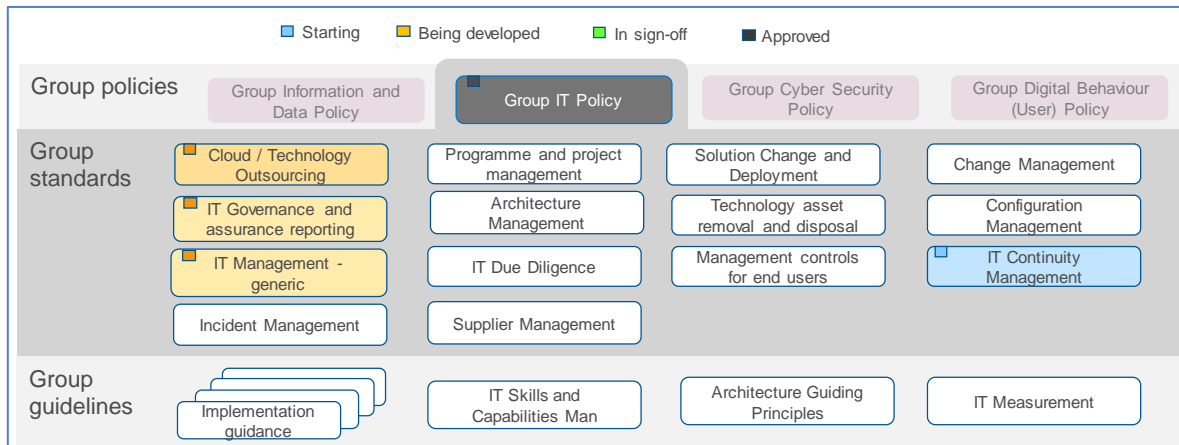


## **Sanlam Allianz IT Policy**



Sanlam Allianz IT Policy	
<b>Classification</b>	Company Confidential
<b>Type of Policy</b>	SanlamAllianz Information and Technology Policy
<b>Sanlam Entities subject to this Policy</b>	SanlamAllianz
<b>Governance Area Addressed</b>	Information and IT
<b>Group Approving Authority</b>	Sanlam Ltd Board
<b>Group ExCo Sponsor</b>	Chief Actuary and Risk Officer
<b>Group Responsible Person</b>	Paul [REDACTED]
<b>Group Policy Owner</b>	Group Technology & Information
<b>Group Author</b>	Group EA & Governance
<b>Group Date of First Approval</b>	10 June 2020
<b>Frequency of Review or Update</b>	Annual
<b>Group Date of Next Review</b>	31 May 2025
<b>Version Number</b>	V1.0 FINAL
<b>Group Policy Status</b>	Approved
<b>Sanlam Allianz Approving Authority</b>	Sanlam Allianz Ltd Board
<b>Sanlam Allianz Responsible Person</b>	Henri [REDACTED] ers
<b>Sanlam Allianz Date of First Approval</b>	31 July 2023
<b>Sanlam Allianz Date of next review</b>	31 July 2025
<b>Sanlam Allianz Version number</b>	V1.0
<b>Sanlam Allianz Status</b>	Final
<b>Related Policies</b>	Sanlam Allianz Cyber Security Policy Sanlam Allianz Information and Data Policy Sanlam Allianz Digital Behaviour (User) Policy

## Policy and status of Group Standards



## 1 Introduction and context

Sanlam Allianz defines IT Governance as the high level, direction-giving and decision-making requirements for the use of IT in the Business. The Board expects Management to establish an IT Governance framework and reporting system that is aligned to the content of this policy, the supporting standards and the System of Governance. Management’s governance framework must be effective in deriving value from the use of IT and realising business strategies, while identifying and curbing risk successfully. It is furthermore expected that the Governance team within Group Technology and Information (GTI) act as a control function and Internal Audit will jointly monitor compliance against IT policies and report an independent view to the relevant Board Committees.

For Information and Technology Policies the Group makes use of an Adaptive Governance model that caters for three styles of Governance, two of which are covered by this policy, namely Command and Control and Outcomes-based Governance. The third style of governance, namely Edge governance deals with the decision making for the agile enterprise as close as possible to the point where solutions and insights are delivered and used in business.

## 2 Purpose

This policy defines the Sanlam Allianz Ltd Board’s requirements regarding IT Governance and Management at a high level. The implementation of the principles in this policy is guided through several supporting standards and guidelines that define a minimum level of IT Governance compliance requirements for Sanlam Allianz.

## 2.1 Goals/Outcomes

IT remains a strategic enabler of business as it is deeply entrenched in the way Sanlam Allianz conducts its daily business activities while it also provides the mechanism through which future aspirations can be achieved. Therefore, IT Governance must achieve Sanlam Allianz's IT Governance objectives namely:

- Align Business and IT strategies.
- Deliver demonstrable value from IT-related investments, services and assets.
- Ensure the successful delivery of Information Technology projects.
- Exploit new technologies which offer capabilities that will position the business for the future.
- Ensure IT sustainability.
- Transparently manage performance of IT capabilities.
- Share where it is in the interest of the Group.
- Protect Sanlam's IT assets.
- Manage the risks posed by old and new technology.
- Enhance agility and innovation by investing in the people and processes engaged in leveraging IT; and
- Enable digital aspirations; namely client, intermediary and employee experience; data fluency; integration and ecosystem.

## 2.2 Dispensation

The policy statements are grouped under headings correlating to Sanlam Allianz Standards and Guidelines in which information is provided on the implementation as well as a description of what would constitute compliance.

In conjunction the Group's Technology and Information System of Governance records the bodies entrusted with the governance responsibilities across the Sanlam Allianz Cluster. In addition to Group Structures, Cluster Level structures are identified and at the lowest level accountability vests with the Chief Executive Officer (CEO) of a Business Unit.

In instances where non-compliance is identified the relevant Business Unit CEO will be expected to show progress towards a compliant state within two quarters and should reach a state of compliance within twelve months, risk exposure permitting. Sanlam Allianz Cluster level Governance structures are expected to oversee and report on compliance and progress towards compliance.

Failing to reach a state of compliance within these guidelines will initiate an escalation to the Sanlam Allianz Cluster CEO who can extend the period to reach compliance while simultaneously reporting to the relevant Board Committee.

## 3 Group IT Policy

The Sanlam Allianz's actions required to manage and govern IT effectively are indicated below. These principles are part of an overall System of Governance and three complementary policies:

- Sanlam Allianz information and Data Policy;
- Sanlam Allianz Security Policy; and
- Sanlam Allianz Digital Behaviour (User) Policy

## General governance

1. IT Governance must be on the agenda of the Board as well as the designated Governance structures.
2. IT Governance must be established and documented at Group, Sanlam Allianz Cluster and Business level. It must clarify authority and responsibilities.
3. The IT Governance model must specify the control responsibilities for 2<sup>nd</sup> and 3<sup>rd</sup> lines of defense as required from a risk and control perspective.
4. IT Governance is foremost a business issue and the primary responsibility for affecting IT Governance must therefore be the Business entities requiring IT services/solutions whilst the IT divisions are providing such services.
5. When acquiring Businesses, IT due diligence must focus on IT risk as well as the cost of integrating into and achieving compliance with the SanlamAllianz IT Governance framework.
6. IT reporting must flow to the Board and the structure of reporting should align with the Group's standardized reporting requirements.

## Strategy and Value

7. The IT strategy must be articulated illustrating alignment with the Business and Group's overall strategy including the Group IT strategy. Resultant investments must be managed by balancing the risk and value dimensions.

## Measurement

8. The expected and actual value realized from IT investments must be articulated, demonstrated and/or measured. If no value is realized the investment must be recorded in the loss register with an appropriate analysis and reporting.
9. An IT measurement culture with fair principles and practices must be established to ensure understanding of operational IT costs, influence behavior and measure delivery productivity.

## Risk

10. IT risks must be managed and reported explicitly to the Board and designated Governance structures.
11. Business continuity plans must be supported with disaster recovery plans and capabilities that must be tested regularly. The scope of such tests must be comprehensive, the outcomes must be reported and where required remediated.
12. The SanlamAllianz uses CobiT as external framework for IT Governance. The IT internal control framework must be documented, and controls duly implemented and monitored taking cognizance of the preferred framework.
13. IT processes and IT systems must comply to relevant legislation and regulation.
14. Assurance must be provided to the Board regarding the compliance to and effectiveness of the IT Governance system. Controls and processes must be implemented to enable users to adhere with minimal effort to the Group's Digital Behavior and Security Policy.

## Organisation

15. A Business Change<sup>1</sup> and IT organization with suitable capacity, structure and capabilities must be maintained to implement business demand for IT. This IT organization must implement technology changes and run the technology operations.
16. The leadership of the Business Change and IT organizations must ensure continuous evaluation and renewal of practices associated with delivery and maintenance of IT.
17. The leadership of the Business Change and IT organizations must actively work towards attracting and developing skills in their organizations to meet the demands of business.
18. Relationships between business and IT departments must be managed formally and should ideally be based on agreed responsibilities of Business, Business Change and IT functionaries.

## Architecture

19. Architecture must be developed and maintained in response to business strategy. The Group architecture through its approval structures must establish principles and identify and define Group responsibilities as well as shared/common capabilities.
20. Architecture must achieve standardization and simplification across the Group, Sanlam Allianz cluster and/or business units using agreed patterns.
21. Architecture must employ a medium to long term planning horizon.

---

<sup>1</sup> The Business Change organization consists of functions such as Business Consultancy, Business Analysts, Process analysts, Programme Management, Business Change Management, etc. The organization can be a part of the IT organization or can be separate to the IT organization.,

22. Synergies and sharing opportunities must be sought after and exploited. Should this not be possible, the alternative approach needs to be motivated and approved.
23. Technical debt must be addressed on an ongoing basis by having a renewal roadmap and annual budget allocation towards technical debt for both Applications and IT infrastructure.
24. Emerging risks and advances in technology must be monitored, including noting opportunities and potential disruptive effects on the organization and its business model.

## Innovation, Change and Projects

25. Innovation must be encouraged to identify where technology advances can enable or support innovation or process improvement.
26. Investments in Change and Project Initiatives must be approved by governing bodies and owned by senior executives.
27. Change and Project Initiatives must follow a process that is adjusted according to the level of risk, complexity and extent of the change.
28. Solutions must be sourced following an objective, transparent, and approved process.
29. Solutions must be designed, developed and implemented following appropriate and documented methodology and project management discipline.
30. Quality assurance and quality controls must be integral to engineering processes.
31. Change and project initiatives must deliver the controls to support a solution.
32. The configuration management of infrastructure, COTS (Commercial Off-the Shelf Software) and bespoke applications must adhere to all standards in order to ensure compliance to areas that include change control and cyber security.

## Outsourcing and 3rd parties

33. IT Outsourcing must be an objective and transparent process, compliant with relevant Group policies and done formally, ethically and with due regard for environmental factors. Reasonable care and caution (due diligence) must be exercised when selecting vendors.
34. Legal agreements with third parties and outsourcers must be managed actively.
35. In an outsourced agreement Management retains accountability and must ensure that oversight is performed by skilled and experienced personnel, with Cloud outsourcing being a specific instance.

## Service provisioning

36. Capacity and performance of systems must be planned and managed by considering workload forecasts and other relevant sources of change.
37. Service expectations must be agreed with service providers and documented. The levels of service delivered must be managed accordingly.
38. A helpdesk and problem management process must enable the reporting of incidents and ensure that problems are resolved, and preventative changes applied where relevant.
39. A process must be provided for servicing and monitoring the consumption of day-to-day requests for service and technology.
40. Operations must be managed by following documented operational procedures and by monitoring systems and service level indicators.

----- end of document -----





## DOCUMENT CONTROL

### AUTHORING AND REVIEW CONTRIBUTIONS

The following stakeholders contributed to the content of this document:

Nr	Name	Representing	Contribution
1	The [Redacted]	GTI	Review
2	And [Redacted]	SPF	Review
3	Ger [Redacted]	SIG	Review
4	Der [Redacted]	SC	Review
5	Mar [Redacted]	Group Office	Review
6	Ant [Redacted]	Group	Review
7	Her [Redacted]	SPF	Review
8	Tho [Redacted]	SIG	Review
9	Mik [Redacted]	SC	Review
10	Cor [Redacted]	SEM	Review
11	Key [Redacted]	Santam	Review
12	Paul [Redacted]	Group EA & Governance	Authoring
Sanlam Allianz Information and Technology Committee			
1	Co [Redacted]	Sanlam Allianz	Review
2	He [Redacted]	Sanlam Allianz	Review
3	An [Redacted]	Sanlam Allianz	Review
4	Pe [Redacted]	Sanlam Allianz	Review
5	Sal [Redacted]	Sanlam Allianz	Review
6	An [Redacted]	Sanlam Allianz	Review

### GOVERNANCE AND CONTROL

BODY	ROLE
Group CIO forum	Consider & propose for approval
Group Information and IT Committee	Consider & propose for approval
Life ManCo & Group ExCo	Consider & propose for approval
Group Risk and Compliance Committee	Consider & propose for approval
Ltd Board	Approval
Sanlam Allianz Information and Technology Committee	Consider & recommend for approval
Sanlam Allianz Ltd	

## REVISION HISTORY

Nr	Date	Ver.	Document	Revision Tracking Notes
1	13-02-2020	0.01	Draft	First draft created in response to GOI 3 compliance requirements. For review internally in GTI EA & Governance
2	30-04-2020	0.10	Draft	A.Gildenhuys comments included
3	08-05-2020	0.20	Draft	Socialisation review comments included
4	10-06-2020	1.0	Final	Approved by the Sanlam Ltd. Board
5	18-05-2023	1.0	Business Cluster Review	Reviewing the Group Policy to recommend for approval to the Sanlam Allianz Board
6	14-03-2024	1.0	Approval	Sanlam Kenya Board approved policy as is

©Sanlam Life (Pty) Ltd, 2019. This information is proprietary to Sanlam (Pty) Ltd and is confidential. No part hereof may be reproduced, copied, and/ or transmitted (in any form or for any purpose) without Sanlam's prior written consent.