

AN EXERCISE IN SUCCESSION PLANNING FOR OUR ISO

Institution Name:

Date:

Purpose: To ensure seamless continuity in our information security leadership, we conducted a table-top exercise addressing the following key areas:

Key Area	Question	Response
Reviewing Past Activities	Have all security tasks been recently evaluated?	
	Are all policies and critical documents current and accessible?	
	Is there a documented history of resolved security incidents?	
	How are past security breaches analyzed for continuous improvement?	
	What is the process for ensuring all stakeholders are aware of their responsibilities?	
Auditing & Preparing for Examinations	What is the status of upcoming audit schedules and regulatory exams?	
	How can we improve our exam readiness?	
	Have we identified areas of potential non-compliance?	
	Are audit findings and recommendations being tracked and resolved promptly?	
	Is information security training up to date for all relevant personnel?	
Innovating & Automating Processes	Which manual security tasks can be automated?	
	How can technology be utilized to innovate current processes?	
	What automation tools or solutions are we currently considering?	
	How is automation monitored for effectiveness and efficiency?	
	Are there opportunities for improvement in our current automation processes?	

<i>Key Area</i>	<i>Question</i>	<i>Response</i>
<i>Securing Access Management</i>	Is there a current list of all individuals with system access privileges?	
	How do we monitor and control access to prevent unauthorized use?	
	What protocols are in place for emergency access revocation?	
	How is user access audited and reviewed for appropriateness?	
	Are access management processes tested regularly for integrity?	
<i>Assessing & Strengthening IT Controls</i>	Are our IT security controls effectively implemented and documented?	
	When was the last assessment, and what were the findings?	
	How frequently are IT controls reviewed and tested?	
	What process is in place for updating IT controls in response to new threats?	
	How are IT control deficiencies prioritized and addressed?	
<i>Enhancing Cyber Insurance Coverage</i>	When was the last review of our cyber insurance questionnaire?	
	Are there any gaps in our current cyber insurance coverage?	
	How do we ensure our cyber insurance is aligned with our risk profile?	
	What is the process for filing and following up on cyber insurance claims?	
	How are cyber insurance requirements communicated to all departments?	
<i>Maintaining Vendor Communications</i>	How are we managing transitions in vendor relationships?	
	Are there ongoing security projects that need to be reassessed?	
	How do we evaluate new vendors for security compliance?	
	What mechanisms are in place for regular communication with critical vendors?	

<i>Key Area</i>	<i>Question</i>	<i>Response</i>
	How is vendor performance measured against security requirements?	
<i>Evaluating Succession Candidates</i>	Do we have personnel identified in our plan for all key IS and Cybersecurity roles?	
	Who are the planned successors?	
	Have personnel identified in our plan been evaluated for the role in terms of temperament and skills?	
	How are areas that need to be enhanced being addressed to ensure a successful transition?	
	What ongoing support will be provided to ensure a successor remains updated on evolving threats and requirements?	
<i>Seeking External Expertise</i>	Do we have contacts with specialized consultants or advisors for enhancing our oversight process?	
	What external resources are we currently utilizing?	
	What criteria are used to select external advisors?	
	How do we ensure the external advice is aligned with our strategic objectives?	
	How are external reviews incorporated into our security strategy?	
<i>Improving Governance Reporting</i>	Are our governance reports actionable and insightful for our Executive Team?	
	How can we improve the clarity and impact of these reports?	
	Are there feedback mechanisms in place for governance reporting?	
	What is the frequency of reporting to stakeholders?	
	How do we measure the effectiveness of our governance reports?	
<i>Utilizing Centralized Data Technology</i>	What technology is in place to centralize critical data and processes?	
	How does this technology enhance task efficiency and repeatability?	

<i>Key Area</i>	<i>Question</i>	<i>Response</i>
	What data governance measures are we implementing?	
	How is data quality maintained in centralized systems?	
	What training is provided for staff on utilizing centralized data systems?	