NATIONAL SECTOR DIALOGUE • BOTSWANA 2026

LEKGOTLA ON CYBERSECURITY AND THE FINANCIAL SERVICES SECTOR

Financial Sector Resilience, Trust and Digital Innovation

CONCEPT NOTE | 11 NOVEMBER 2026

Securing Digital Finance: Strengthening Cyber Resilience, Trust and Innovation in Botswana's Financial Services Sector

DATE	TIME	VENUE
Thursday, 3 December 2026	08:30–17:00 (CAT)	Botswana Digital and Innovation Hub, Gaborone

INITIATED AND ORGANISED BY

Pamol Trading (Pty) Ltd and Cybersec Clinique

INSTITUTIONAL ENDORSEMENT

Ministry of Communications and Innovation. The Ministry's letter dated 10 November 2026 confirms institutional support for the proposed Lekgotla, subject to the applicable administrative arrangements.

PURPOSE

A focused national platform to convert dialogue on financial-sector cybersecurity into practical cooperation, agreed priorities and an implementable cyber-resilience action agenda.

Document status: Event concept for stakeholder circulation and programme coordination. The agenda, invitees, participation and sponsorship arrangements remain subject to confirmation.

01 Executive overview

Pamol Trading (Pty) Ltd and Cybersec Clinique propose to convene a high-level, multi-stakeholder Lekgotla focused on the cybersecurity and resilience of Botswana's financial services sector. The dialogue will bring together policy-makers, regulators, financial institutions, fintech and payment providers, telecommunications operators, cybersecurity practitioners and related public-interest institutions. Its core intention is to strengthen financial-system trust and operational resilience while supporting secure digital innovation.

The Ministry of Communications and Innovation has endorsed the initiative and indicated its institutional support, including collaboration towards stakeholder mobilisation, technical engagement and appropriate representation, subject to administrative arrangements. The Ministry has also encouraged support from private-sector organisations and development partners through sponsorship, technical, logistical and other in-kind contributions.

The 08:30–17:00 programme combines policy engagement in the morning with structured technical collaboration in the afternoon. The event is designed to generate tangible post-Lekgotla outputs rather than a stand-alone awareness session: a prioritised risk register, incident coordination recommendations, an initial action plan, proposals for joint exercises and skills development, consumer protection measures and a public-private cooperation framework.

02 Background and rationale

Financial services are increasingly delivered through digital banking, electronic payments, mobile money, insurance platforms, lending technology, investment applications, cloud computing and artificial intelligence. These innovations are enabling financial inclusion, service efficiency and economic participation. At the same time, they increase the financial ecosystem's exposure to phishing, ransomware, identity theft, payment fraud, data breaches, social engineering, insider threats and attacks on infrastructure that supports essential transactions.

Cyber incidents may extend beyond the institution initially affected. Disruptions to payment systems, telecommunications services, digital identities or financial data can undermine consumer confidence and create wider operational and economic risks. Consequently, effective response requires aligned action across financial supervision, communications regulation, service providers, security agencies and industry.

Botswana's expanding digital financial ecosystem offers an opportunity to establish a more coordinated approach to prevention, detection, reporting, response and recovery. The Lekgotla will provide an institutional setting for identifying the most urgent joint interventions and assigning practical follow-up actions.

03 Purpose and specific objectives

The purpose of the Lekgotla is to examine cybersecurity challenges affecting the financial services sector and agree coordinated measures to safeguard financial systems, customer information, digital transactions and critical national economic infrastructure.

1. Assess current and emerging cyber threats affecting banks, insurers, payment providers, fintech enterprises and other financial-sector participants.
2. Examine cyber governance, risk management, supervisory coordination, legal and regulatory compliance and institutional accountability.

3. Strengthen trusted information-sharing and operational cooperation among regulators, government, financial institutions and technology providers.
4. Identify practical controls against financial fraud, phishing, ransomware, identity compromise and attacks on digital payments.
5. Explore secure adoption of artificial intelligence, cloud services, digital identity, open banking and other emerging technologies.
6. Identify joint cyber exercises, cyber-skills initiatives, research partnerships and financial-consumer awareness priorities.
7. Prepare an action-oriented financial-sector cyber resilience agenda with proposed responsibilities, timelines and progress indicators.

04 Principal discussion themes

Theme 1 | Cybersecurity, financial stability and regulatory governance

Cyber threats to financial stability; board and executive accountability; cyber-risk supervision; regulatory coordination; consistent incident reporting.

Theme 2 | Digital payments, financial fraud and consumer protection

Mobile-money fraud; account takeover; identity theft and phishing; authentication; payment monitoring; customer reporting and public awareness.

Theme 3 | Artificial intelligence, cloud computing and emerging technologies

Secure AI adoption and fraud detection; cloud and third-party concentration risks; data privacy, digital identities and outsourcing safeguards.

Theme 4 | National cyber resilience and coordinated incident response

Threat-intelligence sharing; incident escalation and coordination; business continuity; crisis simulation; ransomware and payment-system disruption scenarios.

Theme 5 | Cybersecurity investment, skills and innovation

Affordable controls for smaller institutions; local skills and research capacity; technology partnerships; shared solutions; regional collaboration.

05 Intended participants and stakeholder engagement

The Lekgotla is conceived as a cross-sector platform led by substantive, decision-oriented discussion. The original format envisages approximately ten panellists, supported by two moderators, with supplementary technical briefings and audience participation. Final individual nominations and the panel balance will be agreed through the organising process.

Stakeholder constituency	Expected contribution
Ministry of Communications and Innovation	Digital-policy perspective, national cybersecurity engagement and institutional coordination.
Bank of Botswana	Banking-system and payment-system resilience; supervisory priorities.
BOCRA	Communications regulatory matters, cybersecurity infrastructure and network-service interfaces.
NBFIRA	Cyber risks and resilience for the non-bank financial sector.

Stakeholder constituency	Expected contribution
Banks, insurers and investment-sector firms	Sector threats, governance, incident management and customer safeguards.
Fintech, mobile-money and payment service providers	Payment security, transaction fraud, interoperability and digital innovation.
Cybersecurity, cloud and telecommunications firms	Technical controls, cyber intelligence, technology risks and incident readiness.
Law-enforcement, financial intelligence and data protection entities	Investigation coordination, fraud response, privacy and consumer protection.
Universities, professional bodies and development partners	Skills, research, training, knowledge exchange and support for follow-up initiatives.

Other invitees may include the Botswana Stock Exchange, financial-sector associations, consumer organisations and relevant SADC or international experts. Inclusion here denotes proposed participation, not confirmation of attendance or institutional endorsement.

06 Event format and indicative programme

A full-day, moderated national dialogue will combine policy statements, technical briefings, sector perspectives, audience interaction, breakout working groups and recommendations. The 08:30–17:00 programme includes incident coordination, technical interventions and development of an initial action agenda during the afternoon. Timings, speakers and participation remain indicative and subject to final confirmation.

Time	Session / activity	Purpose
08:30–09:00	Registration and stakeholder networking	Arrival and participant check-in.
09:00–09:10	Welcome remarks: Permanent Secretary, Ministry of Communications and Innovation (proposed)	National context and objectives.
09:10–09:25	Opening remarks: Assistant Minister of Communications and Innovation (proposed)	Policy direction and priorities.
09:25–09:45	Technical briefing: financial sector and vulnerabilities	Shared understanding of sector risks.
09:45–10:05	Cyber threat landscape	Current and emerging cyber scenarios.
10:05–10:55	Panel I: governance and financial-sector resilience	Supervision, accountability and coordination.
10:55–11:10	Refreshment break	Informal stakeholder engagement.
11:10–12:00	Panel II: digital payments, fraud and consumer protection	Customer safeguards, detection and response.
12:00–12:30	Moderated Q&A and stakeholder interventions	Practitioner challenges and practical proposals.
12:30–13:15	Networking lunch and bilateral discussions	Cross-institution engagement.
13:15–13:45	Technical focus: AI, cloud and third-party risk	Secure innovation and operational controls.

Time	Session / activity	Purpose
13:45–14:30	Panel III: incident coordination and response	Intelligence sharing and sector resilience.
14:30–15:15	Breakout groups: priorities and interventions	Develop proposed sector recommendations.
15:15–15:30	Refreshment break	Informal engagement.
15:30–16:10	Breakout report-back and plenary synthesis	Consolidate priorities and recommendations.
16:10–16:40	Proposed action agenda and follow-up ownership	Suggested owners, steps and focal points.
16:40–17:00	Closing remarks and next-steps confirmation	Final synthesis and follow-up arrangements.

07 Expected outcomes and deliverables

The Lekgotla is intended to conclude with clearly articulated priorities and a pathway to practical implementation. The proposed output package comprises:

- **Financial-sector cybersecurity priorities:** A consolidated shortlist of critical cyber risks, control gaps and near-term areas for intervention.
- **Incident coordination proposal:** Recommendations on escalation, reporting, information exchange, regulatory liaison and law-enforcement interfaces.
- **Financial-sector cyber resilience action plan:** A preliminary matrix of actions, proposed institutional owners, indicative timelines and measurable progress indicators.
- **Joint cyber exercise proposal:** An initial scope for a tabletop or operational simulation addressing ransomware, payment disruption, data breaches and coordinated fraud.
- **Cyber skills development programme:** Priority learning requirements for executives, security professionals, compliance teams and front-line financial-services personnel.
- **Consumer awareness initiative:** Coordinated themes for financial-safety education, fraud prevention and reporting channels.
- **Public-private partnership framework:** Recommendations for ongoing, appropriately protected sharing of threat intelligence, practices and technical expertise.

08 Hosting, governance and delivery arrangements

Pamol Trading (Pty) Ltd and Cybersec Clinique will lead event organisation and coordination, including development of the programme, invitations, moderator and speaker liaison, sponsorship engagement, logistics and production of the outcomes record. The Ministry of Communications and Innovation will provide institutional support and collaborate on relevant stakeholder and technical engagement, subject to its internal administrative processes.

Workstream	Proposed coordinating responsibility
Programme, invitations and protocol	Organisers, in consultation with the Ministry and invited institutions.
Cybersecurity content and technical	Cybersec Clinique and participating technical experts.

Workstream	Proposed coordinating responsibility
facilitation	
Project management and operations	Pamol Trading and the organising secretariat.
Venue, AV, registration and hospitality	Organising secretariat with the venue and confirmed supporters.
Communications and branding	Organising secretariat; institutional names and emblems only with relevant approval.
Outcomes report and follow-up	Organising secretariat with nominated stakeholder focal points.

The Ministry's 10 November 2026 correspondence additionally advises engagement with the Department of Communications Infrastructure and Business, which has responsibilities relating to national cybersecurity. That liaison should be incorporated into the organisers' coordination arrangements.

09 Private-sector sponsorship and partnership

Consistent with the Ministry's endorsement letter, financial institutions, telecommunications operators, technology firms, professional associations and development partners are encouraged to contribute to the delivery of the Lekgotla. The intention is to mobilise resources and expertise without compromising the independence of the event's public-interest discussions.

- Financial sponsorship towards agreed venue, audiovisual, programme, documentation, catering and participant-support costs.
- In-kind assistance, including meeting facilities, connectivity, equipment, registration systems, event services or specialist personnel.
- Technical contributions such as speaker participation, incident-simulation support, cybersecurity training resources and knowledge-sharing.
- Post-event support for the agreed action plan, cyber-skills initiatives, financial-consumer awareness or future sector exercises.

Sponsorship opportunities, budgets, recognition benefits and contribution mechanisms will be documented separately by the organisers. Sponsorship does not confer regulatory approval, public procurement advantage, institutional endorsement or decision-making authority over government or supervisory bodies.

10 Follow-up and measures of success

Following the Lekgotla, the secretariat proposes to circulate a concise outcomes report, consolidate stakeholder observations, seek confirmation of proposed action owners and convene a follow-up technical engagement to advance the cyber resilience agenda.

Success indicator	Proposed evidence of delivery
Cross-sector participation	Attendance and representation across the principal stakeholder groups.
Quality of dialogue	Structured record of panel, audience and breakout contributions.
Actionable outputs	Seven deliverables presented or advanced in the outcomes report.
Institutional continuity	Identified focal points and agreement on next coordination steps.
Private-sector contribution	Transparent record of confirmed cash and in-kind contributions.

11 Confirmation items before publication

The following remain to be finalised through the organising and institutional coordination process: confirmation of the venue booking, Ministry speakers and official protocol, invited regulators' and institutions' participation, final panel and moderators, the 08:30–17:00 programme, sponsor commitments, budget and approval to reproduce official institutional logos in event material.

12 Pre-event finalisation register

For circulation control, the organising secretariat will confirm the following items before release of final invitations and publicity materials:

Item	Required confirmation / action
Programme and event publicity	Publish event information with the confirmed event time of 08:30–17:00.
Institutional protocol	Confirm Ministry speakers, remarks, protocol requirements and the departmental liaison.
Venue and operations	Confirm venue booking, audio-visual requirements, registration, catering and accessibility.
Speakers and participation	Confirm panel composition, moderators, invited institutions and speaker briefings.
Partners and finance	Confirm sponsorship commitments, contribution records and event budget.
Emblems and acknowledgements	Obtain relevant approvals for use of institutions' names, logos and acknowledgements.

Reference materials

Original event proposal; event artwork LEKGOTLA_C.pdf; and Ministry of Communications and Innovation endorsement letter dated 10 November 2026 (Ref. MCI 1/7/3 I (13)).