Cyber Resilient Government Organization of the Year 2024

This is an award bestowed upon a government organization that demonstrates exceptional resilience in the face of technological challenges and disruptions.

This prestigious accolade recognizes government organizations that have implemented robust technology infrastructure, effective cybersecurity measures, and comprehensive disaster recovery plans to ensure continuity of operations and safeguard against cyber threats.

The recipient of this award exemplifies a commitment to innovation, adaptability, and proactive risk management in navigating the evolving landscape of technology.

This award celebrates excellence in technology resilience and serves as a testament to the recipient's dedication to maintaining a secure and resilient technological environment.

The application closing date is Wednesday, March 6, 2024. The judging interview details for the award will be shared only with shortlisted applicants.

*This award is recognized with the support of Sri Lanka CERT. For further information, please contact Mr. Nirosha Ananda at nirosha@cert.gov.lk.

Note: The full PDF version of the application is available at the following link: https://enapp.d.isaca.org/srilankachapter/digit-awards

Disclaimer:
The “Cyber Resilient Government Organization of the Year 2024” award is conferred based on the information provided by the awardee during the application process. While every effort is made to verify the accuracy and authenticity of the information provided, the receipt of this award does not serve as a validation or endorsement of the organization by ISACA Sri Lanka Chapter. The decision to grant this award is dependent on the completeness and accuracy of the information provided by the applicant. ISACA Sri Lanka Chapter assumes no responsibility for any inaccuracies or misrepresentations in the application materials submitted by the awardee.

* Required

Online Form Disclaimer:
Before proceeding, please review the following disclaimer carefully:
1. **Accuracy of Information**: By submitting this form, you certify that all information provided is true, accurate, and complete to the best of your knowledge. Any falsification of information may result in disqualification from the award.

**Confidentiality**: We understand the sensitivity of certain information provided in your application. We will treat all information with strict confidentiality and only use it for the purposes of evaluating your application for the awards. However, please be aware that some award categories may require public presentation of certain information about the nominated individual or organization. We will notify you in advance if any information you provide becomes part of the public record.

**Use of Information**: By submitting your application, you grant ISACA Sri Lanka a non-exclusive, royalty-free license to use, reproduce, modify, publish, and distribute the information related to you (not limited to name, role, designation), your company (including the logos) solely for the purposes of evaluating your application and promoting the Digital Trust Awards 2024.

**Disclaimer of Liability**: ISACA Sri Lanka accepts no liability for any loss, damage, or inconvenience arising from the use of information contained in this application form or participation in the Digital Trust Awards 2024.

**Judging Process**: The decision of the judging panel is final and binding. No appeals or correspondence regarding the judging process or outcome will be entertained.

**Data Privacy**: Any personal data collected through this form will be used solely for the purpose of administering the award and will be handled in accordance with applicable data protection laws and regulations. You can find more information about our data privacy policies at [http://isaca.lk/privacypolicy](http://isaca.lk/privacypolicy).

**Verification**: ISACA Sri Lanka reserves the right to verify the information provided in this form and may request additional documentation or evidence to support your submission.

**Disqualification**: ISACA Sri Lanka reserves the right to disqualify any submission that is incomplete, inaccurate, or does not comply with the eligibility criteria specified for the award.

**Award Results**: Participation in this award program does not guarantee winning an award. Awards will be granted based on the merit of the submissions and the decision of the judging panel.

**Compliance**: By submitting this form, you agree to comply with all terms and conditions outlined in this disclaimer and any other rules or guidelines set forth by ISACA Sri Lanka for the award program.

**Changes to these Terms**: ISACA Sri Lanka reserves the right to modify these terms and conditions with prior notice to the applicants. Your continued use of the application form constitutes your acceptance of any amended terms.

By selecting “Agree” and proceeding further, you acknowledge that you have read, understood, and agree to the terms outlined in this disclaimer.

If you have any questions or concerns regarding this disclaimer, please contact us at [president@isaca.lk](mailto:president@isaca.lk).

☐ Agree
Authorization Letter for Application Submission

This is to formally confirm your participation in the application process. This document verifies that the designated person, possesses the company's full approval to submit an application for the Digital Trust Awards 2024.

The letter further reaffirms that all information provided within the application, submitted on date, is accurate and complete to the best of our knowledge.

Additionally, it expresses your firm belief that your company's qualifications and experience align perfectly with the program's objectives, and we are confident in making a meaningful contribution.

2. Authorization Letter Template and Upload *

Please refer to the template here https://higherlogicdownload.s3.amazonaws.com/ISACA/980b767e-4fbd-1d6b-8887-672b425b917a/UploadedImages/Events/Digit/Templates/Authorization_Letter_for_Application_Submission.docx

and submit signed letter on your company letterhead following URL https://sacalk-my.sharepoint.com/:f:/g/personal/ijakmal_isaca_ik/EpbdvCD7XKvMhjPhyoeF580WcYPlgSh5snw8M1FX9mA

Checkbox: Authorization Letter for Application Submission Uploaded
Details of the Government Organization

3. Organization Name *

4. Size of the Organization *
   Provide Details of the Number of Employees, Number of Branches, etc.
Overview of the Organization

5. **Services**: Details about the products or services offered by the organization. *
Designated Contact Person

6. Name *
   
7. Designation / Job Title *
   
8. Direct Email Address *
   
9. Mobile Number *

The value must be a number
Preparedness

Preparedness refers to the state of readiness to address and mitigate potential risks or disruptions effectively. It involves having robust systems, protocols, and plans in place to anticipate, prevent, respond to, and recover from various challenges, such as technological failures, cybersecurity threats, or natural disasters. Preparedness encompasses proactive measures such as risk assessments, contingency planning, training programs, and the establishment of recovery time objectives to ensure business continuity and resilience.

10. **Technology Infrastructure**: How would you describe your organization's current technology infrastructure? *

   Briefly describe / illustrate your technologies, avoiding sensitive information. Judges can ask for details during the session.

11. **Technology Infrastructure**: Can you provide details on the redundancy and failover systems in place? *

   Briefly describe / illustrate your technologies, avoiding sensitive information. Judges can ask for details during the session.

12. **Cybersecurity Measures**: What cybersecurity measures are implemented to protect against potential threats? *

13. **Cybersecurity Measures**: How frequently is the cybersecurity strategy reviewed and updated? *

14. **Data Backup and Recovery**: Describe your organization’s data backup and recovery processes. *
15. **Data Backup and Recovery:** How often are data backups performed, and what mechanisms are in place for swift recovery? *

16. **Multitasking and Redeployable Employees:** Describe how your company fosters and empowers multitasking and redeployable employees, enabling them to adapt to changing technical challenges and unforeseen circumstances. Provide specific examples of situations where this adaptability and skill diversification contributed to organization operations or strategic goals. *
Adaptable

Adaptable organizations have the ability to respond and adjust to changes in their environment, whether they are technological advancements, market shifts, or regulatory requirements. Being adaptable means being flexible, innovative, and open to adopting new technologies, processes, or strategies to stay competitive and relevant. Adaptable organizations continuously monitor trends, seek feedback, and iterate on their approaches to optimize performance and adapt to evolving circumstances effectively.

17. **Adaptability to Technological Changes**: How does your organization stay informed and adapt to emerging technological trends? *

```

```

18. **Adaptability to Technological Changes**: Share an example of a recent successful technology adaptation in your organization. *

```

```

19. **Continuous Improvement Initiatives**: Share examples of ongoing initiatives aimed at continuously improving your organization's technology resilience. *

```

```

20. **Continuous Improvement Initiatives**: How does your organization learn from past incidents to enhance future technology resilience? *

```

```

https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&id=XdtxFw9RTEw4JX5SZ_djVxVhP-lEj-M_1SEP… 9/13
Collaborative

Collaboration entails working together with internal and external stakeholders, including employees, partners, suppliers, customers, and regulatory bodies, to achieve common goals and solve shared challenges. Collaborative organizations foster open communication, trust, and mutual respect among stakeholders, encouraging knowledge sharing, joint problem-solving, and collective decision-making. Collaboration enhances innovation, efficiency, and resilience by leveraging diverse perspectives and resources to address complex issues comprehensively.

21. **Supplier and Vendor Resilience:** How do you assess and ensure the technology resilience of your key suppliers and vendors? *

22. **Supplier and Vendor Resilience:** Share an instance where your organization effectively managed a disruption caused by a third-party technology failure. *
   Briefly describe / illustrate your technologies, avoiding sensitive information. Judges can ask for details during the session.

23. **Employee Feedback and Involvement:** How does your organization encourage employees to provide feedback on technology-related issues? *
Trustworthy & Responsible

Trustworthiness and responsibility are fundamental principles that guide ethical behavior and integrity in organizations. Trustworthy and responsible organizations prioritize transparency, honesty, and accountability in their actions, interactions, and decision-making processes. They adhere to legal and ethical standards, respect the interests and rights of stakeholders, and uphold commitments to safety, security, and sustainability. Trustworthy and responsible organizations earn trust and credibility from stakeholders, fostering long-term relationships and reputational resilience.

24. **Customer Communication during Disruptions**: Describe the communication strategy in place for informing customers about technological disruptions. *

25. **Customer Communication during Disruptions**: Provide an example of a situation where your organization effectively communicated with customers during a technology-related incident. *

26. **Regulatory Compliance**: How does your organization ensure compliance with relevant technology-related regulations? *
Governance

While these questions may not be formally evaluated, they serve as a valuable diagnostic tool for organizations to assess their IT governance maturity. ISACA Sri Lanka, as a leading IT governance association, can help organizations thrive in this area by:

- **Providing educational resources and training:** ISACA Sri Lanka offers various programs and certifications to equip board members and executives with the necessary IT knowledge and skills.
- **Developing and promoting best practices:** ISACA's COBIT framework provides a globally recognized framework for IT governance, helping organizations implement best practices.
- **Building a community of experts:** ISACA Sri Lanka fosters a network of IT governance professionals, facilitating knowledge sharing and collaboration.
- **Advocating for effective IT governance:** ISACA Sri Lanka raises awareness about the importance of IT governance and advocates for strong governance practices through publications, lobbying, and research.

27. Strategic Integration: How does your organization's vision, mission, strategy, and goals explicitly consider and promote technology resilience?

28. Strategic Integration: Can you illustrate specific examples of how technology resilience plays a role in key organizational decisions?

29. Measurement and Performance: Beyond qualitative descriptions, does your organization utilize defined KPIs to assess and measure the effectiveness of its technology resilience efforts?

30. Measurement and Performance: Share specific examples of these KPIs and how they are used to track and drive progress?

31. IT Strategy & Alignment: How does your IT strategy actively address and contribute to building organizational resilience against potential threats and disruptions?
32. Implementation and Progress: With specific examples, describe the current implementation status of your IT strategy, highlighting both progress achieved and any challenges encountered.

33. Implementation and Progress: How do you ensure effective execution and ongoing monitoring of your IT strategy, adapting to industry trends and evolving regulatory requirements?

34. Forward-Looking Insights: Based on your understanding of emerging technologies and future trends, what are your plans for continuously enhancing your organization's technology resilience?

35. Forward-Looking Insights: How do you foresee adapting your IT strategy and implementation to address potential disruptions and ensure consistent alignment with your organization's long-term goals?