Locked Bag 11
Carlton South VIC 3053
hostplus.com.au

Adam Monteleone
Level 24, 535 Bourke St
Melbourne
VIC 3000

12/12/18

Dear Adam,

HOST-PLUS PTY LTD (Hostplus) Risk Governance Written Assessment

As per APRA's request of 28 June 2018 the Hostplus Board has undertaken a self-assessment against APRA's report into the CBA.

Please find attached the Board endorsed written assessment.

The Hostplus Board welcomes the opportunity to discuss the assessment further with APRA if required.

If you have any questions, please do not hesitate to contact myself or Norlena Brouwer on (03) 8636 7727.

Kind regards,

David Elmslie
Chair of the Board

Executive Summary

This Board endorsed written assessment is the outcome of Hostplus' self-assessment into the effectiveness of its Risk Governance structures.

The Hostplus Board worked closely with the Group Executive team to ensure the self-assessment was in depth, challenged and provided insights across the whole organisation. The report follows the same structure of APRA's report into the CBA and is separated into five sections:

- Section A – Introduction
- Section B – Governance
- Section C – Accountability
- Section D – Culture
- Section E – Assessment Initiatives

Hostplus undertook a series of individual interviews with Directors and Group Executives, as well as a facilitated workshop with senior management to gain sufficient insight into the implementation and effectiveness of governance, accountability and culture across the organisation.

To ensure effective challenge the Hostplus Board engaged KPMG to provide independent challenge and feedback into both the approach Hostplus was taking and its final report. KPMG also facilitated both the individual interviews and the senior management workshop.

Through the assessment process the Hostplus Board identified many strengths, but also a number of areas that could be enhanced to ensure the continuous improvement of Hostplus' risk governance, accountability and culture. The Hostplus Board has agreed to 22 initiatives that it believes will help Hostplus continue to be an industry leader in superannuation. The full set of agreed initiatives can be found in Section E – Assessment Initiatives.

The Hostplus Board and its senior leadership are committed to the successful implementation of these initiatives. An implementation plan will be developed and presented to the Board for approval in February 2019. Ongoing reporting of progress against this implementation plan will be included in both the Board and its Committee's risk reports.

Section A - Introduction

1. Introduction

On 28 June 2018 APRA wrote to the Hostplus Chair requesting a Board endorsed written assessment against APRA's Prudential Inquiry into the Commonwealth Bank of Australia (CBA). The assessment was to be submitted to APRA by 30 November 2018, Hostplus requested and was granted an extension until 14 December 2018.

This request was in addition to APRA's 1 May 2018 press release that suggested all regulated financial institutions would benefit from conducting a self-assessment to gauge whether similar issues might exist in their organisations and required the Board to assess the embedment and effectiveness of governance, culture and accountability across the organisation.

Hostplus has undertaken this self-assessment with the insights and findings identified contained within this report.

2. Background

Hostplus is the national, profit to member, superannuation fund for those that live and love Australian hospitality, tourism, recreation and sport. The Australian Hotels Association and United Voice jointly established the Fund 30 years ago in 1988. Hostplus currently has over 1.1 million members and $37 billion funds under management and employs approximately 280 staff members nationally with the majority based in the Trustee office in Melbourne.

As a regulated superannuation fund, Hostplus was established as a trust and holds superannuation assets for the benefit of its beneficiaries. APRA classifies Hostplus as a not for profit industry fund which caters for particular industries, as well as public offer members. As a registrable superannuation entity (RSE) license holder Hostplus is governed by the Superannuation Industry (Supervision) Act 1993 and its Directors must comply with the trustee and director covenants which include exercising the trustee's or director's powers in the best interests of the beneficiaries of the fund.

One of those specific trustee covenants is the covenant relating to risk management (s52 (8)). This covenant requires the trustee to formulate, review regularly and to give effect to a risk management strategy that relates to the activities, or proposed activities, of the trustee and the risks that arise from operating the entity. As these covenants are required to be reflected in the Fund's Trust Deed and Constitution it embeds risk management within the foundation of the Board, its decisions and ultimately the Fund's culture.

The Trustee is also required to comply with the SIS Acts Sole Purpose Test (s62) which requires the trustee to ensure that the Fund is maintained solely for the provision of benefits on or after a member's retirement.

These requirements coupled with Hostplus' profit to member structure are the foundation of Hostplus' member first culture. All decisions are made through the lens of members' best interest, and ultimately differentiates Hostplus from the CBA as all profits are returned to members and removes the inherent conflict between member or customer outcomes and financial outcomes for stakeholders.

3. Hostplus Approach

In their 28 June 2018 letter APRA encouraged the Hostplus Board to ensure their assessment included:

- Depth
- Challenge
- Insights

The Hostplus Board developed an approach with these three requirements in mind.

Depth

To ensure depth was achieved within the assessment and to enable the Board to examine and ensure that Governance, Culture and Accountability are embedded in practices and behaviours, and enforced across the organisation, Hostplus utilised a number of different mechanisms. These mechanisms included:

- Review of all relevant documentation including the Risk Management Framework, Compliance Management Framework, Governance Framework and internal policies and processes to ensure all policies and processes align and were clear, consistent and concise.
- Individual Director interviews which included targeted questions in relation to the role of the Board, issues and incident oversight, remuneration, accountability, culture, and operational versus financial risk focus.
- Individual Group Executive interviews which included targeted questions in relation to senior leadership oversight, collective accountability for risk, remuneration, incident and issues management, culture, and risk and compliance visibility.
- Facilitated group workshop with the Heads of Departments which explored key themes and utilised a survey tool to generate some hypotheses. Survey themes included collective accountability and responsibility of risk, risk culture, senior leadership oversight of incidents and issues, and the accessibility of risk documentation.
- Analysis of previous staff engagement surveys and Board performance assessments to provide further insight and overlay of interviews and workshop outcomes.

By utilising a number of different inputs, the Board has been able to gain a good cross section and depth of insight into the business. This has allowed for key themes to emerge and to assess if the tone from the top is filtering to all levels of the business.

Challenge

To enable challenge in the process and to provide the Board with fresh perspectives of the strength of the governance, culture and accountability across Hostplus, the Board engaged KPMG to provide independent challenge and feedback. feedback over the design and effectiveness of Hostplus' self-assessment. The scope of their engagement included:

- Feedback on the objectives, scope and approach of Hostplus' self-assessment.
- Consider and review of existing documentation.
- Facilitate a briefing session with the Board to provide insight into the themes of APRA's CBA report and to provide a common understanding of the themes as they apply to financial services.
- Challenge, review and help develop key focus areas and questions to be explored in interviews and workshops.
- Conduct all interviews independent of Hostplus management.

- Facilitate a group workshop with Heads of Department.
- Consider and provide challenge on the format and structure of Hostplus' final report to be submitted to APRA.

The Board determined that KPMG should facilitate all interviews and workshops to provide objectivity and observations outside those of the risk function, as per instruction from APRA.

KPMG were able to determine common themes from these interviews and workshops and to highlight a series of observations and self-identified initiatives for improvement.

Insights

Through the cross section of interviews and workshops KPMG made a number of observations and highlighted a number of self-identified initiatives for improvement. Hostplus management also included initiatives that had already been identified which responded to observations raised by participants.

The insights gained through the process are further documented in the following sections of the report Where possible the observations and insights have been aligned with APRA's CBA report and fall into the three major categories of Governance, Accountability and Culture.

Governance and Management of the Self-Assessment

This self-assessment has been endorsed by the Hostplus Board.

The Hostplus Board was engaged, consulted and kept up to date throughout the self-assessment process. A sub-group of the Board comprising of the Chair and two Deputy Chairs were involved and met regularly to consider interview outcomes and potential responses. Additionally, all members of the Board were provided the full report to enable them to provide individual review and feedback.

Section B – Governance

The compulsory nature of the superannuation system, as well as its size and significance in Australian public policy, requires superannuation funds to implement and maintain the highest standards of governance. As previously stated, Hostplus operates as an established trust and the fiduciary nature of trustees' obligations is such that the trustees' discretionary powers are limited by the terms of the governing rules of the Fund, which include the trustee covenants, and duties are assigned to specifically protect the interests of Fund members and beneficiaries.

Hostplus' self-assessment has reviewed this governance structure, specifically its risk governance structure through all levels of the organisation, (including the reporting of incidents and issues) for its effectiveness and any areas for enhancement.

1. Role of the Board

The Hostplus Board is responsible for the overall governance and strategic direction of the Fund, with the aim of protecting and enhancing the interests of its members. Part of this overall governance is the monitoring and adherence to prudent risk management systems, policies and processes.

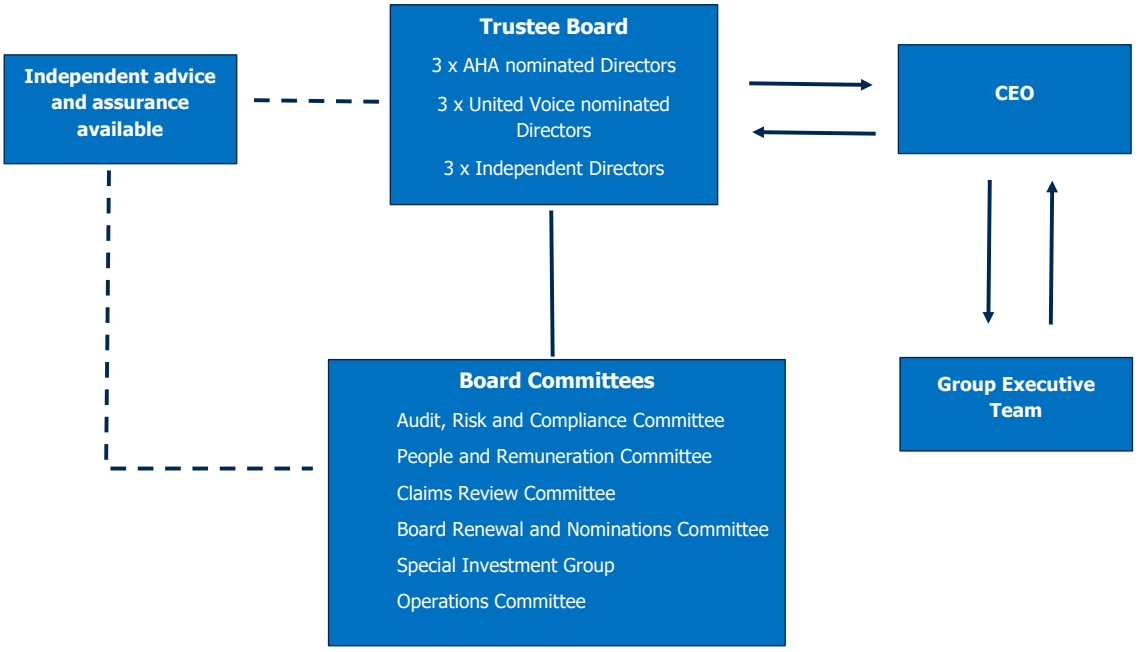
The Hostplus Board is composed of three AHA nominated Directors representing the employers, three United Voice nominated Directors representing the members and three independent Directors. The Board meets seven times per year with the Chair, in conjunction with the CEO and Deputy Chairs, developing the agenda for each meeting ensuring there is adequate time allocated for risk and compliance priorities.

The Board is assisted in its responsibilities through a number of Board Committees, these committees are:

- Audit, Risk and Compliance Committee (ARCC)
- People and Remuneration Committee (PRC)
- Claims Review Committee (CRC)
- Nominations and Board Renewal Committee (NBRC)
- Special Investment Group Committee (SIG)
- Operations Committee (newly created in 2019)

Each of these committees is governed through its own Terms of Reference which is approved by the Board. Figure 1 below outlines the structure of the Board and its committees.

Figure 1 – The Structure of the Board and its Committees



The Board delegates a number of responsibilities to its sub-committees. In relation to risk management and governance it specifically delegates these responsibilities to the ARCC. These delegations are summarised below:

- The ARCC will enquire into, consider and review any of the following matters, and shall as required by the Board or as it considers appropriate, advise the Board in relation to them:
    - The Trustee's ongoing risk management program and its efficacy in identifying all areas of potential risk.
    - That adequate policies and procedures have been designed and implemented to manage identified risks.
    - That a regular program of audits is undertaken to test the adequacy and compliance with prescribed policies.
    - That proper remedial action is undertaken to redress areas of weakness.
    - Recommendation of the appointment of the Fund's auditors to the Board each year.
    - All matters arising from the audits.

The operation of the ARCC is primarily supported by the finance function, the internal auditor (KPMG), the external auditor (PwC) and is attended by the Group Executive Risk and Compliance. The Committee meets three times per year with reporting consisting of internal and external audit reports and the ongoing monitoring of any audit findings, any new or emerging risks, fraud and AML/CTF updates, compliance updates, and any financial and taxation reports. The membership of the ARCC consists of equal representation by three Board members, with the independent Director being the Chair of the ARCC.

In addition to the ARCC, the Board undertakes an annual Board Risk Review where the Board considers and engages with the Risk Management team who present to the Board on emerging risks, key issues facing the Fund and the planned risk activities for the year ahead. It also allows the Board to focus on key risks and review the Risk Management Framework to ensure it remains adequate for Hostplus.

1.1. Assessment Insights

In order to gain assurance that the Board was operating effectively in its responsibility to provide oversight of a prudent risk management framework, the Board wanted to ensure that it assessed its own role in the management and monitoring of risk at Hostplus. It took into consideration the findings from the report into CBA and assessed itself against these findings.

Although the structure and operating model of Hostplus is very different than the CBA and the size of the organisation is much smaller, the Hostplus Board and its committees wanted to assess itself against the shortcomings of the CBA Board that were highlighted in the report.

The key themes that were highlighted in the assessment were:

- Enhancements to Board and Committee operations.
- Improvement to the quality of reporting to the Board and its Committees.
- Ongoing promotion of constructive challenge within the Board and its Committees, both between Board members and of the Group Executive team.

These key themes were taken from interviews with individual Directors as well as the Board's annual performance self-assessment.

Enhancements to Board and Committee Operations

Throughout the assessment it was clear that the Hostplus Board and its Committees operate effectively in performing its responsibilities, however it was acknowledged that there are always opportunities for improvement. The Board also took into account the recent industry focus on Superannuation Fund Governance, such as APRA's 2017 Superannuation Governance Thematic Review and the Australian Institute of Superannuation Trustees (AIST) Governance Code. Prior to this self-assessment the Board has adopted the recommendations from both APRA's thematic review and has also formally adopted the AIST Governance Code. This increased focus on Fund governance has driven a number of enhancements to the Board and its Committee operations such as:

- Introduction of annual individual Director peer assessments in addition to overall Board performance assessments.
- Creation of a Board Renewal Committee to manage the balance and composition of the Board and its Committees' skills and experience.
- Development of diversity metrics for the Fund, Group Executive team and the Board itself.

It was also acknowledged that over the course of the last two years Hostplus has undergone significant growth, not only in funds under management (FUM), but also in the number of people it employs. This growth has instigated a number of changes in order to support the Board in maintaining its high level of oversight and management of not only risks facing the Fund but all other functions across the organisation.

These changes include the introduction of two new committees:

- Special Investment Group Committee
- Operations Committee

The Operations Committee will support enhanced oversight, analysis and reporting of non-financial issues and incidents, in addition to its other responsibilities as detailed in its Terms of Reference. This Committee will also be member and employer focussed which will allow the Board to gain further insights into the maintenance of its member-first culture which underpins Hostplus' risk

culture. This focus will be maintained through increased complaints reporting, third party monitoring and assurance reporting, service operations updates, and employer servicing updates.

All members of the Operations Committee are members of the Board and, as per all Board Committees, the Operations Committee papers and minutes will be provided to all Directors, with a standing invite for any Director to attend meetings. The Board acknowledges that with an increase in the number of Board Committees continued focus on the effective coordination between committees needs to be maintained. This would include:

- The ongoing practice of all Committee papers and minutes being made available to all Directors.
- The ongoing practice of standing invites to all Directors to attend any committee meetings.
- Specific sharing of internal and external audit reports when they impact operational functions of the Fund.
- Ensuring that operational issues and incidents reported to the Operations Committee are also reported to the ARCC to ensure these incidents are incorporated into the monitoring of the Fund's Risk and Control Environment.

Improvement to the quality of reporting to the Board and its Committees

A very clear and consistent insight that was identified through both interviews and the Board's annual performance self-assessment was the quality of reports coming to the Board and its Committees, specifically the 'volume, length, clarity and timing of reporting'. APRA's report into the CBA highlighted that for the Board to effectively challenge senior management it must rely on comprehensive reporting that clearly highlight specific matters warranting attention. On review of Hostplus' Board and Committee packs it has been identified that the comprehensiveness of the reports was actually making it difficult to identify the specific matters warranting attention. This was particularly relevant for the Board reports. The Hostplus Board has an ongoing program to assess the quality of Board reports it receives. It views this as an iterative process with improvements being made regularly.

Hostplus has recently undertaken two key initiatives to improve the volume, length, clarity and timing of reporting to the Board. The first was an externally facilitated session with the Group Executive team to uplift report writing skills and to ensure consistency in reporting across the different functions. The second initiative was a Board and Group Executive 'page turn' of Board papers to agree on areas for improvement of reports. It was agreed that the focus on improvements should be on tailoring the content for the Board so that there was better clarity on key issues, recommendations and risks.

Specific review of the risk and compliance reports to the Board and its Committees, as well as comments from interview participants, showed that although reporting to the ARCC was detailed with a revolving set of metrics, including key risk indicators, risk and compliance reporting to the Board was more operational and focussed on regulatory response and particular issues. Interview participants identified improvements to this including risk reporting becoming more strategic in nature and focussing on key areas/risks, as well as the benefit of having periodic and structured meetings between Committee members and risk owners to improve understanding and to test the information flow to the Board and its Committees is working effectively.

It was also noted that whilst there is strong focus on investment and financial risks, including the reputational risks of investments, participants were comfortable with the level of operational reporting to the ARCC and believed that this will be further enhanced through the introduction of the Operations Committee.

Hostplus is currently implementing a new Governance, Risk and Compliance system (GRC system) that will help to provide an enhanced level of reporting throughout the organisation. This system will help to provide clear dashboard reporting as well as enable thematic reporting to be developed across organisational compliance obligations, controls, processes and risks. This will enable the ARCC to initiate deep dives into specific key areas of the business.

Ongoing promotion of constructive challenge

Through the self-assessment it was very clear that the Board is comfortable with the level of challenge between Board members and the opportunity provided to challenge the Group Executive. This was also supported through the annual Board performance self-assessment.

It was noted the 3:3:3 Board structure contributed to a healthy natural tension that helped to ensure that Board members continued to challenge each other as well as the Group Executive. This observation was also supported at the Group Executive level, with the Group Executive acknowledging the level of challenge they received from the Board.

It was noted through interviews with the Group Executive that the level of challenge within the Group Executive team wasn't as robust as what it was at the Board and that there is reliance on subject matter experts to manage issues and incidents within their specific areas. It was also noted within the senior leadership workshop that each area focused on their specific domain, but there was not enough opportunities to collectively challenge or enough 'cross divisional oversight'. This particular insight could be addressed by the introduction of a shared, collective risk KPI at the Group Executive level. This action is discussed within Section C – Accountability of this report.

Identified Initiatives

Initiative 1

The Hostplus Board to ensure effective coordination and flow of information between all its Committees. This will be achieved by continuing to:

- *Provide all Committee papers to all members of the Board*
- *Provide the minutes of all Committees to all members of the Board to ensure communication of Committee deliberations*
- *Invite all Directors to attend any Committee meeting.*

Initiative 2

The Board to continue to drive improvements in Board reporting, including adequate tailoring of reports to the Board through the ongoing assessment of the quality of reporting it receives.

Initiative 3

The Board to drive improvements in strategic risk reporting. This will be achieved through the introduction of the GRC system which will drive dashboard reporting.

Initiative 4

Introduction of periodic and structured meetings between Committee members and risk owners to improve understanding and to test that the flow of information to the Board and its Committees is working effectively. Accountable Group Executives will be invited to ARCC and Operations Committee meetings to speak to audit findings, issues and incidents.

Initiative 5

The Operations Committee to ensure that identified operational risks are being reported appropriately to the ARCC

Initiative 6

The ARCC to utilise the GRC system to undertake risk and compliance deep dives into key areas across the organisation.

Initiative 7

The Board to ensure that the natural tension that currently exists at the Board level continues through maintaining the 3:3:3 structure and regular self-assessments and peer reviews.

Initiative 8

The introduction of shared risk KPI's to the Group Executive to ensure the same level of constructive challenge is replicated at this level.

2. Senior Leadership Oversight

Hostplus' structure consists of 6 individual areas:

- Investments
- Risk and Compliance
- Member Services
- Service Operations
- Finance, Strategy and IT
- People, Performance and Culture

These areas are supported by specific business units that sit underneath them. Each area is headed up by a Group Executive. It is these Group Executives along with the CEO that form the Group Executive Team. The CEO retains overall responsibility and delegation for the management of Hostplus' business activities, with the Group Executive team responsible for the development and implementation of business plans which align with the Hostplus strategy.

The Group Executive team meet fortnightly to discuss operational matters including risk and compliance. Each Group Executive is an owner of at least one material risk of the Fund which generally aligns with their area of responsibility.

The Group Executive team is supported by the Heads of departments which also have their own forum that meets on a monthly basis. The Heads of each department also own the risk profile of each of these departments and are expected to update their risk profiles if there are any changes to the business operations.

It is expected that the Group Executives present to the Board and its committees throughout the year on key issues, initiatives and activities within their area of responsibility. This also extends to the Group Executive of Risk and Compliance who reports on all risk and compliance activities of the Fund.

Both of these groups were consulted throughout this process with the Group Executives being interviewed individually and the Heads of each department participating in a facilitated workshop.

2.1. Assessment Insights

The focus of the self-assessment into senior leadership oversight focussed on the level of reporting and information provided to this group, as well as their ability to provide the oversight of risk within the areas. It was identified that whilst the relatively small size of Hostplus as an organisation and the small leadership team had protected the Fund in previous years through the agility to communicate and respond to issues when necessary, the level of risk reporting to the Group Executive was low and almost non-existent at the 'Heads of' level. This was supported by comments made within the workshop that when issues were raised Hostplus typically worked collectively to resolve the problem, however it wasn't until there was an issue that the broader group was made aware through having to respond.

The key themes from this assessment were:

- Implementation of risk reporting to the Group Executive team both as risk owners and as a collective to improve the understanding of risk issues and the control environment.
- Implementation of risk reporting at the 'Heads of' level to ensure cross functional collaboration on issues and control weaknesses.

Risk Reporting

A key theme throughout the interviews and workshops was that participants were aware of risk reporting to the Board, however there was a disconnect between how that reporting was then disseminated throughout the rest of the organisation.

It was also noted that risk owners would like more reporting provided to them in regards to the control environment in their area of responsibility.

These insights have highlighted that whilst risk reporting is happening at the Board level there is a disconnect to what is happening at the levels below this. This is a known issue within the risk team and although they have been improving on the risk reporting across the organisation by ensuring risk is a standing agenda item on meeting agendas, more needs to be done to provide coverage across all levels of Hostplus. This will be helped by the introduction of the new GRC system which will allow individual business units to receive more relevant and timely reporting on their own risk profiles and KRI's.

Identified Initiatives

Initiative 9

Development of relevant and timely risk reporting to both the Group Executive team and the Heads of group. Through the inclusion of a risk section in the monthly operations report presented to the Group Executive team

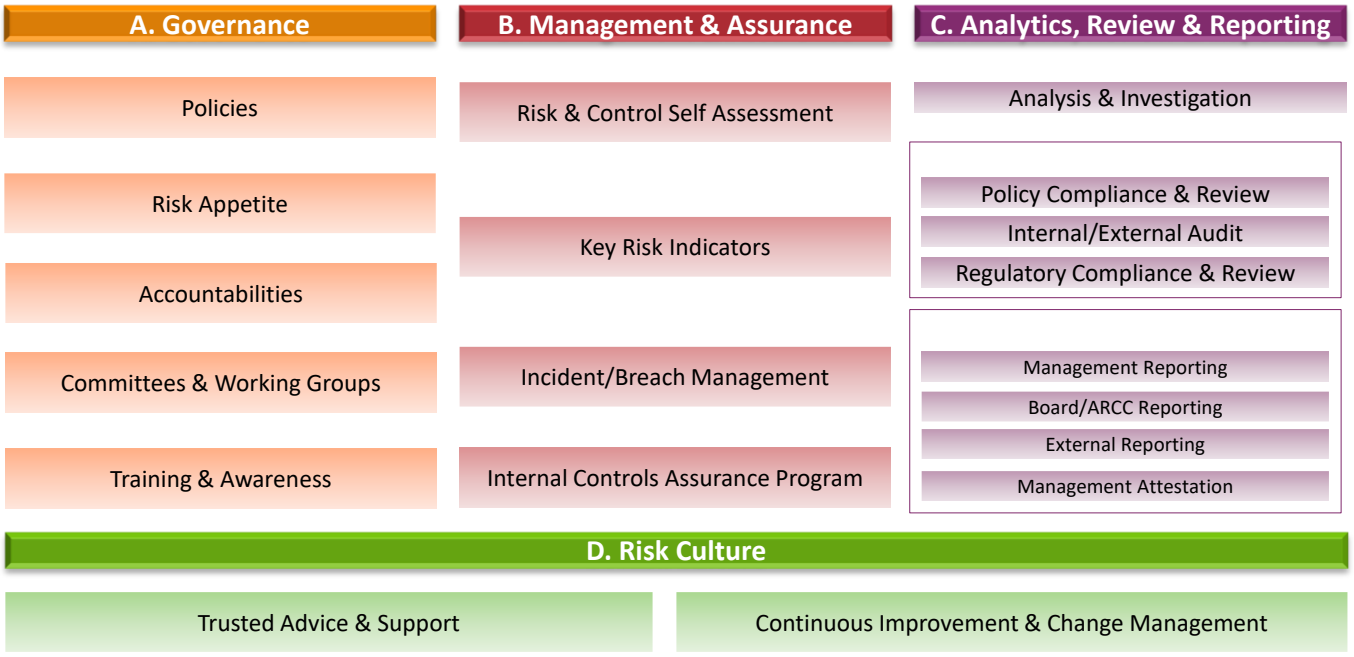
Initiative 10

Creation of a senior leadership risk forum which allows for in depth discussion of operational risks and Hostplus' control environment.

3. Risk Governance

The Hostplus Board recognises that there are risks involved in operating superannuation schemes and that it is impossible to eliminate all risks. The Board retains full responsibility for risk management and the implementation and continuous improvement of a Risk Management Framework that is appropriate to the size, business mix and complexity of Hostplus. The Board does however delegate primary ownership and responsibility for the operational management, within its agreed risk appetite, of its risk practices, policies and controls to the CEO and the Group Executive team. Figure 2 shows Hostplus' Risk Management Framework.

Figure 2 – Hostplus' Risk Management Framework



Hostplus' Risk Management Framework is designed to satisfy the requirements of SPS 220 Risk Management and is effected throughout the organisation through a three lines of defence model. Hostplus' three lines of defence model follows similar general principles as CBA's and is built around the following key elements:

- 1st line – the business owns the risk and must ensure that there are effective and appropriate controls in place to manage the risk in the business.
- 2nd line – the risk and compliance function is responsible for developing policies, processes and systems to promote a consistent approach to risk management and to provide independent challenge to the business.
- 3rd Line – is both internal and external audit and provides independent assurance that the risk management framework is operating effectively.

The three lines of defence model is supported by a suite of risk documentation that details how Hostplus identifies, assesses, manages and monitors risk. This suite of documentation includes:

- Risk Management Framework
- Risk Management Strategy
- Risk Appetite Statement
- Material Risk Register

The Risk Management Framework is soon to be supported by the new GRC system – Riskware, which will allow for the centralised storage of Hostplus' risks, controls, issues and incidents and compliance obligations. Riskware allows for responsibility to be assigned to individuals for risk issues, incidents, and control monitoring. The system will also be used to track and monitor the status of incidents and issues across the business.

As per the requirements of SPS 220, Hostplus undertakes an independent comprehensive review of its Risk Management Framework every three years. The most recent review was completed in June 2016 by KPMG who concluded that Hostplus' Risk Management 'was sustainable to mature'. Another independent comprehensive review is scheduled to be completed in early 2019 with this self-assessment informing areas for future review.

Just prior to, and since the June 2016 comprehensive review there have been significant improvements in Hostplus' Risk Management Framework. The changes are summarised below:

- Resetting of Hostplus' Risk Appetite to categories of risk to provide more clarity to the level of risk the Board was willing to take in each category of risk, including operational risk.
- Introduction of risk appetite principles by the Board to the wider organisation.
- Strengthening of the link between strategy, business planning and risk management.
- Appointment of risk owners to each of Hostplus' material risks.
- Development of business unit risk profiles to ensure a bottom up view and drive accountability through the individual business units.
- Elevation of the risk and compliance function to the Group Executive team reporting directly to the CEO.
- Increased resourcing of the risk and compliance team, including specific roles for AML/CTF and Fraud management and monitoring, and a dedicated monitoring and assurance resource.
- Recent implementation of Riskware, a central system to record all enterprise risks, controls, and compliance obligations.

These improvements were also in addition to the annual risk review the Board undertakes, as well as the continuous improvement initiatives the risk team undertakes. While these activities have materially improved and strengthened Hostplus' Risk Management Framework the current operating environment of the superannuation sector is going through a period of growth and expansion and requires Hostplus to continually review and update its Risk Management Framework to ensure it remains appropriate for the size, business mix and complexity of Hostplus.

3.1. Assessment Insights

The self-assessment of the Hostplus' Risk Governance focussed on the level of implementation of the three lines of defence, the adequateness of Hostplus' risk documentation and the embedment of prudent risk management practices across the organisation.

The key themes highlighted in the self-assessment were:

- Strengthening the implementation and effectiveness of three lines of defence, specifically the effectiveness of the first line.
- Developing more sophisticated risk documentation that reflects Hostplus' size, business mix and complexity.

It was acknowledged throughout the self-assessment process that with the pace and quantity of growth and change that Hostplus' has experienced, and although there have been significant

improvements to the Risk Management Framework, these two areas may have not been developed or matured in conjunction with the rate of growth and change.

Three Lines of Defence

Like most financial service providers Hostplus has adopted the three lines of defence model to manage and monitor its risk management framework. When implementing the model Hostplus gave due consideration to the banking sector and their approach in implementing three lines of defence, this was due to the Hostplus Board recognising that the banking sector was ahead of the superannuation sector in implementing this model. However, it became apparent that given the size of Hostplus embedding line one through existing teams and resources rather than creating a separate line one team was a more appropriate structure for Hostplus.

Initially this was done through appointing 'risk champions' within each line one business unit. These risk champions were to help perform and reinforce line one's responsibilities, however it became apparent that the role of risk champion was too often overlooked for their day to day roles.

In June 2016 the decision was made to elevate the risk and compliance team to the Group Executive team and report directly to the CEO. This drove a change in the approach to three lines of defence. The risk management team developed a risk roadmap that included developing business unit risk profiles, appointing risk owners at the material risk level and strengthening the link between strategy, business planning and risk. This approach enabled a more organic adoption of line one accountability however, it has not been without its own issues with line one and two responsibilities often becoming blurred. Interviewees acknowledged that although there is a strong risk culture of engaging risk some departments did not take true ownership of risk and relied on the risk management team to provide mitigation plans, controls and oversight.

Hostplus has previously recognised the blurring of responsibility between line one and line two and as a result initiated a number of actions to encourage further clarity of responsibility, and to facilitate business unit ownership. These include:

- The introduction of a GRC system which will enable risks, controls, issues and incidents, and action plans to be assigned to individuals.
- A comprehensive risk awareness training plan to ensure clear understanding of the roles and responsibilities of all three lines of defence.
- The introduction of a more robust monitoring and assurance program from line two to drive accountability in the control environment.

It has also been acknowledged that trying to get the balance right between risk expertise and function expertise is difficult within line one and this can sometimes be the driver behind line two performing line one's roles. It has been suggested that where there are high risk areas and a higher level of expertise that specific roles be recruited for, such as an investment risk specialist.

The Hostplus Board acknowledges that as the Fund continues to grow that the three lines of defence model needs to be continually reviewed and refined, this will be achieved through Hostplus' audit program and ongoing reporting to the Board

Risk Documentation

The Hostplus risk documentation outlines how Hostplus identifies, measures and monitors risk. This documentation is reviewed on annual basis, reviewed and endorsed by the ARCC and ultimately approved by the Board.

Through the interview process as well as the workshop with senior leadership it was identified that although there is a known risk culture across the Fund, the risk documentation is viewed as the 'property' of the risk function, and at times could be more sophisticated and accessible. This observation was part of a more encompassing observation on Hostplus' policies in general that they were sometimes not up to date or had different information due to the pace of change making it difficult to keep track of all the changes required across all the Fund policies. This observation also suggests that whilst the Board is clear in its tone and approach to risk, that message may not be reaching all areas of the business if the documentation is not readily accessible.

Through these observations it is clear that more needs to be done in communicating the risk documentation to the rest of the organisation, and also in making it more accessible to the whole organisation by reducing the 'risk language' and using more commonly used business language. This will be achieved partly through the risk awareness training program. This risk management team also needs to do more in ensuring that there is a clear change program in place which includes all policies across the organisation to ensure they remain consistent and up to date.

Identified Initiatives

Initiative 11

Lifting the effectiveness of the first line of defence throughout Hostplus through improving the clarity of roles and responsibilities of line one and line two.

Initiative 12

Increasing the capabilities of line one through further training, understanding of risk documentation, and support with sufficiently skilled resources within high risk areas.

Initiative 13

Organisational wide implementation of the GRC system to help drive accountability within line one.

Initiative 14

Improvement in the communication and dissemination of risk documentation to make it more accessible to all staff.

Initiative 15

Inclusion of policies into Hostplus' change process to ensure they remain up to date and consistent.

4. Issue Identification and Escalation

Hostplus' framework for issue identification and escalation sits within the Risk Management Framework and consists of the following policies:

- Breach and Incident Policy
- Whistleblowing Policy
- Complaints Process
- Compliance Framework

Together these policies allow for the reporting and escalation of issues, incidents and complaints. Hostplus also has an internal and external audit program which, from time to time, identifies issues in certain areas and processes. These findings are reported through to the ARCC on a regular basis.

Breaches and Incidents

The Hostplus Risk and Compliance team manages the breach and incident register for the entire organisation. The Breach and Incident Policy governs the way in which breaches and incidents are reported and managed throughout Hostplus. The majority of breaches recorded are externally reported from the administrator and managed through regular action and mitigation meetings. Breach and incident trends and analysis are reported to the ARCC at each meeting through the compliance update.

Audit Issues

The Finance department manages the internal and external audit program with all audit reports going to the ARCC. Hostplus' internal auditors (KPMG) also attend all ARCC meetings to provide the committee with a complete report of all audit activities within the period. The Finance department also manages an Audit finding tracker, which manages the actions plans, and closure of audit findings, this is also regularly reported to the ARCC. It is the responsibility of individual business units to manage the closure of Audit findings and update the Finance team accordingly.

Whistleblowers

Whistleblowing complaints received via the Hostplus whistleblowing process are managed collectively by People, Performance and Culture and Risk and Compliance, and reported directly through to the Chair of the Board and/or the Chair of the ARCC.

Member Complaints

Hostplus aims to resolve any member issues at the first point of contact, generally through our inhouse call centre. If a member wishes to lodge a formal complaint or the issue is more complex or requires more time it is handled by a dedicated team (Resolutions team) that is part of the broader risk and compliance team.

If members disagree with the outcome of their complaint, they also have the option of an external resolution, by making a complaint to the Superannuation Complaints Tribunal (SCT), since 1 November 2018 this body is the Australian Financial Complaints Authority.

Complaint trends, themes and analysis are currently reported to the ARCC at each meeting and will form part of the agenda for the Operations Committee to ensure that operational decisions have line of sight and consideration of member outcomes.

The resolution team and the operations team also meet regularly to ensure that issues raised through member complaints which may impact other members or have system implications are investigated and actioned appropriately. This meeting is also designed to improve member experience by providing a 'voice of the member' feedback loop to the call centre and to identify areas of friction for members.

4.1. Assessment Insights

The self-assessment has shown that Hostplus has a robust framework to issue identification and escalation which is member focussed and results driven. Participants stated that there was no suppression or fear of reporting issues and that a culture of transparency had been fostered within Hostplus. This is also supported by the Hostplus staff engagement survey which asks questions around the culture of 'no surprises'. It was also noted that the tracking of issues to closure was a robust, disciplined process driven from the Board through the CEO and Group Executive.

Although it was highlighted that the identification and escalation of issues is robust and transparent it was noted that improvements could be made to the visibility of issues and incidents across functions and that sometimes issues were managed within individual departments and lessons learnt were not communicated across different business units. The self-assessment showed that reporting of issues to the Board and committees was in depth, however reporting to senior leadership levels could be improved.

Hostplus' risk and compliance team have also identified that more could be done in regards to testing the internal control environment for control effectiveness. This is supported by the fact that the majority of breaches and incidents captured on Hostplus' register are externally reported. This will help the Board to gain a better understanding of the control environment and allow line two to better fulfil their role in independently reviewing and challenging the business.

Identified Initiatives

Initiative 16

Increased reporting of issues and incidents to senior management through the sharing of audit reports to the Group Executive team, as well as issues and incident reporting to the Heads of forum.

Initiative 17

For the Board to continue to support the development of a more sophisticated monitoring and assurance process for internal control testing as the Fund continues to grow

5. Financial Objectives and Prioritisation

In ensuring completeness of the self-assessment the Hostplus Board has assessed itself against this section of APRA's CBA report as previously mentioned Hostplus does not have the same conflicts between providing shareholder value and customer value that were identified within APRA's report. However, it is noted that whilst Hostplus doesn't have the same conflict there is always a risk of prioritising other initiatives, such as fund growth, over members' best interest. The Hostplus Board ensures that members' interest is front of mind in all decisions and regularly challenges management on expenditure and strategic initiatives.

As Hostplus is a profit to member industry superannuation fund it is bound by legislation that it must act in its members best interest. The Hostplus Board recognises that there are always opportunities to improve and have recently implemented attestations from the Group Executive when strategic projects, financial budgets and key initiatives are proposed to the Board that they are in the members best interest and comply with the Sole Purpose Test.

Section C – Accountability

The Hostplus Board believe that a key foundation to good governance and a strong risk culture is a robust matrix of accountability both down through the reporting lines of an organisation as well as across all areas of an organisation. A robust accountability matrix provides transparent and common understanding within an organisation of where accountability lies within the senior leadership team for any particular part of the organisation.

The Hostplus Board delegates specific authority to the CEO to manage the business through its Board Charter, the CEO has no authority to sub-delegate their authority to other members of the Executive.

The Group Executive and senior leadership accountabilities are managed through their role descriptions, performance management framework and individual Key Performance Indicators (KPI's). These accountabilities are based around delivering on key strategic initiatives, business plans and member outcomes.

The Hostplus Board in undertaking this self-assessment reviewed both the accountability structure and the remuneration structure with the findings detailed in this section.

6. Accountability

The Hostplus Board defines accountability as having actual or effective control for actions, decisions and outcomes within that person's area of responsibility. Within Hostplus this is supported by the organisational structure with the CEO ultimately accountable for the business operations, as delegated by the Board, and the Group Executives accountable for their areas of control and influence.

This type of organisational structure enhances and strengthens the vertical lines of accountability through a business unit but does cause some issues for clear accountability for end to end processes which engage overlapping business units. To counteract this issue the Board and CEO have recently undergone a review of the organisational structure and have aligned functional areas where there are clear interdependencies so as to drive clear ownership of end to end processes.

6.1. Assessment Insights

Although the changes above are helping to provide more clarity, the Board has identified further key themes through this self-assessment:

- Reliance on good culture to drive accountability rather than formal delegations of authority.
- Over-reliance on the Group Executive of Risk and Compliance for ownership and accountability of risk.

Reliance on Good Culture

When undertaking this self-assessment, the Board confirmed that contrary to the issues faced by CBA, Hostplus has a strong culture of accountability driven by its member first ethos. Although there is no delegation of authority below the CEO it was clear that all senior leaders felt accountable, and held to account by the Board, for their area of control.

This is evidenced by a number of processes put in place to ensure that the CEO is completely informed when making decisions and committing Hostplus to certain agreements.

Whilst the Board recognises that this culture is positive it also recognises that this culture drives an over reliance on the CEO. In order to support the continued growth of the Fund, and to formalise what is already a good culture of accountability, Hostplus would benefit from the development of a Fund wide delegation of authority matrix which would provide clarity for all levels of leadership around their areas of control and influence.

Accountability for Risk Management

All participants in the self-assessment showed strong support for the Group Executive of Risk and Compliance and viewed the team as competent and knowledgeable. The previous work that has been completed to enhance the Risk Management Framework was acknowledged with participants agreeing that the risk maturity of Hostplus has improved over the last four years, and that senior leaders were more aware of their risk accountabilities.

Despite these observations, as well as each Group Executive being a risk owner, it was recognized that there is a risk of over-reliance on the Group Executive of Risk and Compliance within the Group Executive team to identify, monitor and manage risk.

It was also identified that the Group Executive KPI's did not capture risk well enough, and that only one Group Executive had a specific KPI of 'no enforceable undertakings'. The Board has recognised that in order to drive collective accountability for risk that it needs to hold all executives accountable for risk management at Hostplus. This will be addressed via initiative 4 – periodic meetings between Committee members and risk owners. It could also be strengthened by the development of individual and collective risk KPI's across the Group Executive team.

Identified Initiatives

Initiative 18

The development of a Fund wide delegation of authority matrix to formalise accountability across Hostplus.

Initiative 19

The development of individual and collective risk KPI's for the Group Executive team.

7. Remuneration

The Hostplus Board delegates many of its remuneration decisions to the People and Remuneration Committee. This Committee is supported by the People, Performance and Culture team and governed by its Terms of Reference and Hostplus' Remuneration Framework. The guiding principals for the Remuneration Framework at Hostplus are:

- simplicity
- consistency
- fairness/equity
- alignment with values
- appropriate risk behaviour
- transparency

The following philosophy also applies to Hostplus' Remuneration Framework:

- remuneration should facilitate the delivery of superior long-term results for the business and promote sound risk management principles.
- remuneration should support the Fund's values and desired culture.
- remuneration should support the attraction, retention, motivation and alignment of the talent we need to achieve our business goals.
- remuneration should reinforce leadership, accountability, teamwork and innovation.
- remuneration should be aligned to the contribution and performance of the business, teams and individuals.
- the remuneration framework places emphasis and consideration on our overall purpose with respect to placing our members financial interests at the outset.

Remuneration for employees at Hostplus is made up of two components:

- Fixed Remuneration – salary and compulsory superannuation paid to all employees.
- Variable Remuneration (CEO, Group Executives and specified non-executive employees only) – short-term incentive (STI) calculated as a percentage of the individuals fixed remuneration; or
- Performance linked incentive – the top 15% of non-executive employees that are recognised as achieving outstanding performance are eligible to receive this incentive.

The People and Remuneration Committee approve all variable remuneration payments and utilise a number of factors to determine the STI payment, including, but not limited to:

- Fund financial and strategic performance.
- Departmental financial and strategic performance.
- individual contribution to team performance.
- individual performance, including alignment with fund values and meeting performance objectives.
- contribution to meeting risk and compliance requirements.

The Board has the discretion to adjust performance-based components of variable remuneration downwards, to zero if appropriate, in relation to persons or classes of persons in circumstances due to Hostplus' capacity to pay such STIs or if such adjustments are necessary to:

- protect the financial soundness of the Fund; or

- in circumstances where there has been an instance of fraud perpetrated by the eligible STI recipient; or
- a serious breach of APRA or ASIC regulations or any breach of other relevant and related legislation; or
- respond to significant unexpected or unintended consequences that were not foreseen by the Board

Performance linked incentives are approved by the CEO upon recommendation by the Group Executive of People, Performance and Culture. Performance linked incentives can range from 8% to 4% of an individuals fixed remuneration.

All employees eligible for either variable remuneration or a performance incentive scheme are subject to performance management assessments in accordance with Hostplus' Performance and Development process.

7.1. Assessment Insights

The Hostplus Board believes that its Remuneration Framework is appropriate given its size, business mix and complexity. In reviewing its application of the Remuneration Framework, the Hostplus Board has effectively applied its guidelines, provided appropriate oversight of remuneration payments and engaged independent advisors to ensure remuneration practices are in line with industry practices.

Through the self-assessment process, it was recognised that risk KPI's across the organisation could be strengthened to provide further clarity on expectations and accountabilities for risk. It was also acknowledged that reliance was placed on overlapping membership of the ARCC and the People and Remuneration Committee to inform decisions about risk behaviours rather than input from the Group Executive of Risk and Compliance. This was determined to be sufficient due to the CEO's input into Group Executive performance as well as the overlapping membership of the committees. It was suggested that with the development of risk KPI's across the business that the Group Executive of Risk and Compliance be engaged to inform senior leadership of any risk issues or incidents that may impact the performance rating of employees below the Group Executive level.

Identified Initiatives

Initiative 20

Development of risk KPI's for all levels and employees of the organisation.

Initiative 21

Engagement of the Group Executive of Risk and Compliance to provide insights into risk issues and incidents when determining performance of employees below Group Executive level.

Section D – Culture

Hostplus' organisational culture is embedded in its industry roots. As a profit to member industry fund its member first culture is a part of Hostplus' DNA. The Hostplus Board, CEO and Group Executive team have revamped the Hostplus values in 2017 to reflect our heritage and our commitment to providing a dignified retirement to our members. These values are:

- We Care – about our work, our members and our colleagues.
- Better Together – we've got each other's backs and we never walk alone.
- Go For It – we are optimistic and focus on solutions, not problems.
- Keep It Real – we are honest, genuine, straightforward and transparent.
- Be Proud – we are proud of who we are and the work we do.

The Hostplus Board recognises that organisational culture, as well as risk culture is more than just values. It is the tone set from the top, the timely response to issues raised, modelling of good behaviours by leadership and the transparent flow of information throughout the organisation as well as to members.

8. Risk Culture

Measuring culture is difficult, measuring risk culture is more so. In order to undertake the self-assessment, the Hostplus Board considered the nine cultural themes listed in APRA's report to help identify key themes or areas for where Hostplus could enhance its risk culture. The inputs into culture were guided by the interviews and workshops, with only two of the nine cultural themes identified.

The following key themes will be discussed within this section.

- Tone from the top.
- Reactive rather than proactive regarding risk.

8.1. Assessment Insights

Participants across all interviews and workshops agreed that there was a known risk culture across the Fund and that all participants felt comfortable engaging with the risk management team. The Hostplus Board recognises that risk culture requires constant attention and improvements can be made to strengthen risk culture across Hostplus and to embed risk into all areas.

Tone from the Top

It was clear from the self-assessment that the Hostplus Board has set a clear tone from the top. Historically the Board has preferred to defer to the CEO for internal and external communications, this was to ensure a consistent voice in terms of messaging. It was viewed that the Board's responsibility was to advise the CEO and to have the CEO be the spokesperson for the Fund. It was clear from the interviews that the voice from the Board was clear and that messaging coming down from the Board, through the CEO was consistent with the Board's views.

Interview participants identified that the Hostplus Board was quick to respond to issues when it became aware of them and ensured timely reporting and closure of mitigation plans from senior management.

The Board recognises that given the current environment in financial services further clarity on their expectations in regards to risk culture will be warranted. In order to achieve this the Board has undertaken a number of initiatives including:

- Continuing to ensure that there is constant challenge to the CEO and Group Executive team around the 'can we versus should we' question, this is also supported by the introduction of the attestations from the Group Executive in regards to members' best interest.
- Introduction of a new material risk 'Failure to maintain Hostplus' member first culture resulting in brand/reputational damage'.

Although the Board has promoted a clear tone from the top it does not receive reporting in regards to how well this is being cascaded to lower levels of the Fund.

Reactive rather than Proactive

It was identified through the Heads of department workshop that the risk culture can sometimes be reactive rather than proactive and that the business can become better in engaging the risk team earlier. This is also supported through the insights identified in regards to the blurring of roles between line one and line two, if line two is sometimes performing line one's role it makes it difficult for line two to be proactive and strategic. The initiatives outlined in Section B – Governance will address this issue of reactivity.

Identified Initiatives

Initiative 22

The Board will continue to promote a clear tone from the top and seek greater reporting on how well this has cascaded below executive management.

Section E – Assessment Initiatives

In this section the Board has summarised its agreed actions as a result of the self-assessment, a lot of these actions are directly linked to, or in support of, already identified initiatives. The next steps of this activity is to develop a plan of implementation of the identified actions, this will be done by the Board in consultation with the CEO and Group Executive team. The implementation plan will be presented to the Board for approval in February 2019. The Hostplus Board envisage that this implementation plan will form the basis of the risk management team strategy going forward and the assessment of its implementation will be included in the comprehensive review of SPS 220 which is due in the first six months of 2019. Ongoing reporting of the progress against the implementation plan will be included in the Board and its Committee's risk reports.

Agreed Actions

Section B – Governance

Role of the Board

Initiative 1

The Hostplus Board to ensure effective coordination and flow of information between all its Committees. This will be achieved by continuing to:

- *Provide all Committee papers to all members of the Board*
- *Provide the minutes of all Committees to all members of the Board to ensure communication of Committee deliberations*
- *Invite all Directors to attend any Committee meeting.*

Initiative 2

The Board to continue to drive improvements in Board reporting, including adequate tailoring of reports to the Board through the ongoing assessment of the quality of reporting it receives

Initiative 3

The Board to drive improvements in strategic risk reporting. This will be achieved through the introduction of the GRC system which will drive dashboard reporting

Initiative 4

Introduction of periodic and structured meetings between Committee members and risk owners to improve understanding and to test the flow of information to the Board and its Committees is working effectively. Accountable Group Executives will be invited to ARCC and Operations Committee meetings to speak to audit findings, issues and incidents.

Initiative 5

The Operations Committee to ensure that identified operational risks are being reported appropriately to the ARCC

Initiative 6

The ARCC to utilise the GRC system to undertake risk and compliance deep dives into key areas across the organisation.

Initiative 7

The Board to ensure that the natural tension that currently exists at the Board level continues through maintaining the 3:3:3 structure and regular self-assessments.

Initiative 8

The introduction of shared risk KPI's to the Group Executive to ensure the same level of constructive challenge is replicated at this level.

Senior Leadership Oversight

Initiative 9

Development of relevant and timely risk reporting to both the Group Executive team and the Heads of group. Through the inclusion of a risk section in the monthly operations report presented to the Group Executive team

Initiative 10

Creation of a senior leadership risk forum which allows for in depth discussion of operational risks and Hostplus' control environment.

Risk Governance

Initiative 11

Lifting the effectiveness of the first line of defence throughout Hostplus through improving the clarity of roles and responsibilities of line one and line two.

Initiative 12

Increasing the capabilities of line one through further training, understanding of risk documentation, and support with sufficiently skilled resources within high risk areas.

Initiative 13

Organisational wide implementation of the GRC system to help drive accountability within line one.

Initiative 14

Improvement in the communication and dissemination of risk documentation to make it more accessible to all staff.

Initiative 15

Inclusion of policies into Hostplus' change process to ensure they remain up to date and consistent.

Issue Identification and Escalation

Initiative 16

Increased reporting of issues and incidents to senior management through the sharing of audit reports to the Group Executive team, as well as issues and incident reporting to the Heads of forum.

Initiative 17

For the Board to continue to support the development of a more sophisticated monitoring and assurance process for internal control testing as the Fund continues to grow.

Section C – Accountability

Accountability

Initiative 18

The development of a Fund wide delegations of authority matrix to formalise accountability across Hostplus.

Initiative 19

The development of individual and collective risk KPI's for the Group Executive team.

Remuneration

Initiative 20

Development of risk KPI's for all levels and employees of the organisation.

Initiative 21

Engagement of the Group Executive of Risk and Compliance to provide insights into risk issues and incidents when determining performance of employees below Group Executive level.

Section D – Culture

Risk Culture

Initiative 22

The Board will continue to promote a clear tone from the top and seek greater reporting on how well this has cascaded below executive management.