Key Takeaways

- Emerging Risk and Stress Testing.

1. Renewable Energy – Emerging market for batteries for Solar Storage & electronic vehicle, new technology of satellite data along with drone usage in plantation industry is on the rise.

2. Geopolitical Risk– Expect inflation on price of Oil & gas and raw materials for EV, post election census between countries could lead to cold war and with that economic volatility is speculated , which could lead to FOREX fluctuation

3. Regulatory Compliance – Increased Reg guidelines on AML and counter-terrorism act, beneficiary ownership is also the need of the hour and with that Disclosure Management and COI (Conflict of Interest) will be on the rise

4. Stress Testing – Ensure data-availability (financial/non-financial) before conducting Stress Test, explore on the best available tools to conduct stress test.

Key Takeaways

- Technology Risk Insights and Cybersecurity Insurance.

1. Risk Segregation – For better management & mitigation of technology risk , practising segregation of risk by impact and various categories is the best practise and organization are advised to follow the same.

2. Regulatory Compliance on Tech Risk – Increased Reg guidelines on AML and counter-terrorism act, beneficiary ownership is also the need of the hour and with that Disclosure Management and COI (Conflict of Interest) will be on the rise.

3. Training & Awareness – Industry leaders must have a robust training and awareness culture built up for their organisation, practises to measure the program is also crucial

4. New Tech laws by Regulation – E-invoicing for various invoices will be the new need of the hour, it facilities government for better ways to govern tax collection, there are various new laws on energy consumption

5. Align Strategy – Ensure organization business strategy is aligned with technology risk implementation, it is key to decide to adapt or not to adapt to certain technology implementation

Key Takeaways

- Technology Risk Insights and Cybersecurity Insurance.

6. Change Management – Organization are advised to leverage technology, do not expect technology to solve critical problems if you are not aligning correct data, process and controls to right tech stack, ensure a robust change management process for your technology programs.

7. Rehearse Regulation – Bank Negara and security commission rehearsed regulation on Third-party risk management programs.

8. Resource – Ensure availability and presence of the relevant talent pool while implementing key technology for your organization, skill factor of resources ensures success for critical tech implementation.

9. Cyber Security Control Framework– Ensure best practices of implementing cyber sec control framework to mitigate key IT Risk. Conducting regular audits on Cyber sec framework is a must need for all major organization for a resilient cyber sec program.

10. Test your Cyber Security program – Ensure Stress Testing conducted at regular interval on your cybersec framework to address new vulnerabilities , conduct Penetration Testing of your cybersec programs

Key Takeaways

- Technology Risk Insights and Cybersecurity Insurance.

6. Cyber Insurance – It is still an expensive unknown maze, explore various cyber security agencies to analyse the best insurance for your organization , conducting correct testing (Stress Test, Pen Test) will provide leaders with a negotiation ground for lowering the premium for the cybersec insurance.

7. Enhanced Operational Resilience – Form a dedicated team to handle Crisis Communication, Disaster Recovery, and Business Continuity, and clearly define key terms like Event, Incident, and Crisis. Budget for testing and improvements, and strengthen Vendor/Supplier Management to mitigate impacts of country sanctions and inflation.

Key Takeaways

- GEN AI – Usage and its challenges.

1. Gen AI Controls – Watch out for various GEN AI controls before industry adapts GEN AI, measure cost and vulnerability before adapting GEN AI Programs

2. Talent – Having the right Talent for execution of GEN AI in your organization is key, watch out for new talents on GEN AI

3. Comprehensive Cyber Attack Crisis Procedures - Develop robust, tested crisis procedures for cyberattacks, considering vulnerabilities, likelihood, asset impact, root causes, solutions, stakeholder communication, data protection, and thorough incident reporting

MODERATOR: Tanay Ghosal
GRC Partners Asia
Email - tanay.ghosal@grcpartnersasia.com