indispensable, but many organisations find themselves chained to single person dependencies resulting from their knowledge of the customisation and business processes. This doesn't mean doubling the workforce. Considerations for succession should include:
  - Technical Succession: aligned with the training plan to cross train employees, allowing for shared responsibility for multiple tasks.
  - Technical Succession: where shared responsibilities are not possible, identify labour hire and/or managed service options that can be used to provide the functions if the single person can not deliver for any reason.
  - Management Succession Planning: supervisor and leadership training, mentoring, and opportunities to act at higher levels.

Chapter 10

Framework for **Workforce Planning**

Options for Resolving Skills

The options for resolving skills gaps to build the workforce can be achieved using four broad approaches:

- **Permanent:** the use of permanent staff is normally because the business needs technical skills with intimate knowledge of the business and the ability to be highly responsive. With the move to Cloud over on premise solutions, there will be a need for different skills. Rather than having permanent staff for on-prem systems and different staff to manage Cloud, consider cross-skilling on-prem support staff to both grow their skills but be able to apply their intimate knowledge of business across both technologies.
- **Labour Hire:** normally labour hire options should only be considered for limited engagements for non-BAU functions, such as projects. It is also a useful way to fulfil necessary BAU skills that are not needed at 100 percent capacity. Using part-time labour hire also allows for the skillset to work at other organisations, learning how others work and potentially adding value to your organisation's workforce.
- **Remote Working:** if you can build into the model skills resources that work remotely for both BAU and non-BAU you can effectively increase the talent pool. For remote working, you need to be able to set outcome targets, as your organisation would for an outsourced function, rather than solely looking at time and materials.
- **Managed Service:** the traditional managed services is not just for outsourcing of functions but also a hybrid for support of service functions, such as SaaS. Use this approach to resolving workforce restrictions when you can identify functions that can be outsourced for less cost than permanent staff. Managed service workforce may also be an option where there is a skills shortage, or where the functions can be provided with improved productivity at reduced risk.

Chapter 10

Framework for **Workforce Planning**

Workforce Implementation

Once all of the above factors have been completed, then the next stage is to finalise the design of your workforce framework and implement it.

- **Workforce Models:** define your workforce framework by identifying the components for retraining and acquisition. A successful framework will always be a mix of sourcing models.
- **Acquisition:** when acquiring the workforce, whether it be through recruiting of permanent and labour hire, or through use of remote working and/or managed services, it is important that all positions have documented position descriptions and/or detailed specifications in place.
- **Investment in People:** organisations need to accept that churn is normal. If your organisation invests in developing its people, that will never be lost. Good investment builds the reputation of employers, which attracts good people when opportunities become available. People may move on and gain experience from other organisations, and potentially return to your organisation in more senior roles, bringing their experiences with them.
- **Measuring Success:** lastly, the workforce framework must allow for measurement of success. In part this is performance management of staff and vendors. The workforce framework and plan must also have KPI's to determine whether the approach used is appropriate. Assessing KPIs for the workforce framework should have line of sight to the business strategy. For example, has the workforce framework and plan:
  - enabled business outcomes,
  - enabled a responsive approach to change, and
  - enable productivity improvement.

Chapter 10

Framework for **Workforce Planning**

What's next?

Assess your enterprise's current workforce structure. By integrating the IBRS framework, you can better cultivate a multifaceted plan that enhances productivity and curtails costs. Executing this plan will subsequently diminish risks and further boost efficiency.

About

Michael Mitchelmore

Michael Mitchelmore is an IBRS advisor specialising in the areas of ICT strategy, program and project management, ICT service delivery and telecommunications. Mike has more than 40 years of experience in the ICT industry during which he has successfully led engagements in the design and deployment of a global telecommunications networks and IT platforms, negotiated managed telecommunications services, introduced new capabilities for call centres and consolidated ICT systems to focus on service delivery for citizen facing services. Mike has also assisted clients in ICT strategy, support planning, system design and architecture, and procurement strategies. Mike is a certified PRINCE 2 Practitioner and an ITIL (V2) Manager.

About

IBRS | ANALYSIS INSIGHT JUDGEMENT

IBRS is a boutique Australian ICT Advisory Company. IBRS helps clients mitigate risk and validate their strategic decisions by providing independent and pragmatic advice while taking the time to understand their specific business issues.