FIFTEENTH PARLIAMENT OF SINGAPORE

First Session

REPORT OF THE PUBLIC ACCOUNTS COMMITTEE

Parl. 3 of 2026

Presented to Parliament on

10 February 2026

PUBLIC ACCOUNTS COMMITTEE

Members

Ms Jessica Tan Soon Neo (Chairman)

Mr Foo Cexiang

Mr Jackson Lam

Mr Victor Lye

Mr Saktiandi Supaat

Mr Dennis Tan Lip Fong

Mr Alex Yeo

Mr Yip Hon Weng

CONTENTS

REPORT OF THE PUBLIC ACCOUNTS COMMITTEE

Overview

1 The Public Accounts Committee considered the Report of the Auditor-General for the Financial Year 2024/25 and deliberated on the observations in the Report. The Committee acknowledges the efforts taken by public sector agencies to address the lapses observed by the Auditor-General's Office (AGO). These efforts include strengthening processes and procedures, leveraging technology and analytics, and building capabilities and competencies of their officers in relevant areas.

2 The Committee discussed the following key areas highlighted in the Report of the Auditor-General:

a. Weaknesses in procurement and contract management;

b. Weaknesses in management of revenue; and

c. Management of research and development (R&D) grants at the Agency for Science, Technology and Research (A*STAR) and the National Research Foundation (NRF), where AGO found lapses as well as good practices that could be useful for public sector learning.

3 AGO observed weaknesses in procurement and contract management across several agencies. These included tender evaluations not carried out in accordance with published evaluation criteria, payments made for goods or services that did not comply with contractual requirements, and inadequate oversight of star rate assessments. The Committee was of the view that agencies should strengthen their oversight of project consultants, contractors and private sector partners, and enhance staff competencies in conducting the necessary checks – to ensure that agencies are able to assess and critique consultants' recommendations. When administering complex Public-Private Partnership (PPP) projects, agencies must retain adequate technical expertise throughout the project life cycle, and not just at the tender evaluation stage.

4 The Committee noted that the agencies have since taken action to recover overpayments where applicable. They have also improved procurement and contract management by strengthening frameworks and procedures, implementing digital tools to reduce human error, and enhancing staff competencies through training and capability building programmes.

5 AGO also noted weaknesses in the management of revenue in two agencies. These included collection of fees and concessions granted not prescribed in law and public monies not properly accounted for. The Committee was of the view that there should be stronger accountability and oversight over the monies managed. The Committee noted that the agencies have taken remedial action to address these lapses. The Maritime and Port Authority of Singapore (MPA) has since regularised the fees collected and concessions granted through legislation or by exercising its statutory power of waiver. The Ministry of Foreign Affairs (MFA) has enhanced its systems and processes to verify the returns needed to properly track and account for the visa fees collected by Honorary Consuls-General/Honorary Consuls (HCGs/HCs).

6 AGO conducted a thematic audit on Research, Innovation and Enterprise (RIE) 2025 R&D grants managed by A*STAR and NRF. Lapses found included deviation from funding policy, lack of independence in endorsement of project and payment documents, inadequate documentation, and human and system errors in processing of grant funding. The Ministry of Trade and Industry (MTI) informed the Committee that A*STAR has since obtained covering approvals, updated its standard operating procedures (SOPs) and reinforced training and guidance to officers. The Prime Minister's Office (PMO) informed the Committee that NRF has since addressed its documentation and approval gaps, revised its SOPs to better clarify policies, and established an in-house Internal Audit (IA) unit to strengthen risk management.

7 The Committee also acknowledged the good practices put in place by both agencies, including their risk-based approaches to grant management and the use of technology like data analytics and dashboards to enhance compliance and operational efficiency. These tools enabled more efficient monitoring of grant statuses, tracking of budget utilisation and review of user activities. The Committee noted the update from the agencies that new grant system features with artificial intelligence (AI) integration, simplified workflows and automated rules would also be rolled out progressively to strengthen existing controls.

Broader Issues

8 The Committee also discussed broader issues which could impact spending, financial governance and controls across the public sector, namely:

a. Procurement, Contract Management and Grant Administration;

b. Revenue Collection and Accounting;

c. Internal Audit Capabilities;

d. IT Controls and Cybersecurity Governance; and

e. Cross-agency Data Sharing and Use of Data Analytics and Artificial Intelligence.

9 In addition to the written responses from the ministries, the Committee convened hearings on 21 January 2026 and called upon the Permanent Secretaries from the Ministry of Finance (MOF) and the Ministry of Digital Development and Information (MDDI) and Smart Nation Group (SNG) to provide oral clarifications and elaboration of their written responses. The areas discussed at the hearings included MOF's central initiatives to improve financial governance, build capabilities and incorporate risk management into financial processes, balancing risk mitigation with compliance costs. The hearings also looked at MDDI's and SNG's roles in addressing cybersecurity risks and encouraging cross-agency data sharing, analytics and AI adoption in the public sector. The focus was on strengthening competencies of officers and resilience of government systems and digital services while ensuring accountability.

Procurement, Contract Management and Grant Administration

10 The Committee noted that lapses in procurement, contract management, and grant administration continue to be recurring findings by AGO. The Committee asked MOF about the root causes underlying these recurring findings and the implementation status of central initiatives to address them.

11 MOF informed the Committee that the recurring findings stem from a combination of people and process factors, such as non-compliance by individual officers arising from knowledge gaps or prioritising operations over process or documentation, inadequate controls over and monitoring of contractors' compliance with policies and procedures, inadequate management of conflict-of-interest situations, and inadequate documentation. There is also a need to strengthen the capabilities of consultants such as Quantity Surveyors who play a key role in public sector procurement and contract management.

12 The Committee noted MOF's multi-pronged approach to strengthen controls while balancing risk mitigation and compliance costs. With a focus on uplifting competencies, central initiatives to build capabilities in procurement and contract management include compulsory e-learning module for officers new to procurement functions, establishment of the Finance and Procurement Academy, issuance of good practice guides, and designation of JTC as the Building and Infrastructure Centre of Excellence to support agencies lacking such capabilities. A Taskforce for Architectural and Engineering Consultants has been established to strengthen the built environment sector's talent pipeline and firm capabilities. Other measures to uplift industry competencies include introducing the Accredited Professional Quantity Surveyor (APQS) scheme and anti-fee diving measures to prioritise quality over cost in procurement evaluation. MOF has also been tracking agencies' performance in managing construction contracts. It reported improvement in timely approval of variation orders from about 70% in 2018 to above 90% in 2023. New initiatives include digitalising procure-to-pay processes, convening of an AI Workgroup among procurement teams, and exploring AI tools to provide guidance and process validation in procurement.

13 The Committee also asked MOF whether agencies have sufficient capabilities to exercise proper oversight of PPP projects that involve complex financing models or terms. MOF informed the Committee that while PPP projects are more complex, the process and fundamentals of evaluation and management of such contracts are similar to those using other procurement approaches. Agencies are required to assess whether they have the necessary internal capabilities and may tap on the expertise of external consultants and advisers if needed. The Committee was of the view that agencies should assess whether they have the requisite internal capabilities not just at the procurement and tender evaluation stages, but throughout the project lifecycle. MOF informed the Committee that to support agencies on procurement processes for complex or nascent projects, it has established a Commercial Advisory Team. It is also encouraging agencies to support their procurement officers undertaking infrastructure projects to obtain APQS certification, and examining whether to require the engagement of accredited Quantity Surveyors for larger projects.

14 For grant administration, MOF regularly reviews and updates its central guidance, incorporating good practices and learning points from AGO's annual audit observations, to ensure that it remains relevant and addresses emerging risks. It has also established a Grants Management Committee with sectoral and domain leads. Examples of central initiatives introduced include the Fraud Detection Platform, a DocAnalytics document analysis tool, and

an intel-sharing network covering over 350 officers from 40 agencies. All grant sectors have attained foundational and intermediate levels of maturity in the grants administration capability-building roadmap for the areas of data analytics and systems, and fraud detection and investigation. They are working towards attaining the advanced level of maturity. Recent initiatives include the issuance of a Grant Risk Management Guide and red-teaming exercise piloted with the Commercial Affairs Department and the Inland Revenue Authority of Singapore for selected grant schemes before roll-out of the schemes or enhancements.

Revenue Collection and Accounting

15 The Committee noted several audit observations relating to revenue collection and accounting. It asked MOF about the measures taken to ensure that agencies collect fees and provide concessions with the necessary legal authority, and the guidance and oversight that MOF provides to ensure agencies properly account for public monies collected overseas, or through overseas partners.

16 MOF informed the Committee that agencies are responsible for ensuring fees collected and concessions provided are prescribed in law as appropriate. MOF sets central rules and policies, and works with agencies to implement their fees and charges. MOF has been strengthening oversight through enhanced senior leadership engagement and regular policy reviews to improve whole-of-Government (WOG) compliance with legal and administrative requirements.

Internal Audit Capabilities

17 The Committee noted MOF's multi-year transformation efforts to restructure IA, digitalise audit processes and deepen public sector IA capabilities, spearheaded by the Accountant-General's Department (AGD). The Committee asked MOF for an update on its central initiatives and the platforms and mechanisms through which IA functions across public sector share best practices and learn from one another.

18 MOF informed the Committee that AGD's initiatives include appointment of Group Chief Internal Auditors (GCIAs) in Ministries, progressive onboarding of agencies to the central Audit and Governance Enterprise Management System, issuance of revised WOG IA Manual aligned with Global Internal Audit Standards, and conduct of IA Foundation Programme with a Middle Management Programme under development for commencement in FY2026. AGD also issued the first annual WOG Central Guidance for IA in July 2025, which emphasises governance of the IA function and the value of moving towards more upstream advisory to identify and mitigate risks early. These initiatives are supported by regular knowledge sharing through quarterly GCIA meetings, annual IA Round Table and IA Community Day. The inaugural Governance Week was held in October 2025 to build WOG awareness on governance concepts and risk management.

IT Controls and Cybersecurity Governance

19 The Committee observed that audit findings concerning weaknesses in privileged access management have been recurring over the years. The Committee asked MDDI and SNG

about the implementation of privileged access management framework and initiatives to address such systemic issues.

20 MDDI and SNG informed the Committee that they manage the Government's Information and Communications Technology and Smart Systems through partnership with agencies. At the policy level, MDDI and SNG establish broad WOG governance frameworks via the Government Instruction Manual (IM) and related Circulars. The rules and standards set out in these documents balance the need for standardisation across the public sector with flexibility for agencies to customise solutions to their specific contexts. At the operational level, MDDI and SNG empower agencies through education, tools and capability development, with the Government Technology Agency (GovTech) deploying approximately 1,700 officers across 56 agencies, including Chief Information Officers (CIOs), Chief Information Security Officers (CISOs) and IT delivery teams. MDDI and SNG are enhancing their digital competency framework to increase agencies' capabilities, starting with leadership engagement from Permanent Secretaries to Directors to raise awareness of the importance of technology in agencies' operations and the associated pitfalls.

21 The guiding principle is that while MDDI and SNG establish baseline standards, agencies, who are most familiar with their own policy imperatives and operational contexts, retain ultimate accountability for their systems and can determine the appropriate tools and processes to meet these standards. At the system level, MDDI and SNG have specified baseline controls for privileged account management that all agencies must implement, including account inventories, multi-factor authentication, monthly reviews and proper logging. Requirements are tiered based on system criticality, with GovTech conducting annual audits to ensure compliance. Agencies are required to remediate any gaps identified within approved timeframes.

22 MDDI and SNG acknowledge that agencies' heavy reliance on manual processes for privileged account management makes this area more prone to human lapses. They have introduced automation tools, such as the Central Accounts Management and Automated Baseline Log Review, to automate user account and access rights management and review, although limitations remain in their coverage and effectiveness. They plan to extend additional privileged account management controls to higher-risk systems, enhance training programmes and review policies to improve tracking and management of privileged accounts.

23 The Committee noted that agencies' adoption of automation and modern tools is constrained by "tech debt" arising from legacy systems and outdated codes, which can increase vendor dependency, raise costs, complicate integration and heighten security risks. Long-standing policies and practices also need to change to enable effective digital transformation. Given the many IT systems in the public sector, it will take time to bring all the systems up to date. MDDI and SNG are thus partnering agencies to identify and prioritise the more critical systems for modernisation first through the Ministry Family Digitalisation Programme, with support from GovTech.

24 The Committee also asked MDDI and SNG if they have considered mandating regular independent cybersecurity audits for mission-critical government systems. MDDI and SNG informed the Committee that a government system may already be subject to between three and four different independent audits, depending on system criticality.

Cross-agency Data Sharing and Use of Data Analytics and Artificial Intelligence

25 The Report highlighted the potential for greater use of data analytics and data sharing among agencies to enhance detection of irregularities and operational insights. The Committee asked MDDI and SNG about their approach to facilitating data sharing and enabling agencies to access relevant data for analytics, operational improvements and risk management.

26 MDDI and SNG informed the Committee that they have established a comprehensive WOG data governance framework through the Government IM, enabling effective data management and sharing while maintaining high data protection and security standards. The framework sets out detailed policies and requirements governing the entire data lifecycle, roles and responsibilities of data requestors and providers, and guidelines for data sharing. This helps ensure data is fit-for-purpose and improve interoperability across agencies.

27 The Government Data Architecture (GDA), introduced in 2019, provides a shared technical foundation for data management and sharing across the public sector, with 40 agencies designated as Single Sources of Truths and four designated Trusted Centres processing core data to ensure it meets baseline standards and consistency. The catalogue of all core data is made discoverable to all agencies. The GDA has significantly improved data sharing across WOG, with 99% of core data requests now fulfilled within seven days.

28 As part of the GDA, central platforms have been developed to facilitate secure data sharing and data exploitation within Government. DataHive, launched in August 2024, is the internal WOG data discovery and access platform that enables users to seamlessly search, request and access Government-owned datasets, and provides users with a set of data analytics tools. It currently serves more than 80 agencies and supports 7.9 million system queries per month on average.

29 The Committee also asked MDDI and SNG about WOG AI adoption and how MDDI and SNG promote the adoption of AI and emerging technologies across agencies. MDDI and SNG informed the Committee that they have observed an increasing use of AI across agencies to enhance productivity. For example, about 80% of the 150,000 public officers have used Pair Chat, the Government's general use chatbot, for general productivity tasks, and over 9,000 officers use Transcribe, an AI-powered transcription tool, every month to transcribe meetings across multiple languages. In total, over 20,000 bots have been created to tackle specific tasks. Beyond the use of AI for routine tasks, more than half of all agencies leverage AI to enhance public service delivery through prediction, personalisation, anomaly detection and automation.

30 MDDI and SNG highlighted that successful AI adoption across WOG requires a strong partnership between them and agencies, with a support framework encompassing AI governance structures, strong digital foundations, capability development and encouraging leadership commitment. With regard to accountability and risk management, the Government seeks to gain practical familiarity with new technologies and monitor global developments before introducing regulation. Accountability can be considered across three dimensions – policy, operational and system. Within this context, the WOG AI governance framework emphasises agencies' responsibility for their own AI use cases, while maintaining central oversight of 'high-risk' use cases, and emerging areas. MDDI and SNG facilitate impactful AI deployment through good quality data sharing access, central products on scalable platforms, and good product practices.

31 Initiatives to strengthen capability building include mandatory AI literacy training for all public officers, specialised programmes for public service leaders, and knowledge sharing initiatives like Lorong AI, which fosters collaboration between public sector policymakers and AI practitioners, academia, and industry.

32 From the replies given by and discussions with the agencies, the Committee was assured that the Government has adopted a systematic, multi-pronged approach to address the complex challenges and remains committed to strengthening public sector governance. The Committee recognised that while agencies are taking swift action to address the lapses, sustained improvements in governance systems and institutional capabilities are long-term endeavours. Such transformation requires patience, continued investments, and commitment from all levels in the public sector. It also requires the support of the industry ecosystem, in terms of responsible and capable consultants, contractors and vendors in delivery. The Committee would like to emphasise the following:

a. **Supervisory Oversight.** Many of the lapses are not about lack of rules but about inadequate supervision and oversight. Hence, corrective actions should strengthen supervisory oversight and not rely solely on tighter SOPs or training at the officer level.

b. **Capability Building.** Beyond upskilling existing officers, the Government must continue to focus on attracting, integrating and retaining talent, and providing good career pathways. This is particularly important in areas with capability gaps and in responding to emerging challenges and technological developments. The Committee also noted the importance of a competent external ecosystem of consultants, contractors and vendors, and acknowledged the Government's efforts to uplift competencies in key industries.

c. **Procurement and Contract Management.** Agencies should strengthen their oversight of project consultants, contractors and private sector partners, and build capabilities in conducting proper due diligence and contract monitoring. For complex projects, such as PPP projects, agencies must also regularly assess and ensure that they have the requisite expertise to manage these arrangements effectively throughout the project lifecycle.

d. **System Modernisation.** It is critical that the public sector modernises its legacy IT systems, policies and practices for operational effectiveness and security. However, this requires considerable time and resources. The Committee supports the Ministry Family Digitalisation Programme as a systematic approach to identify digital priorities and develop modernisation roadmaps to strengthen system resilience, taking a phased approach. Agencies should also endeavour to develop internal capabilities over time, especially for the maintenance and management of critical systems.

e. **Data Analytics and AI Adoption.** To improve operational insights and risk management, agencies should continue to enhance their use of data analytics and AI solutions. Agencies should ensure that officers receive appropriate training to develop necessary skillsets, take accountability for their specific AI use cases, and adhere to WOG governance frameworks, while central oversight is maintained for high-risk applications.

f. **Risk-based Approach.** Given the scale and complexity of operations, it is neither feasible nor cost-effective to eliminate all errors. Agencies should therefore adopt a risk-based approach to control design and implementation, focusing resources on higher-risk and material areas. Controls should be proportionate, targeted, and periodically reviewed to ensure continued effectiveness and operational efficiency, with risk assessments properly documented. As part of sound risk management, agencies should also be given sufficient time to build fit-for-purpose systems and implement controls to safeguard against potential risks before rolling out new schemes or enhancements.

g. **Partnership between Central and Individual Agencies.** The Committee acknowledged that addressing recurring issues rooted in people, system and process factors requires strong partnership between central agencies and individual agencies. The Committee recognised the comprehensive efforts undertaken by MOF, MDDI and SNG in strengthening accountability and WOG capabilities through initiatives such as establishing governance frameworks, providing central expertise where gaps exist, facilitating digitalisation, and adopting a systematic approach towards capability building. While these central agencies set overarching frameworks and provide support, individual agencies retain ultimate accountability for their own operations and financial governance. They must abide by the central frameworks, leverage the support provided, and take ownership of building capabilities and putting in place the processes that are appropriate for their specific contexts. Their feedback and experience on the ground should also shape the policies and the support provided by the central agencies.

33 The Committee's enquiries and the agencies' responses, as well as responses from MOF, MDDI and SNG to the broader issues, are discussed in the following sections.

Committee's Enquiries and Responses from Ministries

A. Observations in the Report of the Auditor-General for the Financial Year 2024/25

34 The Committee deliberated on the audit observations raised in the Report of the Auditor-General for the Financial Year 2024/25. The Committee asked the respective agencies to address the following questions:

a. What are the root causes of the lapses and what are the further follow-up actions taken/to be taken to address these lapses?

b. What are the Ministry's / Statutory Board's / agency's plans to address the underlying weaknesses and lapses found, including through capability building, enhanced risk management and ensuring compliance with policies, procedures and other requirements?

Ministry of Education

35 The Ministry of Education (MOE) informed the Committee that the lapses in administration of Post-Secondary Education Account (PSEA) withdrawals were attributed to the reliance on PSEA members to authorise withdrawals and identify discrepancies based on the statements sent to them. This is on the premise that PSEA funds belong to the members.

36 On the outcome of checks on past duplicate withdrawals, MOE reviewed withdrawal transactions amounting to $62.8 million from 185 Training Providers (TPs) over the past six years and found that:

a. 600 withdrawal transactions were duplicates that had been refunded by TPs through their own verification process prior to the review; and

b. 54 withdrawal transactions, totalling $23,000, were further identified as duplicates. Of these, 52 have been refunded and the remaining will be refunded by 31 December 2025.

37 To address the lapses, MOE has revised its SOPs to provide clearer guidance to TPs on what constitutes excess withdrawals warranting refunds. The revised SOPs were disseminated to the TPs in August 2025.

38 Several actions have been taken to strengthen oversight and prevent excess withdrawals. From 2026, MOE will require TPs to declare annually that PSEA funds withdrawn and paid to them in the past year were utilised as intended and that any refunds were made promptly. This will serve as a reminder to prevent inadvertent errors by TPs. The declaration will be subject to regular selective audits to be commissioned from 2026. The audits are independent of the annual financial audit of the Post-Secondary Education Fund, specifically to verify the TPs' PSEA withdrawal and refund processes, and identify instances of excess withdrawals that have not been refunded.

39 MOE is developing a new system to replace the current PSEA system by end FY2026, which will incorporate a revised withdrawal process and measures to minimise withdrawals requiring refunds. Past withdrawals, with the same course and amount, will be flagged for PSEA members' attention before new withdrawals are authorised, and TPs will be required to submit members' attendance before funds are disbursed to them.

Ministry of Foreign Affairs

40 For the observation on visa fees not accounted for as Government revenue, the Ministry of Foreign Affairs (MFA) informed the Committee that the fees collected by HCGs/HCs are determined by Singapore and published in the Diplomatic and Consular Officers (Fees) Order 2012. MFA's policy has been to allow HCGs/HCs to retain and use the fees collected to defray their operating expenses. HCGs/HCs are not MFA employees but rather citizens of foreign countries who provide services for Singapore on a voluntary basis with no remuneration. They represent Singapore in cities and countries where it is not feasible to establish a resident diplomatic mission.

41 MFA acknowledged that there were lapses in the documentation of the fees collected. While MFA required HCGs/HCs to submit statements of account for visa fees collected and expenditure incurred, there were lapses in communication of instructions and follow-up. MFA has since implemented a system to verify the number of visas issued by each HCG/HC. Beyond the existing quarterly performance reports, MFA now requires HCG/HCs to also submit their revenue and expenditure returns on a half-yearly basis, with the first submission by FY2025. In addition, MFA is establishing a digital submission system for HCG/HCs to provide their returns. All submissions will be stored in MFA's recently upgraded digital knowledge repository system and tracked to facilitate follow-up with the HCGs/HCs.

Ministry of Home Affairs

42 On the observation regarding lapses in management of contract for renovation of office space at the Home Team Science and Technology Agency (HTX), the Ministry of Home Affairs (MHA) informed the Committee that the root causes were as follows:

a. Approvals not obtained before commencement of contract variations: There was inadequate follow-through on documentation, although approvals for the variation works were obtained from the approving authority during project progress meetings.

b. Inadequate assessment of cost reasonableness of star rates used, and contractor's claims not properly verified before payment certified: Most of the identified lapses pertained to works carried out before March 2023, when HTX's Request for Variation Orders (RVO) process did not incorporate the methodology for star rates cost assessment provided in the Government IM on Procurement. This also led to inaccurate certification of payments.

c. Inadequate checks on consultant's cost assessment: The current risk-based approach of 10% sampling checks on the cost reasonableness assessment was insufficient to uncover the identified discrepancies.

d. Delay in actions taken to terminate contract with non-performing contractor: There was a need to carry out due diligence to ensure legitimate grounds for termination. HTX had decided against termination because the contractor was still working on defect rectifications, despite slow response times. However, the monitoring efforts by the project management team and senior management to ensure contractor compliance were not properly documented.

43 To address the lapses, HTX has strengthened its process workflows and included it as a standing item for project progress meetings to track approvals and document key decisions. These enhanced workflows and procedures, and reminder to maintain proper records have been shared with HTX Building & Infrastructure (B&I) Division officers and Home Team officers at the annual B&I Community of Practice session in June 2025. These were reinforced through subsequent internal sharing sessions, which was last conducted in October 2025.

44 Since March 2023, HTX has formally integrated the Government IM methodology for assessing star rates into its RVO process. Consultants must now provide cost assessments for star rate items before seeking Project Director's approval. Standardised variation order templates have been adopted to serve as checklists on Government IM guidelines for the management of both variation orders and star rate items.

45 To identify payment claim anomalies, HTX plans to expand its risk-based sampling checks by stratifying payments into categories, such as Mechanical & Electrical works, Builder's works, and specialist systems, followed by verifying valuation methods in RVO forms, and examining supporting documentation for completeness and accuracy. An HTX working group has been formed to develop the sampling check principles and guidance, with a trial to be conducted in January 2026, before the rollout of the revised checks for contract variations and payments in March 2026.

46 MHA will focus on capability building, technology adoption, and enhanced risk and audit management to address the underlying contract management weaknesses. On capability building, HTX has institutionalised milestone training programmes since 2022, incorporating AGO findings into their Basic Project Management course and Contract Management course. The MHA Risk Management and Audit Group has also reinforced awareness of contract management lapses reported by AGO to Home Team officers via various meetings and circulars throughout late 2025.

47 HTX will leverage technology and develop a centralised digital workflow to automate payment anomaly detection and strengthen verification checks, including star rates assessment and application of correct contractual rates. The Minimum Viable Product will be trialled by the second quarter of 2026, with further enhancements planned thereafter. On enhanced risk and audit management, the HTX Audit Division will track rectification progress and report to HTX and MHA oversight and governance bodies. Additionally, HTX has engaged external auditors to audit B&I projects in FY2025 and FY2026, focusing on contract management and payment for significant MHA development projects.

48 HTX has strengthened oversight of consultants and contractors through several measures. Newly appointed consultants and contractors are briefed during project kick-off meetings on the need to adhere to Government procedures. Additionally, tracking of key project milestones and approval timeliness has been embedded into the agenda for regular progress meetings. Specific to the renovation contract lapses, HTX engaged with the consultant's senior leadership in July 2025 to address performance shortfalls and recovered the excess payment to the contractor.

49 The consultant also presented to HTX their digitalised project administration system to enhance project management for other projects under their purview on 29 December 2025. This system serves as a centralised repository for project documentation, streamlines project management processes and strengthens governance throughout the project life cycle, including areas such as design and tender documentation and variations management. It also digitalises the variations workflow and approval process and automates email notifications for outstanding tasks and pending approvals. Following the presentation, HTX has begun collaborating with the consultant to conduct a trial implementation on one project in phases, with the first phase planned for Q2 2026, before potentially rolling out for all construction projects.

Ministry of Law

50 The Ministry of Law (MinLaw) informed the Committee that the lapses regarding investment of Companies Liquidation Account (CLA) monies without liquidator's consent at the Insolvency and Public Trustee's Office (IPTO) arose due to the erroneous impression that such investments were permissible under the Centralised Liquidity Management (CLM) framework even in the absence of a liquidator's request.

51 MinLaw has implemented safeguards to prevent the investment of funds without liquidators' authorisation. A new investment framework took effect on 28 April 2025, ensuring that CLA monies are only placed in bank fixed deposits upon liquidators' requests. Additionally, the CLA was delinked from the CLM framework on 3 July 2025. Moving forward, MinLaw's Finance division will seek legal advice before implementing any significant changes to the investment framework, ensuring that changes comply with relevant legislation.

52 The interest earned from the investment of CLA monies without liquidator's consent has been credited to the Consolidated Fund since the CLA came under the CLM framework in April 2019. This mirrors the arrangement that would have applied had liquidators not consented to investment, where the monies would have remained in the current account with interest from daily balances transferred to the Consolidated Fund. As there was no financial loss to the creditors and stakeholders of the companies, no refunds will be made to the affected companies.

53 For the observation on weaknesses in controls over case processing systems at IPTO, MinLaw informed the Committee that it was attributed to the officer's lack of awareness that accessing his parents' case accounts in the Public Trustee's Office (PTO) case processing system constituted improper use. He had no fraudulent intent and was attempting to test whether certain system-generated notifications would be triggered as per design in the newly implemented system.

54 Several measures have been implemented to prevent and detect future unauthorised system actions. All PTO officers have been reminded not to conduct system testing using actual cases, and that proper testing should be done in a test environment with system vendor's assistance. Quarterly audits of system logs were also introduced with effect from 1 April 2025. To enhance its risk management, IPTO has included the number of unauthorised system actions as a key risk indicator for ongoing monitoring. These checks have not revealed any anomalies. IPTO officers have been informed of the quarterly audits, and brown bag sessions are planned to remind officers not to access systems without authorisation or perform unauthorised actions.

Ministry of Manpower

55 On the observation on weaknesses in management of most privileged operating system (OS) account (i.e. "root" account), the Ministry of Manpower (MOM) informed the Committee that the root causes and follow-up actions were as follows:

a. Inappropriate command granted to OS administrators: There were inadequate protocols to prevent unauthorised changes to the "root" account password by OS administrators. MOM has since adjusted the OS administrator commands to align with updated protocols preventing password changes to the "root" account, and executed a change of all affected server "root" account passwords as a precaution. Moving forward, MOM will strictly adhere to the Government Technology Agency (GovTech)'s guidance regarding servers' security and policy settings, with any deviations requiring Agency CISO's review before implementation. Additionally, MOM has strengthened its SOPs to staff and vendors, to include explicit password change controls, regular reminders to OS administrators, and enforce the use of "root" account for only emergency situations with approval from the IT management team.

b. Non-compliance with MOM's security guide for "root" access: This was a result of staff oversight where the security settings were not reconfigured after a pre-approved troubleshooting session on 21 August 2024 that temporarily permitted remote access. The settings were reconfigured on 22 October 2024. To prevent recurrence, MOM enhanced its processes on 6 March 2025 to require an independent verifier to review security setting changes and ensure temporary modifications are promptly reversed.

c. Inappropriate use of "root" account and password of "root" account not changed after each use: A staff member did not adhere to the established guidelines governing the use of the "root" account for convenience. Disciplinary action has been taken to send a stern message of deterrence against the violation of security practices.

d. Inadequate reviews of activities carried out using "root" account: There was a gap in MOM's review process. MOM has since enhanced the review process to include all activities performed by both direct "root" account logins and "SU root" activities to allow detection of any unauthorised activities.

56 In addition to the above, MOM has updated ministry-wide practices, including SOPs for log reviews and security hardening guidelines, across all systems by June 2025, and conducted an internal review of IT systems. Findings were shared with business stakeholders at various committee meetings to ensure understanding of risks and ownership of IT security. To reinforce awareness, all IT staff were briefed on 6 March 2025 about proper adherence to policies and procedures, specifically restricting "root" account use to emergency situations only. This guidance will be integrated into onboarding and annual refresher training. To strengthen compliance and oversight, for mission-critical systems, internal audits are conducted at a higher frequency of every 2 years, and vulnerability assessment penetration tests are conducted every 12 months and before major releases, with the results presented to Audit Committee. To boost independence and capability of IT audits, IT audit management has been transferred to MOM Internal Audit in FY2025 with support from GovTech Shared Services.

Ministry of Sustainability and the Environment

National Environment Agency

57 For the observation on failure to monitor compliance with requirements in project agreement at the National Environment Agency (NEA), the Ministry of Sustainability and the Environment (MSE) informed the Committee that it was attributed to process weaknesses and people factors. There were inadequate oversight mechanisms for managing the project agreement, with no structured annual compliance checks and no formal consultation process on legal and financial issues. There was also insufficient financial modelling expertise within the contract management team to handle such a complex contract.

58 NEA acknowledged that greater due diligence should have been exercised on the submitted financial models. NEA has since completed recovery of the overpayment in October 2025, with subsequent payments adjusted to account for the lapses. The financial models have been updated and reviewed by the project partner's financial adviser and NEA's contract management and finance teams. An independent auditor has completed the audit on the updated financial models in August 2025, and has verified that the models are accurate and consistent with relevant project documentation.

59 Regarding the higher post-restructuring payment of $8.09 million over 25 years, NEA's external financial consultant assessed the payments as reasonable and justified. This is given that the then-minority owner had to inject additional equity and accept a significantly reduced project equity rate of return below market expectations, while lenders accepted less favourable financing terms. Overall, the project restructuring has delivered a satisfactory outcome for NEA.

60 NEA has implemented several measures to enhance the management of the project partner and contract. In November 2025, a formal Work Instruction was issued mandating consultation with NEA's Finance and Legal Divisions on project agreements and financial models, including engaging external professional experts when necessary. From December 2025, annual compliance reviews will be conducted for PPP projects using a dedicated checklist developed by external legal advisers to cover due diligence requirements and contractual obligations. An Engineering and Safety Department was established in March 2025

to strengthen oversight and technical assessments of operational issues across all PPP contracts for waste management facilities. Since August 2025, NEA has strengthened on-site checks and inspections of the project partner through more comprehensive and frequent physical verification of operational data, maintenance records, and direct witnessing of equipment repairs and servicing to ensure that physical data corroborates with submitted reports.

61 In November 2025, NEA established a contract risk management steering committee comprising senior leadership to strengthen organisation-wide contract management. Taking reference from the "Three Lines Model" of governance and risk management, NEA has implemented the following:

a. Line 1 (Key operational divisions): Strengthen capabilities of divisions that oversee large or complex contracts through structured training courses and sharing of best practices. The use of the checklist for PPP projects mentioned above will ensure that complex contract milestones are promptly escalated to senior management.

b. Line 2 (Central capabilities): Develop central oversight and guidance capabilities for management of large or complex contracts, ensuring that Line 1 divisions have the necessary systems, expertise, and processes to handle complex contract issues.

c. Line 3 (Internal audit): Updated contract audit planning methodology (effective June 2025) to ensure more timely audits of large contracts.

62 NEA has conducted checks across other PPP project agreements to ensure no similar lapses exist. These agreements have less complex financial structures and do not require any changes to the financial model. NEA has also strengthened governance, oversight, and contract management of PPP projects by ensuring that complex issues are adequately supported by in-house legal and finance expertise or, when necessary, professional legal and financial advisers.

<u>Public Utilities Board</u>

63 On the observation on lapses in management of biocide and chemical supply contracts, at the Public Utilities Board (PUB), MSE informed the Committee that the root causes were due to (a) people factors: inadequate supervision and officer diligence in performing the required checks, and (b) process weaknesses: inadequate SOPs and the use of manual stock tracking records which were prone to error.

64 In response, PUB took disciplinary actions against accountable officers and counselled others for less serious mistakes in September 2025. PUB has tightened its SOPs since May 2025 and reminded staff of the checking procedures required for stock deliveries, including ensuring compliance of certificates of analysis (COAs) with contractual requirements before making payment. For chemical stocks, contractors are required to submit original COAs to ensure independent laboratory testing. For biocides, PUB reviewed its SOPs since May 2025 and transitioned from manual spreadsheets to a centralised enterprise inventory system for tracking of stocks to prevent errors in stock level projections. Arising from AGO's observations, PUB confirmed that all stocks received met quality requirements with no operational impact, and obtained compliant COAs from contractors for the affected stocks. It has also reviewed and improved contract specifications across all affected contracts since October 2025.

65 For the observation on poor management of PUB analysers maintenance contracts, MSE informed the Committee that it was due to process weaknesses - a lack of comprehensive coverage in the maintenance contracts. PUB's analysers at the two PPP plants stored water quality data in localised systems requiring manual download and forwarding to PUB, as an interim arrangement pending the long-term plan to transmit data directly to PUB's central system. However, the maintenance contracts did not include requirements for maintenance of functions for data transmission and alert-related systems. When the analyser data loss problem first surfaced in October 2023, PUB and the maintenance contractor took action to troubleshoot but the contractor did not have the capabilities to resolve the issue. This resulted in extended resolution time as PUB had to approach the original equipment manufacturer who did not respond and had to take another few months to source for their authorised contractor to address the data and SMS alert problem.

66 PUB had been addressing the gap before AGO's audit and has fully resolved the issues by November 2024. During the period when the data and alert-related systems were down, PUB relied on the PPP plants' analysers data, with duplicate analysers providing cross-checks on product water quality. Since January 2021, PUB has imposed strict controls to prevent the changing of water quality data without PUB's approval. PUB officers conduct weekly on-site visits to view plant data or assess analyser and equipment conditions as part of regular monitoring and deterrence. Additionally, product water samples are sent to third-party accredited laboratories for testing. These standing measures collectively provided PUB with assurance on product water quality.

67 Since January 2025, PUB has linked all analysers from the PPP plants directly to its centralised system, automating data transmission and alert functions for central monitoring, while leveraging other contracts to provide more comprehensive maintenance coverage and minimise downtime. Following the migration to the centralised system, PUB completed a review of its maintenance contracts in May 2025 to ensure adequate coverage for managing PPP plants, including troubleshooting analysers and addressing data and signal problems, with regular reviews planned going forward. PUB communicated this case during its Procurement Townhall in November 2025, emphasising the need for comprehensive maintenance contracts, and will continue reinforcing these lessons through its training programme.

68 MSE informed the Committee that possible irregularities in audit records and star rate item quotations were primarily due to people factors, with the following follow-up actions taken.

a. Possible irregularities in audit records: The officer had asked the contractor to alter the COAs to conceal incomplete original documents. PUB completed its internal investigation in August 2025 and issued a formal reprimand to the officer in September 2025, and will downgrade his 2025 performance grade. The case has been shared as a cautionary tale with all staff through an August 2025 email and November 2025 Procurement Townhall. Safeguarding document integrity would be incorporated into contract management training programmes. Notwithstanding the COA alterations, PUB confirmed the biocide stock quality was satisfactory with no operational impact.

b. Potential irregularities in star rate item quotations: There were malpractice and non-compliance with procurement guidelines by the PUB officer and consultant where independent quotes were not obtained for the star rate items. PUB has reported the

matter to the Police to investigate potential fraudulent practices, with investigations ongoing. PUB will follow up with disciplinary actions should any wrongdoing be uncovered, or legal action for recovery should there be any financial loss. A thorough review of similar contracts completed in April 2025 found no other irregularities. PUB is exploring digital tools to detect such irregularities more effectively, with a feasibility study to be completed by March 2026.

69 Additionally, PUB has tightened its SOPs for contract management since May 2025 to ensure alignment with contractual requirements and increased the scope of regular internal audits on procurement and contract management. This includes additional checks on star rates in contract variations and the use of digital tools, including AI, to improve checks and detect fraud. Since November 2024, PUB has strengthened its consultancy contracts for professional engineering services by incorporating Government IM guidelines for star rate assessment into contracts and providing consultants with updated SOPs to carry out checks on quotations for star rate assessment. A whistleblowing channel is available for staff to report irregularities for independent investigation, and learning points have been communicated to staff through a Procurement Townhall session in November 2025 and digital communications.

70 To further drive competency development and process improvement, PUB will take the following actions:

a. Enhance officers' competency through mandatory refresher training on procurement and formal attestation requirements, to be rolled out from January 2026, aiming to raise staff awareness of possible irregularities in procurement and contract management.

b. Emphasise the need to safeguard the integrity of supporting documents for contract management and financial transactions through its training programme for officers managing contracts and update PUB's Code of Conduct by January 2026.

c. Continue to reinforce lessons from AGO's audits through annual Procurement Townhalls and e-learning to be conducted in November every year.

d. Regularly review adequacy of coverage of maintenance contracts, starting from January 2026.

e. Establish datasets of prices and rates to facilitate the assessment of star rates, to be available from March 2026.

f. Review SOPs for other contracts to ensure alignment between contractual requirements and checks to be performed by staff, by July 2026.

g. Explore the use of digital tools to detect irregularities more effectively, with feasibility study to be completed by March 2026.

h. Automate processes wherever feasible to reduce reliance on manual monitoring and the risk of human error, with specific automation/AI tools targeted for roll-out by July 2026.

Ministry of Trade and Industry

71 The Ministry of Trade and Industry (MTI) informed the Committee that the lack of robustness in tender evaluation and award of contract for the Global Media Agency Services at the Economic Development Board (EDB) was due to human oversight. The Tender Evaluation Committee (TEC) failed to maintain proper documentation of reasons for accepting data after the tender closing date[1], clarify with the tenderer on discrepancies, and flag these issues to the Tender Approving Authority. Following AGO's observation, EDB's internal audit review found this to be an isolated incident with no other irregularities in its procurement cases.

72 EDB has put in structural and process improvements to strengthen procurement governance. This included:

a. Implementation of Procure-to-Pay (P2P) system in December 2022 that includes systematic procurement workflows, central document repository, and built-in checkpoints to improve documentation trails and ensure proper approvals at key stages.

b. Enhancement of procurement checklist to provide officers with clearer guidance on key requirements and common pitfalls to avoid across the procurement lifecycle.

c. Regular training programmes and knowledge-sharing sessions on procurement guidelines and risk management, supplemented by case studies and best practices, to strengthen officers' awareness and competencies.

d. Introduction of multi-layered review framework from 1 October 2025 which includes additional reviews by senior procurement officers and the IA team for high-value or complex tenders during sourcing and evaluation phases. This enables the proactive identification of potential issues and compliance with procurement policies and procedures.

73 For the observation on lapses in administration and weaknesses in design of Singapore Global Network Funding Programme (SGNFP), MTI informed the Committee that the root causes were due to (a) outdated eligibility criteria that had not been reviewed since SGNFP's inception, (b) absence of requirements for conflict of interest (COI) declaration and document retention, and (c) inadequate claims verification processes that lacked COI checks and formal approval documentation for deviation cases.

74 To address these lapses, EDB has implemented the following measures to strengthen SGNFP's operational processes:

a. Updated the eligibility criteria to align with Singapore Global Network's expanded engagement mandate, specifying eligible applicants, nature of supported events, and types of participants covered.

[1] According to EDB, as the original quoted fee of $9.45 million was not supported by a breakdown of remuneration data by individual roles, the TEC had sought clarifications from the vendor after tender-close and accepted the remuneration data which resulted in the derived fee of $11.54 million.

b. Standardised retention processes for supporting documentation to ensure all documents are saved.

c. Enhanced pre-event application and post-event reporting forms to require COI declarations and established a formal process to assess and manage these declarations.

d. Tightened the approval process for deviation cases to include formal documentation of approvals.

75 To address and eliminate applicants' potential gaming behaviour, EDB has revised SGNFP's reimbursement criteria from May 2025 to be the lower of the pre-event approved amount, or 80% of the net eligible actual event cost (which EDB will validate during claims verification against original receipts). At the post-event reimbursement stage, EDB has strengthened its processes to ensure that SGNFP's policy intent is met. This includes verifying supporting documentation to confirm that the event has achieved its projected scale. Where there is significant shortfall, applicants are deemed as non-compliant with SGNFP's terms and may be disqualified from the programme. EDB will continue to monitor and conduct annual reviews of SGNFP's design and administration.

Ministry of Transport

76 For the observation on dumping and monitoring fees and port dues concessions not prescribed in law at the Maritime and Port Authority of Singapore (MPA), the Ministry of Transport (MOT) informed the Committee that the root causes were due to misalignment in understanding of legislative requirements and oversight in drafting of legislation.

77 The dumping fees had been charged by the then-Port of Singapore Authority (PSA) and had continued when MPA was established in 1996. MPA understood its provision of sites for dumping of materials as contractual in nature rather than pursuant to a regulatory function, hence without the need for legislation. The 20% port dues concessions for annual and six-month schemes were inadvertently omitted due to legislation drafting oversight. As for the 100% port dues concessions for government bodies, schools, and non-profit organisations inherited from PSA, MPA had interpreted the MPA Act as permitting indefinite fee waivers.

78 Parliament has passed the Transport Sector (Miscellaneous Amendments) Act 2025 to validate all dumping and monitoring fees collected, which will be brought into force by 1 February 2026 along with the subsidiary legislation prescribing the fees. For the 20% port dues concessions, the MPA Board exercised its statutory waiver power in May 2025 to validate past concessions and continue granting them until the subsidiary legislation takes effect in February 2026. Similarly, for the 100% port dues concessions, the MPA Board exercised its waiver power in May 2025 to validate past concessions and continue them until December 2026, pending a review of the scheme.

79 MPA has commenced a phased review of all other fees and concessions to ensure they are prescribed in law where required, with completion targeted by end of 2027. MPA will also enhance its processes for implementing new programmes and services, including establishing

SOPs to assess whether associated fees and concessions need legislative prescription and to ensure legislation captures policy intent. MOT will work with MPA on this review.

80 On the observation on errors in scoring for tender evaluation, MOT informed the Committee that the error arose from MPA's tender evaluation team's decision to consider the role of the tenderer's subsidiary in the evaluation process. Given the tenderer's group corporate structure, the evaluation team recognised the subsidiary's certification as part of the tenderer's overall capabilities and awarded points on the basis that the subsidiary would be providing the service. This evaluation approach of considering the subsidiary's capabilities was an exception to standard practice.

81 MPA acknowledged that future tenders can more clearly provide for procurements with bids coming from companies and their subsidiaries. MPA is revising procurement templates for such tenders, to be completed by early 2026, and has informed all heads of division on this audit observation. MPA will also include this as a learning point in its regular staff engagement on corporate governance.

82 On the observation on inadequate checks to ensure payments were properly made, MOT informed the Committee that it was due to the operational team advising the Goods/Service Receipt Officer based on its assessment of the delivery of goods and services, without checking to the specific contract requirements.

83 In response, MPA obtained all maintenance reports from March 2022 to November 2024 from the contractor and verified that the patrol craft had been properly maintained. Similarly, for the marine salvage and anti-pollution operations, MPA retrieved the relevant internal operational logs, playback vessel traffic images and photographs to verify that the services were satisfactorily delivered as per contract requirements. There were no new findings.

84 MPA has developed and implemented two sets of SOPs for services provided by the operational craft and for marine salvage and anti-pollution operations to ensure the contractor has fulfilled contractual requirements satisfactorily before payments are made. Officers have been briefed on these procedures since March 2025.

85 MPA will also share the lessons learnt from AGO's audit with its officers during staff corporate governance briefings and other engagements. MPA's regular internal audits will incorporate the relevant checks so that similar issues in other contracts can be promptly addressed.

Thematic Audit on Research and Development Grants

86 The Committee considered the key findings made on RIE 2025 – R&D grants managed by the Agency for Science, Technology and Research (A*STAR) and the National Research Foundation (NRF) and asked the supervising Ministries to address the following questions:

a. What are the root causes of the lapses and what are the further follow-up actions taken/to be taken to address these lapses?

b. What are A*STAR's/NRF's plans to address the underlying weaknesses and lapses found, including through capability building, enhanced risk management and ensuring compliance with policies, procedures and other requirements?

c. For purposes of public sector sharing, regarding the good practices put in place by A*STAR/NRF as observed by AGO, whether A*STAR/NRF can:

(i) Elaborate on its risk-based approach in grants administration; and
(ii) Provide further details about the dashboards and/or systems used for grant administration and management, including the key features and functionalities, and how they enhance oversight and operational efficiency?

Ministry of Trade and Industry

87 MTI informed the Committee that for the observation on approval not sought for deviation from policy on funding of indirect costs, the lapse occurred as the affected projects were negotiated and submitted in RIE 2020 and during the transition period to RIE 2025. Consequently, the RIE 2020 rate of 20% of direct costs was used in the computation and approval of indirect cost funding for these projects instead of the RIE 2025 rate of 30%. As A*STAR's SOP did not require explicit approval for using a different rate, it was assumed that the Project Approving Authority's approval constituted approval of the 20% rate.

88 A*STAR has since obtained covering approvals from NRF for the affected projects and updated its SOP to require documentation and approval for any deviation from the prescribed indirect cost rate. Grant officers will now receive regular updates on grant matters, and an online training course covering RIE policies and A*STAR's grant administration process is being progressively rolled out. The first module has been launched, with the remaining modules expected to be completed by the end of the first half of FY2026.

89 For the observation on manpower costs for seconded researchers incorrectly funded, it was a result of human error and oversight arising from staff turnover at the Host Institutions (HIs). Newly assigned HI resource personnel did not follow the SOP, which requires amending the cost recovery to a new cost centre when an HI staff begins secondment or a double-hat arrangement. The errors occurred only at 2 HIs, and A*STAR's checks on other HIs did not uncover similar issues. The SOP owner has since briefed the relevant HI resource personnel on the correct procedures and rectified the issue. Onboarding sessions are also conducted for new HI resource personnel involved in manpower cost allocations, during which the need to follow established procedures is reinforced.

90 On the observation concerning the sampling approach for checks on first fund requisitions (FRs) not working as intended, the lapse was caused by a gap in the sampling logic in iGrants (A*STAR's grant management system). iGrants did not account for cases where budget revisions were made before submission of the first FR, resulting in some cases being incorrectly auto-approved instead of sample-checked. A*STAR has since reviewed the affected FRs manually and obtained covering approvals. The sampling logic in iGrants has also been updated to account for such scenarios. A*STAR has deployed a monitoring dashboard on 5 January 2025 and it has been used to assess past cases and verify that the updated sampling

logic is functioning correctly. The updated sampling logic will be incorporated in iGrants 2.0 that is scheduled to go live by the end of 2026.

91 The observation on lack of independence in endorsement of progress reports was due to the absence of an explicit requirement in A*STAR's SOP to check for segregation of duties. While iGrants can re-route report endorsements to an alternate endorser when HI Executive Directors submit progress reports as Principal Investigators, this process requires manual intervention by grant officers. Independent alternate approvals have since been obtained for the affected progress reports. A checklist to verify segregation of duties and guidance on manual re-routing have been added to A*STAR's SOP for progress report reviews, and this has been communicated to all grant officers. An updated checklist will also be issued to all grantees by end March 2026. Features to prevent conflicting endorsements and approvals will be included in iGrants 2.0. In the interim, A*STAR has rolled out a daily-updated dashboard on 30 April 2025 to monitor progress report endorsements and approvals and alert grant officers to cases of potential COI for prompt follow-up.

92 The Committee asked MTI to provide further details about the dashboards A*STAR uses for grant administration, noting this as a good practice. MTI replied that A*STAR has developed a suite of customised monitoring dashboards to enable fast, user-friendly extraction and analysis of grant data. The dashboards have enhanced compliance and operational efficiency by:

a. Providing grant officers with quick, convenient access to daily project data for monitoring and reporting at scale;

b. Offering a top-level view of key statistics of awarded projects under different funding initiatives; and

c. Enabling rapid identification of incidents requiring attention – such as stalled processes and potential non-compliance – so that corrective action can be taken in a timely manner.

93 Examples of how A*STAR employs data analytics and the use of dashboards include:

a. Monitoring FR and progress report submissions and approvals – Dashboards, paired with automated email reminders, help identify bottlenecks and enable prompt resolution to ensure that fund disbursements remain on schedule.

b. Tracking grant budget utilisation – Early identification of projects struggling to utilise their budget enables intervention. The data also reveals trends in fund consumption over a project's lifecycle, improving prudence in future budget awards and supporting more accurate cashflow forecasting.

c. Reviewing activities by users with elevated system privileges – Consolidated dashboard aggregates relevant action trail data dispersed across various parts of the iGrants interface into a single report and provides contextual information to support efficient review.

94 On A*STAR's risk-based approach in grant administration, which the Committee noted as a good practice, MTI informed the Committee that A*STAR employs a risk-based sampling

logic in iGrants that automatically approves most low-value FRs while routing higher-risk FRs above a specified threshold to project officers-in-charge for review. FRs below the threshold are sampled randomly. First FRs of projects follow a separate sampling logic – they are evaluated based on whether the requested amount exceeds a fixed proportion of the project's total budget. Through this risk-based approach, A*STAR sampled 34% of all FRs submitted in FY2024, accounting for 84% of funds disbursed, thereby achieving a strong balance between oversight and operational efficiency.

Prime Minister's Office

95 The Prime Minister's Office (PMO) informed the Committee that the lapses identified by AGO stemmed from 3 primary root causes – people, policy, and process. NRF has adopted a systematic approach to address each area and prevent recurrence of the observations.

96 The observation on inadequate documentation of COI declarations was attributed to documentation weaknesses – a people-related root cause. NRF immediately followed up with the affected reviewers to obtain retrospective COI declarations.

97 Policy-related issues occurred when the policy intent or decisions were not explicitly documented or where guidelines lacked clarity. For the observation on approval not sought for deviation from policy on funding of indirect costs, the deviation was consistent with NRF's intent to apply the prevailing funding rate at the time of grant call launch. However, formal approval was not clearly documented. NRF has since obtained approvals for all affected projects and revised its guidelines to specify that prevailing guidelines at the time of a grant call's launch will apply by default. Similarly, changes in funding modality between NRF and an HI were not formalised through addenda to Letters of Award (LOAs), as this requirement was not stipulated in existing guidelines. NRF has issued formal addenda to LOAs for affected projects and introduced a standard addendum template for key variations such as changes in financial obligations, effective 13 March 2025.

98 The observations on inadequate segregation of duties in endorsement of FRs and potential or perceived COI in payments processing were a result of inadequate internal processes. NRF officers serving as ex officio directors on the boards of research entities lacked clear procedures for declaring conflicts and recusing themselves from FR verification or payment approval. To address this, NRF has updated its COI Management Framework on 28 October 2025, clarifying policies on declarations and recusals. Officers with present or potential conflicts are now excluded by default from fund disbursement decisions. Additionally, NRF has stipulated an explicit rule, effective 13 March 2025, that FRs can only be endorsed by non-conflicted persons from the HI's management.

99 To strengthen its governance framework, NRF has implemented a Three Lines Model with the establishment of an in-house IA unit (the third line of defence), effective 1 November 2025, while retaining the existing in-house Assurance function (the second line of defence). This will strengthen NRF's organic capability to manage risks more responsively through regular and timely reviews of policies and procedures, as well as the integration of technology (such as the new Research Grants Portal) to improve grant administration, risk management and compliance. NRF is also developing a plan to enhance its onboarding and training

programmes to ensure that all officers are made aware of key policies, procedures and risks when they join the organisation.

100 The Committee asked PMO to elaborate on its risk-based approach in grant administration. PMO informed the Committee that NRF introduced a funding initiative paper template requiring all RIE Agencies to provide baseline information when seeking approval for renewal of existing initiatives or new funding initiatives. This ensures that each RIE Agency incorporates a systematic process for risk identification, assessment and mitigation as a core part of the funding initiative design and approval. RIE Agencies are also required to define governance structures, including oversight mechanisms.

101 Regarding NRF's grant management system, which the Committee noted as a good practice, PMO informed the Committee that it serves as a single platform for RIE Agencies to manage grant applications, reviews, and funded projects. The system consists of a standardised workflow and template for the submission of grant proposals, and a project management module for deviation requests and progress reporting. The claims module incorporates controls to prevent duplicate claims or claims beyond the funding duration, while the reviewer module consolidates reviewers' information within a central database to facilitate sharing across RIE Agencies. A dashboard with a consolidated overview of funding status and grant utilisation has also been made available to the RIE Agencies. Overall, the system has enhanced grant administration efficiency through a unified process for the research community applying for RIE grants, and a common workflow and data structure for grant processing.

102 To cater to the evolving needs of the RIE sector, a new Research Grants Portal will be rolled out progressively in FY2026. The portal will include configurable workflows and templates, simplified processes, reduced data entry requirements, automation of grant rules and validations, and enhanced analytics and outcome linkage.

B. Broader Issues

103 The Committee also discussed broader issues which could impact spending, financial governance and controls across the public sector, namely:

a. Procurement, Contract Management and Grant Administration;

b. Revenue Collection and Accounting;

c. Internal Audit Capabilities;

d. IT Controls and Cybersecurity Governance; and

e. Cross-agency Data Sharing and Use of Data Analytics and Artificial Intelligence.

Procurement, Contract Management and Grant Administration

104 The Committee noted that lapses in procurement, contract management, and grant administration continue to be recurring findings by AGO. The Committee asked the Ministry of Finance (MOF) about the following:

a. Evaluation of the root causes underlying recurring lapses in procurement, contract management, and grant administration.

b. Update on the implementation status of MOF's central initiatives, including new measures, and the extent that they have addressed root causes and enhanced financial governance outcomes.

c. Statistics, metrics and/or key performance indicators demonstrating if governance in these areas has improved across agencies.

d. Assessment of whether agencies have sufficient capabilities to exercise proper oversight, specifically for PPP projects that involve complex financing models or terms; and the guidance MOF provides to agencies in this regard.

105 In addition to a written response from MOF, the Committee also called upon the Permanent Secretary of MOF to provide oral clarifications and elaboration of MOF's written response.

Ministry of Finance

106 MOF informed the Committee that recurring lapses in procurement, contract management and grant administration stem from a combination of factors, mainly:

Area	Factors
Procurement and Contract Management	a. Non-compliance by individual officers, arising from knowledge gaps or prioritising operations over process or documentation; b. Inadequate supervision by supervisors; c. Inadequate controls over and monitoring of contractors' compliance with policies and procedures; and d. Inadequate documentation of decisions made or work done.
Grant Administration	a. Inadequate management of COI situations; b. Insufficient checks when conducting grant eligibility assessment and disbursement; c. Lack of segregation of duties in processing grant claims; and d. Inadequate documentation on basis of key decisions or deviations made.

107 MOF is mindful that there are trade-offs between introducing additional controls and maintaining processing efficiency. It is also important as part of risk management to provide agencies with sufficient time to build appropriate systems and implement controls, ensuring adequate protection against potential risks, before rolling out new schemes or enhancements. Hence, MOF and agencies adopt a calibrated approach to balance risk mitigation and compliance costs while continuing to strengthen controls over procurement and contract management, and grant administration.

Procurement and Contract Management

108 For procurement and contract management, a key focus is to uplift competencies. Training and capability building initiatives include a compulsory e-learning module introduced in 2018, covering standard procedures for Government procurement that all officers new to the procurement function must complete. This e-learning module was enhanced in 2024. Additionally, the Finance and Procurement Academy, set up by MOF, regularly shares lessons from past lapses and good practices to adopt with public officers involved in procurement and contract management.

109 Agencies have established specialised competency frameworks and training programmes to address competency or domain gaps. For example, the Building and Construction Authority (BCA) implemented the Built Environment Procurement Competency Framework in 2023 to develop procurement competencies for construction projects. BCA has also strengthened contract administration capabilities through courses like Understanding and Applying the Public Sector Standard Conditions of Contract (PSSCOC) and specific training in areas such as financial modelling for complex PPPs. To address issues relating to star rates, MOF and BCA have also jointly issued a good practice guide on managing variation orders and identifying fraudulent quotes, which is complemented by a central repository of agencies' Schedule of Rates for reference.

110 MOF has worked with JTC to establish the Building and Infrastructure Centre of Excellence (B&I CentEx), which provides project management and advisory services to agencies lacking B&I capabilities. For agencies that collaborate with the B&I CentEx, project progress will be tracked through a steering committee co-chaired by JTC and MOF to ensure proper oversight. Knowledge sharing is facilitated through the Built Environment Community

of Practice (CoP) with specialised courses including the Public Project Leadership Programme (PPLP) and Project Management Intermediate Course (PMIC). For construction contracts, MOF has been tracking agencies' performance in contract management, based on a set of governance indicators, and observed improvement over time in the timely approval of variation orders. Based on sampling checks, the proportion of contracts with timely approval of contract variation has improved from about 70% in 2018 to above 90% in 2023.

111 MOF informed the Committee that new initiatives introduced for procurement and contract management include supporting agencies in their streamlining of processes and digitalising procure-to-pay-and-contract management processes. There are also efforts to explore using digital tools such as AI to provide guidance and process validation in the procurement process. An AI Workgroup has been convened among procurement teams across agencies, to share AI use cases and encourage the adoption of such technologies. These initiatives complement MOF's ongoing efforts to strengthen procurement and contract management capabilities and systems across agencies, such as through the Procurement Competency Framework and associated training courses.

112 The Committee asked whether agencies have sufficient capabilities to exercise proper oversight of PPP projects that involve complex financing models or terms. MOF informed the Committee that although PPP projects may be more complex, the process and fundamentals of evaluation and contract management are similar to contracts established using other procurement approaches. Agencies must assess whether they have sufficient internal capabilities to structure, evaluate and manage PPP projects, throughout the project lifecycle, and may tap on the expertise of external consultants and advisers if needed. Procurement and finance training courses would also enable agencies to build the necessary capabilities.

113 MOF also informed the Committee that it has established a Commercial Advisory Team to support agencies embarking on complex or nascent projects. The Team provides advice on both upstream and downstream processes, including the setting up of the procurement structure, tendering approaches and contracting models. To embed continuous professional development within the process and enhance agencies' project management capabilities, MOF encourages agencies to support their procurement officers undertaking infrastructure projects to obtain Accredited Professional Quantity Surveyor (APQS) certification. MOF is also examining the introduction of a requirement for agencies to engage accredited Quantity Surveyors for projects above a certain scale.

Grant Administration

114 MOF collaborates closely with sector lead agencies, GovTech, the Inland Revenue Authority of Singapore (IRAS), and the Commercial Affairs Department (CAD) to support grant-giving agencies.

115 MOF regularly reviews and updates its central guidance, incorporating good practices and learning points from AGO's annual audit observations, to ensure that it remains relevant and addresses emerging risks. The Government IM and Good Practice Guide on Grants Governance provide updated guidelines on areas such as detecting ineligible claims, managing COIs, segregation of duties, grant documentation, and system controls. The Good Practice Guide was further enhanced in 2025 to include project progress reviews and stronger system checks.

116 To reduce lapses arising from people and process factors, CoP forums and e-learning courses have been introduced to enhance officers' knowledge and support them to improve grant processes. CoP forums jointly organised by MOF, IRAS and CAD are held annually for grant-giving agencies to learn and share best practices on grant administration, as well as fraud prevention and detection, with the most recent forum held in May 2025. MOF and the Civil Service College (CSC) introduced the "Fraud Awareness for Grant Officers" e-learning course in September 2025, building on the "Introduction to Grants Governance" course launched in July 2023, which over 4,000 officers have completed as of October 2025.

117 Several central systems, platforms and tools have also been introduced:

a. Central systems for grants within the same sector – enable the application of common analytics and checks to strengthen due diligence, consistency, management of COI, segregation of duties, and other requirements including documentation.

b. Fraud Detection Platform – provides network analytics to perform due diligence checks on grant applicants and identify suspicious entities or individuals as part of their grant evaluation process, with over 30 agencies onboarded.

c. DocAnalytics – a document analysis tool rolled out in February 2025 to further support public officers (e.g. to screen documents in PDF format for irregularities), with over 43 agencies onboarded.

118 To facilitate cross-sharing of more real time information on fraud-related modes of operations, an intel-sharing network was set up by MOF/CAD in August 2023. As of November 2025, more than 350 officers from 40 agencies have signed up to be part of this network.

119 To ensure overall capabilities are deepened within and across sectors, all grant sectors have attained foundational and intermediate levels of maturity in the grants administration capability-building roadmap for the areas of data analytics and systems, and fraud detection and investigation. They are now working towards attaining the advanced level of maturity.

120 On new initiatives introduced for grant administration, MOF informed the Committee that it introduced a Grant Risk Management Guide in November 2024 to help agencies strengthen their grant risk management. This guide outlines grant-related risks and mitigating measures, and includes sample risk indicators, a scoring matrix and a risk register template. In 2025, MOF worked with CAD and IRAS to pilot a red-teaming exercise for selected grant schemes — particularly new schemes or those up for renewal with higher impact and risk — to supplement existing central guidance and resources. The pilot exercise involved five grant schemes where risk scenarios and corresponding risk mitigation measures were identified. These exercises were generally conducted before the grant scheme roll-out or implementation of enhancements to ensure that risk considerations were addressed upfront. Key insights gleaned will be incorporated into existing references such as the Good Practice Guide and communicated to agencies.

Revenue Collection and Accounting

121 The Committee noted several audit observations relating to revenue collection and accounting, and asked MOF about the following:

a. Measures MOF has taken to ensure that agencies collect fees and provide concessions with legal authority where required.

b. Guidance and oversight that MOF provides to ensure agencies properly account for public monies collected overseas, or through overseas partners.

Ministry of Finance

122 MOF informed the Committee that agencies administer fees and charges (F&Cs) to ensure that the provision of Government goods, services and facilities is fiscally sustainable. In setting F&Cs, MOF requires agencies to manage the costs of such provision, the impact on households and businesses, and ensure that the governance processes are in line with relevant laws and administrative guidelines.

123 MOF sets central rules and policies, and works with agencies to implement their F&Cs. Respective agencies are responsible to ensure compliance with guidelines and relevant laws. Agencies must ensure that F&Cs collected and any concessions provided, including through overseas partners, are prescribed in law as appropriate and accounted for as required.

124 MOF has been stepping up oversight of F&C management through strengthened senior leadership engagement, tracking and reminding agencies yearly to review their F&Cs, and regular policy reviews to improve central oversight and WOG compliance.

Internal Audit Capabilities

125 The Committee noted that MOF, through the Accountant-General's Department (AGD), has embarked on multi-year transformation efforts to restructure IA, digitalise audit processes and deepen the capabilities of public sector IA. The Committee asked MOF about the following:

a. Update on the central initiatives, including new initiatives introduced to address recent developments.

b. Platforms and mechanisms through which IA functions across public sector share best practices and learn from one another, providing details on the frequency of such interactions and examples of how shared learnings have been implemented to address common audit findings across agencies.

Ministry of Finance

126 MOF informed the Committee that AGD has embarked on a multi-year IA transformation roadmap since 2022, covering policy/standards, system/process, and structure/workforce. Ministries have appointed their GCIAs to consolidate their IA functions at the Ministry family level. This has enabled the public sector IA to make good progress on various fronts.

127 Since the launch of the central Audit and Governance Enterprise Management System (AGEM) in December 2023, AGD has progressively onboarded agencies to the system which helps to generate audit insights for better decision-making, improve audit productivity and facilitate collaboration across the public sector.

128 Following the issuance of the revised WOG IA Manual to support compliance with the Global Internal Audit Standards (GIAS) in 2024, AGD issued the first annual WOG Central Guidance for IA in July 2025. The Guidance emphasises the governance of IA function and the value of moving towards more upstream advisory as set out in the GIAS. For instance, IA is expected to work closely with management to identify and mitigate risks early, rather than focusing solely on post-implementation reviews. In addition, to uplift audit quality, the Guidance also highlights common audit lapses and suggests enhanced audit procedures and central analytics tools for grants and procurement.

129 MOF/AGD has also successfully conducted three runs of the IA Foundation Programme for 73 IA officers since October 2024. To strengthen collaboration between Finance and IA, the Finance Leadership Programme has been extended to IA leaders. MOF/AGD is developing an IA Middle Management programme for FY2026.

130 MOF informed the Committee that good practices and learning points are regularly shared at the Ministry family level via the GCIAs, as well as at the WOG level via the quarterly GCIA meetings, annual IA Round Table and IA Community Day. Examples of good practices shared include central analytics tools that have been widely adopted by agencies. In October 2025, AGD worked with the public sector IA community to organise the inaugural Governance Week to build awareness on key governance concepts and risk management, with sharing by

both private and public sectors. Around 1,700 public officers participated across the 8 events held.

IT Controls and Cybersecurity Governance

131 The Committee observed that audit findings concerning weaknesses in the management of the most privileged operating system account and privileged access management have been recurring over the past years. The constantly evolving nature of cyber threats has also underscored the critical need for robust cybersecurity governance. The Committee asked the Ministry of Digital Development and Information (MDDI) and Smart Nation Group (SNG) about the following:

a. Whether MDDI and SNG have an established privileged access management framework that is mandated and enforced across all agencies; and if so, what is the framework and how it is being implemented.

b. What WOG initiatives MDDI and SNG have implemented or are currently implementing to address the systemic issues noted in audit findings.

c. Whether MDDI and SNG have considered mandating regular independent cybersecurity audits for mission-critical government systems; and if such a framework is already in place, whether details can be provided on its scope and implementation across agencies.

132 In addition to a written response from MDDI and SNG, the Committee also called upon the Permanent Secretary of MDDI and SNG to provide oral clarifications and elaboration of MDDI and SNG's written response.

Ministry of Digital Development and Information and Smart Nation Group

133 MDDI and SNG informed the Committee that the management of the Government's Information and Communications Technology and Smart Systems (ICT&SS) relies on the strong partnership between them and respective agencies, and MDDI and SNG support agencies in two key areas.

134 First, at the **policy level**, MDDI and SNG set out the broad WOG governance frameworks for agency ICT&SS management. Under the Public Sector (Governance) Act 2018 (PSGA), all public sector agencies must comply with the Government's policy on use or development of information technology, data governance (including personal data protection) and data sharing. This policy is set out in the Government IM on "Info-communications Technology and Smart Systems", and related Circulars. These documents set out rules and standards to (a) promote good governance of ICT&SS, balancing the need for public sector standardisation with affording flexibility and customisation to context; (b) provide guidance on the use of technology and best practices while ensuring tiered risk mitigation; and (c) enable the use, sharing and management of data by agencies for citizen benefit.

135 Second, at the **operational level**, MDDI and SNG empower agencies through education, tools and capability development. GovTech has deployed approximately 1,700 officers across 56 agencies, including CIOs, CISOs and IT delivery teams. This approach ensures that agencies benefit from specialised technical expertise while maintaining autonomy to discharge their

accountabilities and make policy-operational decisions within established governance standards. MDDI and SNG are also enhancing their digital competency framework aimed at increasing the capabilities of both public officers and leaders, starting with engagement at the leadership level that includes Permanent Secretaries, Deputy Secretaries, Chief Executives, and Directors, to raise awareness of the importance of technology in agencies' operations and the associated pitfalls.

136 The key guiding principle of MDDI's and SNG's support to agencies is that while MDDI and SNG establish baseline standards and rules within the Government IM, agencies retain ultimate accountability for their systems and can determine the tools and processes to meet these standards. Being the most familiar with their own policy imperatives, operational needs and contexts, agencies are best positioned to assess the trade-offs between risk, cost and performance of their systems, and decide on new ICT technology adoption and management approaches.

137 At the **system level**, MDDI and SNG informed the Committee that through the Government IM, they have specified a set of baseline technical and process controls on privileged account management that agencies are required to put in place for all their systems. Some examples include:

Area	**Requirements**
Privileged Account Management	• Maintain inventory of all accounts (including privileged accounts) and their access rights; • Deny access by default and grant only minimum permissions required; • Require Multi-Factor Authentication for privileged accounts at login; • Review privileged accounts and access every month; and • Disable or remove inactive or expired accounts within defined time.
Credential / Secret Management	• Change default credentials prior to first use; • Rotate static credentials or use time-restricted credentials; and • Securely store secrets in an appropriate secrets management solution.
Log Management	• Subscribe to the Government Cyber Security Operations Centre (GCSOC) for centralised cybersecurity monitoring across WOG; • Log all security-related events and review privileged activities every month; • Separation of roles from system administration and log management system; and • Ensure logs are tamper-free.

138 For Critical Information Infrastructure (CII) and Significant Information Infrastructure (SII), agencies are required to implement additional controls to tighten privileged account

management and usage tracking. For example, agencies are required to automate privileged account management using tools that provide time-bound privileged access and on a need-only basis.

139 MDDI and SNG have also promulgated best practices[2] for agencies to consider based on their use cases and criticality of their systems. One recommendation is that agencies should enforce tracking of commands executed by root users, since not all Operating Systems track such commands by default. Given the diverse range of systems deployed across WOG, MDDI and SNG have focused on establishing baseline requirements and emphasising a risk-based methodology, and avoided a one-size-fits-all approach that simply prescribes an exhaustive list of controls.

140 Agencies are required to meet the control requirements tiered based on the criticality of systems. Beyond these requirements, they have the flexibility to adopt appropriate tools, methods, and processes that best suit their operational needs. To ensure agencies properly manage their privileged accounts, GovTech conducts annual audits that include privileged account management controls. Agencies are required to remediate any gaps identified within approved timeframes.

141 MDDI and SNG acknowledge that there are areas for improvement and a key underlying cause of lapses identified by AGO is agencies' heavy reliance on manual processes for privileged account management, which are more prone to human lapses. Automation tools such as Central Accounts Management (CAM) and Automated Baseline Log Review (ABLR)[3] have been introduced since 2021, and they have helped to reduce IT lapses related to timely account removal and review of privileged account activities. However, there are limitations in the use of these tools. For example, not all accounts are onboarded and the activity logs by ABLR are still voluminous for agencies to review. MDDI and SNG will continue to explore enhancements to CAM and ABLR to minimise manual efforts required from agencies.

142 MDDI and SNG further explained that modern solutions could not be implemented readily because of legacy systems and codes (collectively termed as "tech debt"), which make it prohibitively expensive and complex to implement basic modern security controls. This legacy issue also extends to long-standing policies and operational practices that have remained unchanged over time, which would need to be changed to enable effective digital transformation. Given the many IT systems in the public sector, it will take time to bring all the systems up to date. MDDI and SNG are thus partnering agencies to identify and prioritise the more critical systems for modernisation first through the Ministry Family Digitalisation Programme (MFDP), with support from GovTech. The agencies must strengthen internal capabilities and assess which systems are critical and should be managed in-house, versus those that may be suitable for outsourcing. Such modernisation efforts require concurrent policy and operational transformation while maintaining service continuity.

[2] For example, recommendations on specific tech solutions for identity and device management, rotation or usage of time-restricted credentials. In 2020, GovTech also issued an advisory with guidelines and a checklist for controls relevant to privileged account management of Unix/Linux operating systems.

[3] CAM automates user account and access rights management and ABLR automates the review and analysis of logs related to privileged users across various platforms.

143 Additionally, MDDI and SNG will:

a. Consider extending the additional privileged account management controls currently applicable to CII and SII to higher-risk non-CII/SII systems, such as those performing financial functions. This includes automating privileged account management to reduce manual handling.

b. Step up education to support agencies in strengthening privileged account management by enhancing training and developing playbooks and implementation checklists to address common privileged access pitfalls. This includes targeted briefings for CIOs and CISOs to reinforce the understanding of privileged account risks, alongside sessions with vendors, system owners, and administrators to help them appreciate and implement 'least privilege' and 'zero standing privileges' principles.

c. Review existing policies and controls to improve tracking and management of privileged accounts. Currently, different product teams, vendors, and system owners manage their environments using varying practices and standards, creating challenges for both agencies and MDDI and SNG in maintaining an accurate picture of who has privileged access and whether controls are applied consistently. MDDI and SNG will evaluate potential implementation of new technical solutions, standards or process controls to enhance tracking of privileged accounts, trigger reviews and synchronise account provisioning/de-provisioning with staff movements.

144 Even with central support, agencies must exercise greater ownership and accountability to strengthen capabilities and tighten processes. To address issues such as poor system configuration and over-provisioning of access, agencies need to hire appropriate personnel and provide comprehensive training. While GovTech deploys CIO teams to some agencies, about half of all agencies across WOG have chosen to develop and maintain their own in-house capabilities for ICT management. GovTech will continue to strengthen capability support to agencies without in-house expertise through training, technical consultancies, and forward-deployment.

145 A holistic approach to ICT&SS risk management entails three lines of defence. Beyond strengthening capabilities at the operational level as the first line of defence, agencies must enhance their second line of defence through improved supervision, which is often inadequate. Agencies bear responsibility for ensuring sufficient resourcing and adequate oversight of ICT management and compliance with relevant rules and standards. MDDI and SNG, alongside agencies' IA functions, constitute the third line of defence.

146 MDDI and SNG informed the Committee that a government system may be subject to between three and four different independent audits, depending on the criticality of the system:

a. Under the Government IM, agencies are required to conduct independent audits on their ICT systems and cybersecurity risks must be included as part of the audit scope.

b. The Cybersecurity Code of Practice (CCOP) mandates bi-annual independent cybersecurity audits for all CII systems across government agencies,

comprehensively covering essential cybersecurity controls including privileged access management.

c. GovTech conducts periodic central audits for systems with significant materiality but are not subject to the CCOP audits, covering various cybersecurity risk areas, including privileged access management. As part of these audits, GovTech has also introduced the Proactive Risk Assessment & Incentive System Enhancement (PRAISE) initiative to encourage agencies to proactively manage their ICT risks and ensure their systems are sufficiently secure.

d. AGO conducts selective and thematic audits on government systems, usually those with financial impact.

e. Agencies either have their own internal IT auditors or external audit service providers to conduct IT audits.

147 GovTech's central audits reinforce AGO's observations on the key gaps in agencies' management of privileged accounts, namely heavy reliance on manual processes for access rights management, inadequate oversight and competency gaps at the agency-level. Agencies were found to maintain long-lived privileged accounts with extensive permissions for administrators (e.g. to facilitate frequent manual software patching) and have competency gaps in managing privileged access for new technology stacks (e.g. outdated processes that did not incorporate cloud-native access controls despite migration to cloud).

148 MDDI and SNG have since guided agencies to remediate the issues, including eliminating shared accounts where feasible, establishing more comprehensive coverage for monitoring, and implementing more systematic review processes. These efforts are progressing according to established timelines. Audit insights on common areas for improvement are also incorporated into training for agencies to help them proactively identify and remediate gaps.

149 A diverse suite of central capabilities and automation tools has also been developed to support agencies in better identifying vulnerabilities and gaps in their implementation of various system security measures:

a. The GCSOC platform provides end-to-end cyber defence operations capability to WOG agencies. It centralises cybersecurity monitoring and detection to better detect threats and enable faster responses at the agency level. It also performs proactive threat hunting to detect unknowns and facilitates swift sharing of such discoveries across WOG. GCSOC also receives threat intelligence from multiple sources and translates them into actionable intel for agencies.

b. CloudSCAPE automatically checks if IT systems deployed by agencies in cloud environments have correctly implemented the baseline security controls in the Government IM.

c. Secure Hybrid Integration Pipeline-Hive Agile Testing Solutions (SHIP-HATS) provides a common platform and templates to help agencies integrate security compliance early in their application development processes.

d. The Vulnerability Management System (VMS) identifies, assesses, and mitigates vulnerabilities in IT systems. This includes scanning servers and devices against the Common Vulnerabilities Scoring System (CVSS) database to evaluate the severity of vulnerabilities.

Cross-agency Data Sharing and Use of Data Analytics and Artificial Intelligence

150 In view of the Report of the Auditor-General for the Financial Year 2024/25 highlighting the potential for greater use of data analytics and data sharing among agencies to enhance detection of irregularities and provide insights that agencies could leverage in their work, the Committee asked MDDI and SNG about the following:

a. How MDDI and SNG facilitate and encourage data sharing and what mechanisms are in place to ensure agencies can access relevant data to run data analytics, and improve their operations and risk management.

b. How extensively are agencies currently using AI and technology in their operations to enhance efficiency, detect irregularities and generate insights; and how do MDDI and SNG promote the adoption of AI and emerging technologies across agencies.

Ministry of Digital Development and Information and Smart Nation Group

151 MDDI and SNG informed the Committee that they set out a clear WOG data governance framework, and build central platforms, tools, and products to facilitate effective and responsible data use across agencies.

152 The Government's data governance and sharing framework is implemented pursuant to the PSGA and Government IM, and enables agencies to manage, use, and share data across WOG to serve the public better, while maintaining high data protection and security standards. The framework is operationalised through the Government IM, which provides detailed policies and requirements governing the entire data lifecycle from acquisition to protection. To facilitate inter-agency data sharing, under the Government IM, agencies are to share data with other agencies upon request if there is a valid legal basis and no national security concerns. The Government IM clearly defines the roles and responsibilities of data requestors and providers to ensure accountability and responsible data handling and usage, including assessments of whether identifiable data should be shared and is protected against loss and unauthorised use. Additionally, the Government IM establishes requirements for agencies to provide quality data that meets data standards, to ensure data is fit-for-purpose and improve interoperability across agencies.

153 MDDI and SNG introduced the GDA in 2019 to provide a shared technical foundation for data management and sharing across the public sector, with 40 agencies designated as Single Sources of Truths (SSOTs) to provide clean, verified and authoritative core data fields commonly used throughout WOG. Four designated Trusted Centres (TCs), including the Department of Statistics, process and fuse core data from SSOTs to ensure it meets baseline standards and is managed consistently. The catalogue of all core data is made discoverable to all agencies. The GDA has significantly improved data sharing across WOG for policy making, operations or service delivery, with 99% of core data requests now fulfilled within seven days.

154 As part of the GDA, central platforms have been developed to facilitate secure data sharing and data exploitation within Government. DataHive, launched in August 2024, is the internal WOG data discovery and access platform that enables users to seamlessly search,

request and access Government-owned datasets, and provides users with a set of data analytics tools. It currently serves more than 80 agencies and supports 7.9 million system queries per month on average. MDDI and SNG are progressively onboarding more datasets and users onto DataHive to make inter-agency data sharing faster and easier than existing custom bilateral arrangements.

155 MDDI and SNG have also been supporting agencies in using data for analytics through development of central tools and products, such as a fraud detection tool developed by GovTech that draws on various administrative data sources for due diligence checks in grant evaluation processes, as well as for finance/procurement checks and audits. Currently, 54 agencies use this tool, which has enabled more robust due diligence checks and time savings through automation.

156 On AI adoption, MDDI and SNG informed the Committee that they observed an increasing use of AI across agencies to enhance productivity. About 80% of the 150,000 public officers have used Pair Chat, the Government's general use chatbot, for general productivity tasks, such as assisting in drafting notes, crafting emails, summarising documents, and retrieving information. Over 9,000 officers use Transcribe, an AI-powered transcription tool, every month to transcribe meetings across multiple languages. Also, over 8,000 officers are using custom chatbot assistants every month to tackle specific tasks such as helping to answer HR-related queries and provide guidance on budget and procurement processes. In total, over 20,000 bots have been created.

157 Beyond the use of AI for routine tasks, MDDI and SNG estimate that more than half of all agencies also tap on AI to deliver more effective and efficient public services, through the following archetypes:

a. Prediction – help agencies predict and respond to events more quickly. For example, PUB's X-Band Radar System uses AI to forecast rainfall and support flood alerts for public and ground response.

b. Personalisation – enable agencies to tailor digital services to the public's needs. For example, MOE's LangBuddy provides support to students with customised practice in speaking their Mother Tongue languages, helping them improve at their own pace.

c. Anomaly detection – help agencies spot unusual or irregular activities faster and better. For example, GovTech's recursive Machine-Learning Site Evaluation (rSME), an in-house AI-powered classifier, supports the Singapore Police Force in detecting and blocking scam sites at scale.

d. Automation – allow for increased efficiency gains in delivering services to the public. MHA is piloting R-COP, a Digital Co-Pilot for Police Report Lodging, which makes the report lodging process faster and more convenient for members of the public, and reduces the extra time spent on follow-up calls by the Police.

158 Successful AI adoption across WOG requires a strong partnership between MDDI and SNG, and agencies. MDDI and SNG act as an enabler to help agencies implement AI applications that meet their operational needs. This entails establishing robust AI governance, strong digital foundations, capability development, and encouraging leadership commitment.

159 In terms of accountability and risk management, the Government, recognising both the opportunities and risks involved for new technologies, seeks to gain practical familiarity and monitor global developments before introducing regulation. When regulation is introduced, the emphasis is placed on addressing the potential harms that may arise, rather than regulating the technology itself. Accountability can generally be considered across three dimensions: **policy accountability** (e.g. clarifying policy intent, thresholds, and guiding principles or criteria for decision-making), **operational accountability** (e.g. identifying who is responsible for decisions and their implementation), and **system** (e.g. ensuring that systems align with policy and operational intent). Within this context, the WOG AI governance framework emphasises agencies' responsibility for their own AI use cases, while maintaining central oversight in certain areas, such as 'high-risk' use cases, and emerging areas such as Agentic AI. MDDI and SNG also support agencies by developing practical guidelines and technical tools to facilitate policy compliance.

160 Impactful AI deployment requires robust and reliable systems and infrastructure. MDDI and SNG facilitate this by:

a. Working with agencies to reduce tech debt and facilitating the discovery, sharing and access to high-quality, diverse datasets across WOG.

b. Providing central products on scalable and compliant platforms that accelerate AI development, reduce costs and enable easier experimentation.

c. Encouraging agencies to adopt good product practices, such as solving problems through rapid iteration on user feedback, and building teams with both technical skills and domain knowledge.

161 With regard to capability building, MDDI and SNG ensure that all key stakeholders possess both domain expertise and technological skills to harness the potential of AI through the following initiatives:

a. MDDI, SNG and CSC have rolled out a mandatory AI Literacy course for all public officers to help officers develop a baseline understanding of AI, including its limitations and risks. The curriculum will be routinely refreshed to keep pace with technological developments. For example, MDDI, SNG and CSC intend to progress public officers from simply knowing basic prompt engineering to context engineering, which involves providing the AI tool with appropriate knowledge bases and system instructions for a particular context, in order to optimise the output obtained.

b. MDDI and SNG conduct training for public service leaders on topics such as modernising systems, building better products, cybersecurity, data, and AI adoption and governance. This provides decision-makers with the baseline intuitions on necessary pre-requisites of responsible AI adoption.

c. For public sector AI practitioners, MDDI and SNG facilitate knowledge sharing and collaboration through community building initiatives such as Lorong AI, an AI community hub. Lorong AI regularly brings together policymakers and public sector AI practitioners, research/academia, and industry for talks and interaction activities.

d. MDDI and SNG facilitate partnerships between agencies and research institutions (e.g. A*STAR) and technology players (e.g. OpenAI) to help government agencies access cutting-edge capabilities.

162 Beyond the abovementioned initiatives, AI transformation requires leadership commitment to re-imagine business processes, develop a learning and experimentation culture, encourage upskilling, and address staff concerns around job displacements. MDDI and SNG will continue to support agencies in their journey to achieve impactful, sustainable and scaled implementation of AI applications.

163 MDDI and SNG recognise that the public service's ability to adopt automation and modern tools to strengthen governance and cybersecurity, enable greater data sharing, and harness AI hinges on addressing the growing challenges posed by older systems. These challenges include over-reliance on vendors for system maintenance, which has resulted in diminished in-house capabilities to understand the underlying architecture and evolution of these systems. If left unaddressed, these older systems can result in higher maintenance costs, difficulties in integrating new features, increased security risks, and ultimately become bottlenecks in the delivery of services to the public.

164 To address this, the Public Service has made the modernisation of outdated systems a priority in its digital government plans. Recognising the long-term horizon required for transformation, agencies are required to build capabilities to manage systems effectively, beyond identifying the outdated systems that need to be modernised. As mentioned in paragraph 142, the Government has implemented the MFDP to identify key digital priorities and create modernisation plans for critical systems to strengthen resilience. Several agencies, such as the Central Provident Fund Board, have successfully built and are continuing to build their own in-house digital capabilities to modernise complex systems over the years, demonstrating that investing in internal capabilities delivers sustainable, long-term value.

MINUTES OF PROCEEDINGS

1st Meeting

Friday, 7 November 2025

10.30 a.m.

PRESENT:

Ms Jessica Tan Soon Neo *(in the Chair)*
Mr Foo Cexiang
Mr Jackson Lam
Mr Victor Lye
Mr Saktiandi Supaat
Mr Dennis Tan Lip Fong
Mr Alex Yeo
Mr Yip Hon Weng

---

1. The Committee considered the Report of the Auditor-General for the Financial Year 2024/2025.

2. The Committee deliberated.

3. The Committee examined the findings contained in the Auditor-General's report and agreed to write to the Ministry of Culture, Community & Youth, Ministry of Digital Development and Information, Ministry of Education, Ministry of Finance, Ministry of Foreign Affairs, Ministry of Home Affairs, Ministry of Law, Ministry of Manpower, Ministry of Sustainability and the Environment, Ministry of Trade and Industry, Ministry of Transport, and the Prime Minister's Office to submit memoranda on the matters raised.

Adjourned to 21 January 2026.

MINUTES OF PROCEEDINGS

2nd Meeting

Wednesday, 21 January 2026

9.30 a.m.

PRESENT:

Ms Jessica Tan Soon Neo *(in the Chair)*
Mr Foo Cexiang
Mr Jackson Lam
Mr Victor Lye
Mr Saktiandi Supaat
Mr Dennis Tan Lip Fong
Mr Alex Yeo
Mr Yip Hon Weng

---

1. The following officials were examined on matters contained in the memoranda:

Ministry of Finance
(i) Mr Lai Chung Han, Permanent Secretary
(ii) Mr Adrian Chua, Deputy Secretary (Development)
(iii) Ms Esther Wee, Accountant-General
(iv) Mr Tay Ter Long, Chief of Government Procurement
(v) Ms Tan Pei Yin Sharon, Director (Performance & Evaluation) and Programme Director (Grants Governance Office)
(vi) Mr Kwa Chin Lum, Director (Fiscal Policy)
(vii) Ms Lee Mei Chern, Deputy Accountant-General

Ministry of Digital Development and Information
(i) Mr Joseph Leong, Permanent Secretary (Digital Development and Information), Permanent Secretary (Smart Nation), and Permanent Secretary (Cybersecurity), Prime Minister's Office (PMO)
(ii) Mr Chng Kai Fong, Permanent Secretary (Development), Ministry of Digital Development and Information (MDDI), and Permanent Secretary (Development)(Smart Nation)(Cybersecurity), PMO
(iii) Mr Sim Feng-Ji, Deputy Secretary (Digital Government), MDDI
(iv) Mr Goh Wei Boon, Chief Executive, GovTech
(v) Mr Justiin Ang, Assistant Chief Executive, GovTech
(vi) Mr He Ruimin, Chief AI Officer, MDDI
(vii) Mr Tan Pei-En, Senior Director (Governance and Government Data), MDDI; Assistant Chief Executive, GovTech
(viii) Mr Low Quan Ming David, Director, Legal (Smart Nation Group), MDDI

(ix) Mr Lim Thian Chin, Senior Director (Digital Governance, Strategy, Corporate & Governance), GovTech
(x) Mr Jerald Tan, Director (Strategy Policy and Resourcing), MDDI

2. The Committee considered replies received from the Ministry of Culture, Community & Youth, Ministry of Education, Ministry of Finance, Ministry of Foreign Affairs, Ministry of Home Affairs, Ministry of Law, Ministry of Manpower, Ministry of Sustainability and the Environment, Ministry of Trade and Industry, Ministry of Transport, and the Prime Minister's Office.

Adjourned to 9 February 2026.

MINUTES OF PROCEEDINGS

3rd Meeting

Monday, 9 February 2026

2.30 p.m.

PRESENT:

Ms Jessica Tan Soon Neo *(in the Chair)*
Mr Foo Cexiang
Mr Jackson Lam
Mr Victor Lye
Mr Saktiandi Supaat
Mr Dennis Tan Lip Fong
Mr Alex Yeo
Mr Yip Hon Weng

---

1. The Committee considered the further replies received from the Ministry of Foreign Affairs, Ministry of Home Affairs, and Ministry of Trade and Industry.

2. The Committee deliberated.

Report

3. The Chairman's report brought up and read the first time.

4. Resolved, "That the Chairman's report be read a second time paragraph by paragraph.".

5. Paragraphs 1 to 164 inclusive read and agreed to.

6. Resolved, "That this report be the report of the Committee to Parliament.".

7. Agreed that the Chairman do present the Report of Parliament when copies are available for distribution to Members of Parliament.

Adjourned sine die.