SEPTEMBER - 2021 ISSUE

ISACA
Bangalore Chapter

# INFOCITY AUDITOR

## *ISACA Bangalore Chapter - News Letter*


*24th Annual Karnataka Virtual Conference held on 04th September 2021*

## PRE-CONFERENCE FREE TRAINING & SILVER JUBILEE CELEBRATION

ISACA Bangalore Chapter – 03 Sep 2021

**Pre-Conference Free Training for Bangalore Chapter Members – Session Agenda -**

**Ransomware Incident Investigation and Resolution demonstration –**

**Mufaddal Taskin** | Cyber Technical Trainer, Cyberbit

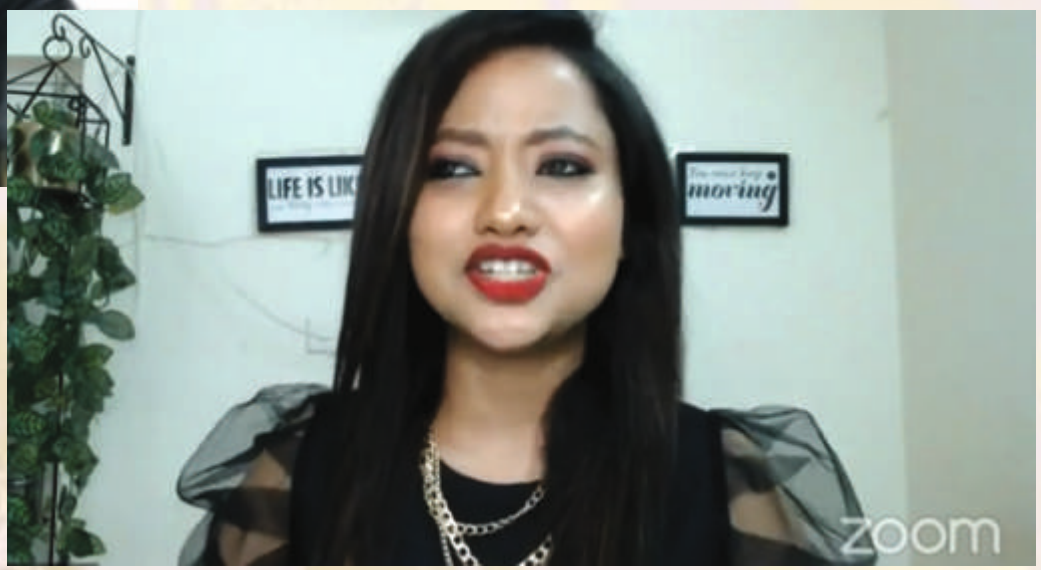
**3rd Sept 2021 – 14:00 – 16.30 PM**

**Silver Jubilee Celebration**

**AGENDA**

| TIME (IST) | Silver Jubilee Gala Event | |
|---|---|---|
| 17:00 | Silver Jubilee Gala Event curtain Opens at 17:20 PM | MC - Rukhmini Saha |
| 17.30 to 17:40 | Welcome Address by ISACA Bangalore Chapter President | Mr. Velmuruga Venkatesh |
| 17:45 | Program start with lighting the digital lamp and devotional song | |
| 17.50 to 18:10 | Silver Jubilee @ Special messages – ISACA Bangalore chapter Presidents | Past Presidents |
| 18:10 to 18:40 | Celebrating abilities- soulful performance by Razi fame Ananya Halankar, Artist on the Autism spectrum* | Ananya Halankar |
| 18:45 to 20:00 | Interactive mind tickling program - Reading your security program and mind by renowned mind reader Mr. Rakesh Syam | Mr. Rakesh Shyam |
| 20:00 to 20:15 | Games by MC - Rukhmini | MC |
| 20:15 to 20:30 | Wrap-up & Vote of Thanks | Mr. Vaidyanathan Iyer |

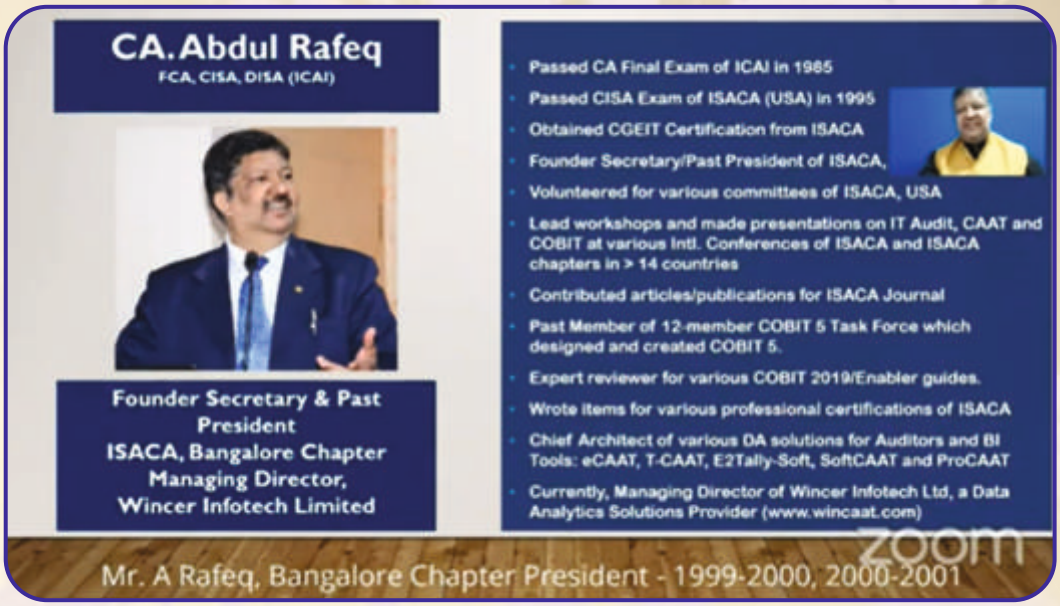
**VELMURUGA VENKATESH**
President, ISACA Bangalore Chapter




**RUKHMINI SAHA**
Host


**Mr. Anil Jogani**
***Bangalore Chapter President***
***1995-1996, 1996-1997***

**Mr. A. Rafeq**
***Bangalore Chapter President***
***1999-2000, 2000-2001***





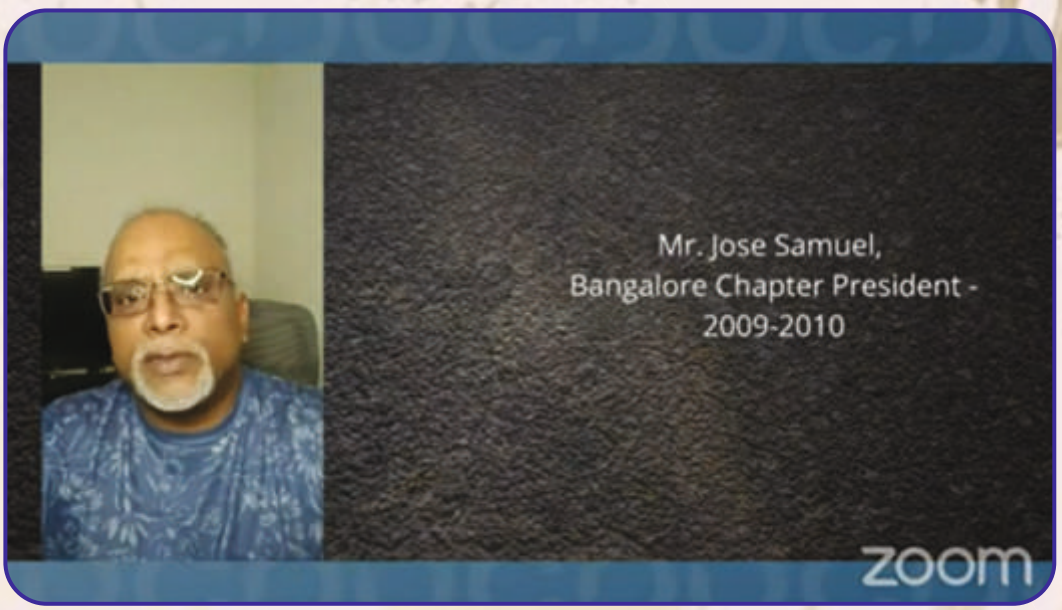
**Mr. G. Dwarakanath**
***Bangalore Chapter President***
***2001-2002***


*Soulful Performance by Razi fame*
**Ms. Ananya Halankar**
*Artist on the Autism spectrum"*

**Mr. Raghavendra Rao H.**
*Bangalore Chapter President*
*2005-2006*

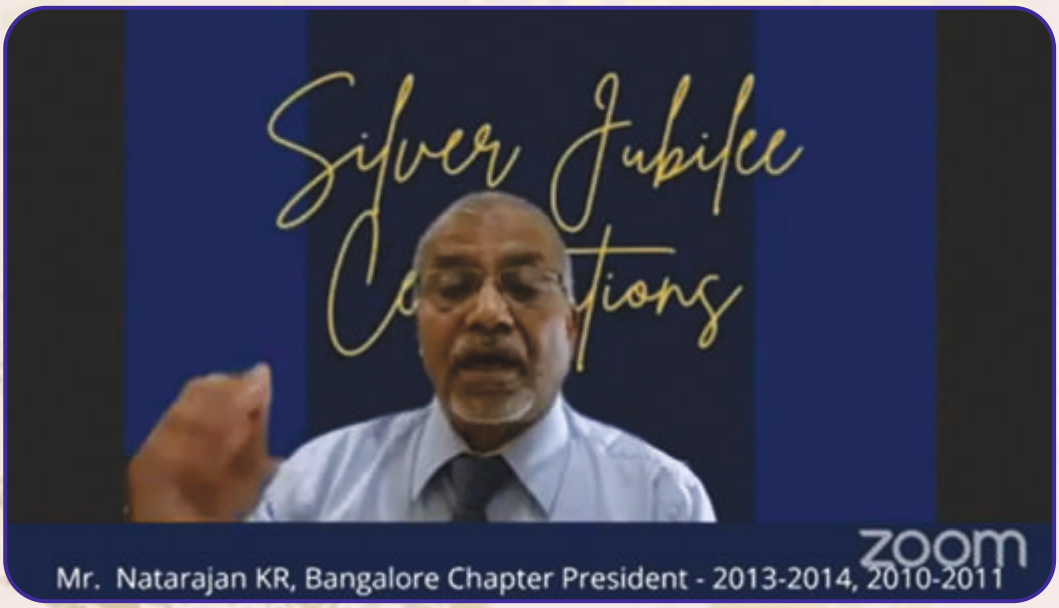


**Mr. Manjunatha Babu A.**
*Bangalore Chapter President*
*2008-2009*




**Mr. Jose Samuel**
***Bangalore Chapter President***
***2009-2010***

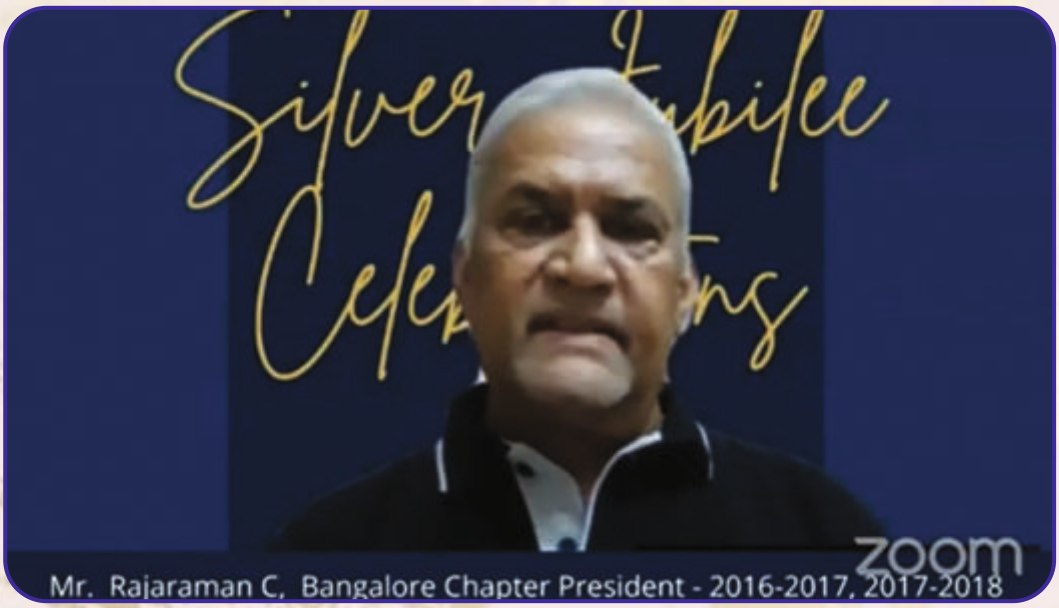
***Interactive mind tickling program***
**Rakesh Shyam**
***Reading your security program and mind by renowned mind reader.***


**Mr. Natarajan KR**
***Bangalore Chapter President***
***2010-2011, 2013-2014***


**Mr. Sarat Chegu**
***Bangalore Chapter President***
***2011-2012***

**Mr. Shashidhar CN**
***Bangalore Chapter President***
***2012-2013***


**Mr. Rajaraman C.**
***Bangalore Chapter President***
***2016-2017, 2017-2018***

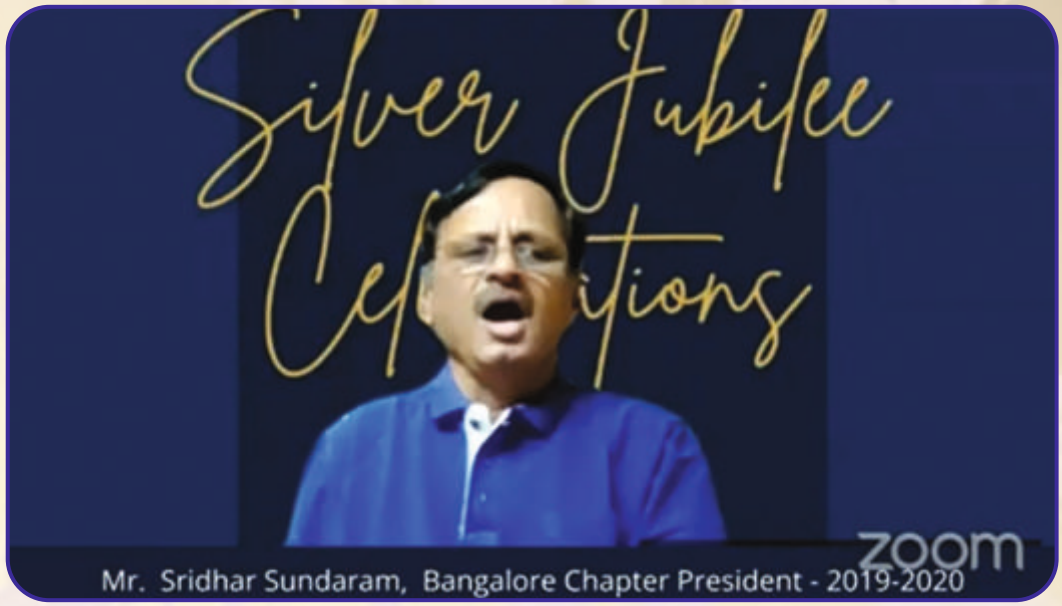

*Interactive mind tickling program*

**Rakesh Shyam**

***Reading your security program and mind by renowned mind reader.***

**Mr. Sridhar Sundaram**

***Bangalore Chapter President***
***2019-2020***





*Vote of Thanks by :*

**Mr. Vaidyanathan Iyer**

***Program Director***
***ISACA Bangalore Chapter***

# 24TH ANNUAL KARNATAKA CONFERENCE

## ISACA Bangalore Chapter - 24th Annual Karnataka Virtual Conference – 04 Sep 2021 ( 9 AM – 6PM)

**Theme: Digital Transformation - Saviour for Pandemic and Cybersecurity**

| TIME (IST) | SESSION AGENDA | SPEAKER |
|---|---|---|
| 08:30 | Conference Bridge Opens | |
| 09:00 to 09:10 | Welcome Address by ISACA Bangalore Chapter President – – Mr. Velmuruga Venkatesh | |
| 09:10 to 09:15 | Welcome address by Conference Chair – ISACA Bangalore Chapter Vice President – Mr. Rajasekharan | |
| 09:15 to 10:00 | Chief guest and Keynote speaker (MC to consider the time for lightening the lamp and cultural song) | Mr. Arindam Banerji, Executive Vice President & Managing Director, India & Philippines, Wells Fargo & Company |
| 10:00 to 10:15 | Message from ISACA, CEO | Mr. David Samuelson, CEO, ISACA |
| 10:15 to 11:00 | The remote workforce Cyber problem – Resistance to adoption | Mr. Debashish Jyotiprakash , CTSO, Qualys Inc |
| 11:00 to 11:15 | Tea Break | |
| 11.15 to 12.00 | Managing the evolving threat landscape – Effective Strategies to stop attacks and to stay ahead of breaches | Mr. Ashok Prabhu , Chief Executive – Sales and Mr. Bobby Sandeep, AVP Technology, Value Point |
| 12:00 to 12:45 | Cyber Risk in a Post Pandemic Era - Trust Nothing, Distrust Nothing | Mr. Krishnanand N. Bhat, Director, Technology advisor, Nexdigm (SKP), |
| 12:45 to 13:30 | Building a Next Generation Cloud Native Smarter SOC | Mr. Anand Trivedi, APAC - Business Head, UST Global |
| 13:30 to 14:00 | Lunch Break | |
| 14:00 to 14:45 | No more Ransomware Strike – With SuperHuman AI Cybersecurity Defense | Mr. Yashaswi Mudumbai, Technical Director - India & SAARC, Sentinel One |
| 14:45 to 15:30 | Key Inflection Points on your Journey to XDR | Mr. Setu Kulkarni, VP Corporate Strategy & BD – Whitehat security US / NTTS |
| 15.30 to 15:45 | Tea Break | |
| 15.45 to 16:30 | Preparing the Next Generation of Cybersecurity Professionals. Sidharth Mutreja, Cyberbit, Regional Director- SE- South Asia & ASEAN | |
| 16:30 to 17:30 | Panel Discussion - **Security transformation for digital transformation- Challenges and approach**<br>Vaidyanathan Iyer, COO IBM Cybersecurity Command Center(Moderator)<br>1. Mr Pawan Desai, CEO Mitkat Advisory<br>2. Mrs. Seema Bangera, Independent Cyber Security Consultant<br>3. Mr Damanjit S. Uberoi., Executive Director, Grant Thornton<br>4. Mr. P C Joseph, independent Consultant & Academic Researcher | |
| 17:30 to 18:00 | Wrap-up & Vote of Thanks | |

Earn 8 CPEs


*Welcome Address by ISACA Bangalore Chapter President – Mr. Velmuruga Venkatesh*


*Welcome address by Conference Chair – ISACA Bangalore Chapter Vice President – Mr. Rajasekharan*


*Chief Guest & Keynote Speaker*

ISACA Bangalore Chapter

InfoclTy Auditor

September - 2021

# From The Desk Of The President

Dear Members,

Greetings of the day to you!!!!

We had an overwhelming response and participation for our Silver Jubilee Celebrations and for our 24th Annual Karnataka Conference with the theme "**Digital Transformation - Saviour for Pandemic and Cybersecurity"** which was held on the 3rd of September, 2021 (Silver Jubilee Celebrations) and 4th September, 2021 for the Annual Karnataka Virtual Conference. The much awaited Silver Jubilee celebrations took place in the virtual platform. It was a well planned and executed program. We had the opportunity to hear from our Past Presidents, hosted loads of programs for our members. It was a well received and celebrated evening. 4th Sep was another big day, where we had our stalwart speakers talking through the Conference theme. We engaged a vendor and executed the same for the first ever time in the history of ISACA Bangalore Chapter.

It is that time of the year where we would be meeting as a team to go over the entire year's performance and plan some of the new requirements that would help our Chapter's growth. Yes, we are referring to the Annual General Meeting (AGM) which is scheduled to take place on the 30th of Oct 2021. We are looking forward to meeting you all and taking the inputs and suggestions on the way forward and also glad to seek your support in helping us to elect the new Executive Committee for 2021-2022.

This year was filled with loads of activities. We have tried our best to get maximum value add to the Members during the COVID situation. We had conducted series of virtual events on:

- Intro Seminars
- CPE Meets
- Review classes
- Short Learning Bytes (SLB)
- Workshop

My sincere thanks to all the members and the colleagues in the Executive Committee for providing excellent support in the entire Chapter related activities. The current team will sign-off post the AGM and the new team will be in place for the next term starting 31st of October 2021.

Looking forward to meeting you all at the Annual General Meeting!!!!!

Stay Safe and Stay Healthy!!!!!

Warm Regards,

**VELMURUGA VENKATESH,** CRISC, CDPSE, COBIT-5 (F), ISO 27001 LA, ISO 31000 CRM
President

# *Message From the Vice President*

Dear Friends,

Greetings!!

We hope this message finds you healthy and happy, we know these are trying times, please take the necessary precautions to help ensure your health and safety and that of your loved ones.

We had a fantastic Virtual Silver Jubilee celebration and Annual conference. I believe most of you have attended and those who have missed, watched the recorded session of 25th ISACA conference held virtually on 4th Oct 2021 on a 3D platform. The theme was '**Digital Transformation - Saviour for Pandemic and Cybersecurity'.** The conference was attended by more than 500 participants**.**

Mr. Arindam Banerjee, MD CEO Wells Fargo was the Chief Guest and keynote speaker for the annual conference. We had several speakers from various sectors of industry from India and abroad presenting a variety of topics relevant in the cybersecurity domain. A power packed panel discussion with experts from the industry on **'Security transformation for digital transformation - Challenges and approach'.**

The gala event as part of silver jubilee feedback was marvelous with renowned mind reader Mr. Rakesh Syam and Celebrating abilities - soulful performance by Razi fame Ananya Halankar, artist on the Autism spectrum". The special messages from past ISACA Bangalore Chapter Presidents recorded session was nostalgic and gave motivation to all members who associate with the Chapter.

Our Chapter continues to engage members and provide value to members through online CPE sessions. We experienced members are attending these online sessions with good active participation and engagement. Thank you all including our speakers for your active support and participation.

As part of community day on Oct 2, few members from the Chapter visited the **Sparsha Trust**. The goal of the **Sparsha Trust** is 'to touch a needy' and for over a decade and half the team has been helping such deprived kids to live a life of entity, hope, and respect. Our chapter volunteers interacted with children and donated clothing for needy children.

Lastly and before I sign off, I would like to say a huge thank you to our Chapter EC, members & sponsors for all its hard work throughout the last few months for making a fantastic silver jubilee and 24th Annual Karnataka Conference.

Our AGM is scheduled on 30th Oct 21 and request all to attend the AGM and see you in AGM.

I am sure we are moving steadily, transitioning into a brighter future.

Regards,

**RAJASEKHARAN K R,** CISM, CDPSE®, PMP, ITIL (E), CSM, SAFe, ISO 27001 LA
Vice President

# Message From Secretary

Dear Bangalore Chapter Members,

Hopefully this newsletter finds everyone well and enjoying a busy festival season.

India is finally seeing the light at the end of the dark COVID-19 tunnel. The chances of a third Covid-19 wave appear remote under the "present circumstances" with only the Delta and its derivatives as the main SARS-CoV-2 variants in circulation and the weekly caseload dropping steadily, as per experts. With favourable stats and the increase of vaccines administered, Bangalore city is finally opening up. However, continue to practice safe measures, wear a mask and practice social distancing.

In September 2021, the Chapter commemorated its 25th year Silver Jubilee Celebration. The purpose of this event was to recognize our Past Presidents. The Past Presidents shared their experiences with participants during the celebrations. A BIG THANK YOU to all our Past Presidents.

This year's Annual Karnataka Virtual Conference in September 2021 themed as **"Digital Transformation - Saviour for Pandemic and Cybersecurity"** was a huge success. The Conference was attended by 535 delegates. The conference session included national and international speakers from various industry presenting on a variety of topics. Very positive feedback was received from delegates of the conference.

Finally, it is hard to believe the Chapter year is coming to an end in a few days, and we are done!

BOARD ELECTIONS……. GET READY TO VOTE!

You all, as the members of the Bangalore Chapter, would have received AGM Notice on 8th October 2021 via email. Information included instructions to cast your vote for candidates running for board positions (If need arises). You will be voting for the Chapter board officers which include: President, Vice President, Secretary, Treasurer and 10 Director positions. The Chapter's Bylaws link was given as well. Request all to attend the AGM on 30th Oct 2021 without fail.

I also want to give a huge "THANK YOU" to the members in the Executive Committee for providing support in all the activities related to Chapter. Our team is signing off and the new Team will take over the reins. We will celebrate elected board officer and directors at the AGM.

Thank you for reading the newsletter.

Regards,

**VIJAYAVANITHA,** CISA, CIA, MBA, M Com
Secretary

# Chapter Highlights for the period from July to September 2021

## SHORT LEARNING BYTES (SLB) :

**Topic : "Technical Security Audit of Cloud"**
**Venue : Web-based ONLINE session via Zoom Webinar Platform**
**Date : 10-Jul-2021 (Saturday) Time : 5:30 PM - 6:30 PM IST**

**Topic Summary:**

- High level Cloud Architecture
- Services provided by the Cloud providers
- Applicable standards
- Auditing Challenges with Cloud computing
- Native security services provided by cloud providers
- Sample case study with AWS

**Speaker: Atul Prakash**

**Speaker profile:** Atul Prakash is currently working as "Director - Cybersecurity Operations & Engineering" with Envestnet & Yodlee. He has seventeen years of professional experience in Information security, Cybersecurity and is successful in designing, developing, managing, operating, reviewing and assessing global enterprise security solutions within BFSI, Telecom, Oil & Gas, Insurance and Manufacturing domain across APAC, MEA, EU and Americas.

## CPE MEETINGS:

**Topic : "Combating Application Abuse by Automated Traffic Detection and Bot Prevention - Use cases from Financial Sector & e-Commerce"**
**Venue : Web-based ONLINE session via Zoom Webinar Platform**
**Date : 31-Jul-2021 (Saturday) Time : 5:30 PM - 7:30 PM IST**

**Topic Summary :**

Automated Traffic is a central part of digital business and revenue generation. Through cross industry case studies, understand how application abuse can be mitigated by identifying automated attack vectors and how you can support your digital business initiatives better."

**Speaker: Vaibhav Khandelwal**

**Speaker profile:** Vaibhav Khandelwal (VK, is Manager for Cloud Security & Fraud Solutions at F5 Networks looking after sales for ASEAN and South Asia markets. He has been working at intersection of Banking and Technology with prior roles in Cybersecurity, Digital Banking Transformation, Fraud Prevention and Risk Management. Before F5, VK worked across several markets with IBM, RBS and ABN AMRO Bank.

## Short Learning Bytes (SLB) :

1. **Topic : "IoT Security - Overcoming the Security Challenges in Connected World"**
   **Venue : Web-based ONLINE session via Zoom Webinar Platform**
   **Date : 21-Aug-2021 (Saturday) Time : 5:30 PM - 7:30 PM IST**

**Topic Summary:**

- Overview of IoT
- Introduction to IoT Security
- Recent attack trends in connected technology
- Attack surfaces and Security challenges
- Global standards and regulations
- Leading practices to follow

**Speaker: Neeraj**

**Speaker profile:** Neeraj is a seasoned cyber security professional with master's in information security having 9+ years of extensive experience in product security, penetration testing (hardware, firmware and software) a wide range of embedded /IoT enabled devices, ICS/OT security and Plant/factory/site security assessment using ISA-62443. Vast hands on experience with penetration testing of web and mobile application, API security, Cloud, thick client and product security testing and Network security architecture review/audit.

Followed by the SLB, we have scheduled for a one hour 'Introductory Seminar' where we will be walking you through the ISACA Certifications, Review class scheduled for the upcoming session. Kindly share this information with your friends and family who are interested in pursuing ISACA Certifications. The training schedule is attached in the email for your perusal.

2. **Topic : "Proactive Data Analytics Driving Convergence of CISO and CSO Function"**
   **Venue : Web-based ONLINE session via Zoom Webinar Platform**
   **Date : 25-Sep-2021 (Saturday) Time : 5:30 PM - 7:30 PM IST**

**Topic Summary:**

Deep dive into various data analytics driving scenarios, methods and the decision making for Convergence of CISO and CSO function with real case studies.

**Speaker: Pawan Desai**

**Speaker profile: Pawan Desai,** CISA, CISSP, CBCP, Co-founder & CEO, MitKat Advisory is an acknowledged cyber security thought leader and entrepreneur who speaks regularly at prestigious forums like Horasis Annual Meeting, CyberFrat, OSAC, ACSG, ASIS, BCI, Duty of Care, WiCyS India, (ISC)²Singapore Chapter, Symbiosis Institute of Digital & Telecom Management (SIDTM), ET Edge - An Economic Times Initiative, CORE Global online Summit, OSPAs, CII, Secutech, GWFM etc.

## INTRO SEMINAR:

1. **'Introductory Seminar' - conducted on ISACA Certification Courses.**
   **Venue : Web-based ONLINE session via Zoom Webinar Platform**
   **Date : 21-Aug-2021 (Saturday) Time : 5:00 PM - 7:00 PM**

The Chapter team imparted an over view on ISACA Membership benefits, ISACA certifications, CISA, CISM, CRISC, CGEIT & CDPSE Certifications to all Participants who appreciated the seminar very well.

## PLANS FOR THE NEXT MONTH (OCTOBER 2021)

25th Annual General Body Meeting.

## RENEWAL OF YOUR ISACA MEMBERSHIP FOR 2021- RETAIN YOUR VALUABLE CERTIFICATION AND MEMBERSHIP

Warm Greetings from ISACA Bangalore Chapter!!! We thank you for your continued support and commitment to professional excellence by earning one or more of ISACA Certifications.

Use your ISACA® membership and ISACA certification(s) as the platform for your growth by utilizing the opportunities for professional development. As you would have experienced, your ISACA membership and certification(s) increase your advancement opportunities by keeping you informed of standards and good practices in the fields that matter most to you and providing access to leading edge research and knowledge through Journals, Webinars, Blogs, ISACA e-library, local chapter events and many more.

Also, you are aware ISACA Bangalore Chapter provides significant benefits and local networking opportunities to its members. The chapter has been in the forefront and served its members in their quest for acquiring professional knowledge by conducting regular CPE Sessions, Webinars, Conferences and other professional development programs. At the chapter it is our endeavor to bring to the table the most relevant of the current topics and encourage active participation of members.

**Visit www.isacabangalore.org for more information.**

Now it is time for renewing your ISACA® membership for 2021 if not already done. Please ensure to renew your membership before the PURGE to ensure the benefits arising out of continued membership.

Please click below to renew *(login with your ISACA username and password to renew)*
**http://www.isaca.org/renew**

In case you need any assistance, please do not hesitate to reachout to me or Chapter Office at chapter@isacabangalore.org

***PS: If you have already renewed your membership - Thank you for your support. Please ignore this reminder.***

**For your information, the membership dues are indicated here below:**

International Membership Dues: **$135.00**
ISACA Bangalore Chapter Dues: **$10.00**
Total Dues for 2021 membership renewal: **US$ 155.00**

**Note:** ***Apart from the above, certification maintenance dues may apply as per the certifications held.***

### Whitepaper Contest

ISACA Bangalore chapter invited for the first ever Whitepaper contest as part of our chapter 24th Annual Karnataka Virtual Conference.The topic for the Whitepaper was '**Digital Transformation - Cyber Security Challenges'.** Around 11 papers submitted by our chapter members. Following are the winners and chapter congratulated the top 3 winners during the and rewarded with gift vouchers.

| **Winners** | **Name** |
|---|---|
| 1st Prize | Ms. Praveena K R |
| 2nd Prize | Ms. Shini Menon |
| 3rd Prize | Mr. Udayshankar Tadigadapa |

The articles **Significance of Risk Culture in an Organization** by Ms. Shini Menon which bagged the 2nd Prize & **Significance of Risk Culture in an Organization** by Mr. Udayshankar Tadigadapa which bagged the 3rd Prize in Whitepaper Contest will be published in our next issue.

*Affix your Photo*

# ISACA Bangalore Chapter

Registration Form for CISA & CISM for
Computer Based Exams in 2021

**Venue: Chapter Office-Address mentioned underneath**

1. NAME:……

2. ☐ CISA ☐ CISM ☐ CRISC ☐ CGEIT (Please tick for Registration)

2. ISACA MEMBERSHIP NO:……NON MEMBER (Please tick as applicable)

3. DESIGNATION: ..... QLFN: .....

4. ORGANISATION: .....

6. ADDRESS: .....
.....

7. PH:OFFICE……RES……MOBILE:.....

8. EMAIL: ……

9. PRESENT WORK AREA :.....

Registration Fee per batch classes : Rs. 8500/- for ISACA Members and for Non members Rs. 9500/- (Inclusive of Taxes) A Local Cheque/Bank Pay Order in favour of **ISACA, Bangalore Chapter** and the same may be despatched to the Office address

***or***

NEFT (Wire transfer) to : **State Bank of India**, PBN 1027, 14th Main, 1st Block, Rajajinagar Branch, Bangalore-10.
Savings Bank Account No.54003825745. Account Holder : ISACA, Bangalore Chapter
IFSC Code-SBIN0040197 / MICR 560002408

Date_____ Candidate Signature

Course Material - Received / to be received.

No.S-13, 531/A, 2nd Floor, Priya Chambers, Dr. Rajkumar Road, Opp. St. Theresa's Hospital, 2nd Stage, Rajajinagar, Bangalore - 560 010, Ph. : 080 65640042 / +91 9535197405
Email ID : chapter@isacabangalore.org. Website : www/isacabangalore.org

# Framework to Understand Behavioural Influences on Cybersecurity Culture of Organisations

*- Praveena K. R.*

**About the Author: PRAVEENA K R,** *MCom, ACA, CISA*

*ISACA ID: 344257*

***(White paper submitted to ISACA Bangalore chapter under the theme - Significance of Risk Culture in an Organization, August 2021)***

Praveena is a Finance and InformationSecurity professional. She is a Chartered Accountant (ACA) and Certified Information Systems Auditor (CISA) by qualification. Praveena has undergone the ISO Lead Auditor course (Information Security Management System) and has a Six Sigma Green Belt. She has over fifteen years of experience in accounting, auditing and consulting.Her areas of expertise include Information Systems Audit, IT Security Audit, Internal and Management Audit, Business Process Reengineering, MIS, Business Plans and Feasibility Studies. Her countries of work experience include India, UAE, Bhutan, Bangladesh, Netherlands, and UK. She is anExecutive Director &Senior Consultantat MaGC and can be reached at praveena@magc.in

**Abstract**

Cybersecurity risks are top priority for organisations of all sizes, sectors, and geographies. Examination of commonplace security incidents clearly establishes that the human element has an overbearing influence on the underlying causes.CyC is about making information security considerations an integral part of an employee's job, habits, and conduct, embedding them in their day-to-day actions.

The proposed Cybersecurity Culture (CyC) Framework, is based on The Cultural Web model, which is for organisational behaviour. Attributes have been defined under each of the six elements that are tailored to CyC. The framework focuses on behavioural aspects and is designed to be simple, flexible, measurable, and provide pointers for practical interventions to improve CyC health. CyC Framework provides a method to measure cultural health using CyC Health score.This is also visually represented as CyC Health Score Web, showing position against each element.

It can provide key inputs to stakeholders such asBoard/ Governing body level decision makers and internal/ external/IS Auditors. This framework can be integrated with the existing IT Governance Framework and Enterprise Risk Management (ERM) framework of organisations. Further it will lend itself to Artificial Intelligence/Machine Learning (AI/ML) solutions for continual behavioural tracking.

Structured research may be required to refine the attributes, map CyC Framework to existing cybersecurity frameworks/standards, and develop AI/ML use cases.

**Key Words**

Risk Culture, Cybersecurity Culture, User Behaviour, Framework, Assessment, Cybersecurity Culture Health score, AI/ML use case

**Framework to understand behavioural influences on Cybersecurity Culture of Organisations**

**Praveena K R, MCom, ACA, CISA**

(White paper submitted to ISACA Bangalore chapter under the theme - Significance of Risk Culture in an Organization, August 2021)

## 1. Introduction

Every organisation has its distinct risk universe and its own unique approach to manage and mitigate its risks. The risk culture of the organisation is a key factor which influences the strategies and practices adopted in risk management. A healthy risk culture facilitates successful risk management.

In this cyber age, Cybersecurity risks are top priority for organisations of all sizes, sectors, and geographies. Technological advancements have also resulted in democratised IT environments, necessitating Organisations to think beyond boundary security controls. Examination of commonplace security incidents clearly establishes that the human element has an overbearing influence on the underlying causes.Therefore, there is a need to ensure Cybersecurity Culture is closely assessed, monitored, and managed such that it results in least risky behaviour.

While much research work is available on risk culture, a framework to understand behavioural influences which impact Cybersecurity Culture is not available. This white paper ideates a practical framework to address this gap. The framework is intended for use to understand the current CyC, measure its health, and identify areas for intervention.

The objective of this paper is to bring out a behavioural framework for assessing CyC and if possible attempt to configure a CyC Score for organisations, irrespective of the size and complexity of the organisations. This is important as Cybersecurity risk is omnipresent and insensitive to configuration of organisations. Also, organisations can attempt to improve the CyC scores there by continuously keep reinventing strategies in this regard. Hence, it is expected that the CyC Framework could pave way for structuring Cybersecurity strategies.

## 2. Definition of Risk Culture in the context of Cybersecurity

Risk culture is a term describing the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with a common purpose(IRM, n.d.). IRM's Risk Culture Framework complements this definition by recognising the importance of the individual's 'predisposition to risk' and 'personal ethics' in shaping people's attitudes. It then describes the link between these attitudes driving behaviours and behaviours in turn shaping organisational culture. The framework recognises that risk culture, in turn, is a product of the organisation's overall culture (**Figure 1**) (IRM, n.d.).

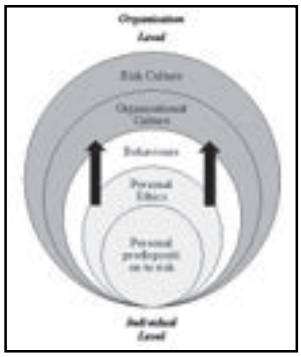


*Figure 1: IRM Risk Culture Framework*

In the context of mitigating Cybersecurity risks, the risk culture is commonly referred to as Cybersecurity Culture (CyC), which is about making information security considerations an integral part of an employee's job, habits, and conduct, and embedding them in theirday-to-day actions ((ENISA), 2017).

## 3. Importance of Cybersecurity Culture (CyC)

Cybersecurity is a superset of the practices embodied in IT security, information security, operational technology (OT) security, and offensive security(Weiss, et al., June 2013). It casts a wider net than information security, and is impacted by human behaviour. In cybersecurity, human factor has an additional dimension - as potential targets of cyber-attacks or even unknowingly participating in a cyber-attack (Reegard, et al., 2019). This makes CyC an important instrument to manage cybersecurity risks.

In Verizon's Data Breach Investigations Report 2021, Phishing and Social Engineering are top modes of breaches (Verizon, 2021), clearly establishing that the human factor is a weak link when managing cybersecurity risks. The only mitigation is to strengthen CyC in organisations, which can in turn propel desirable human behaviour.

In a Cybersecurity Culture study conducted by ISACA & CMMI Institute, 95% of respondents recognised that there is a gap between the organization's desired and actual culture of cybersecurity; and 87% confirmed that establishing a stronger culture of cybersecurity would increase their organization's profitability or viability(CMMI&ISACA, 2018). The same study also infers that successful Cybersecurity Culture helps in - reduction of cyberincidents, building customer trust, and improving brand reputation.

The need for nurturing good CyC is amplified by the fact that with the COVID pandemic, increasingly employees are working from environments that are not under the control of organisations.

Further, monitoringCyC can help organisations in devising interventions that can prevent occurrence of a breach or materialisation of a cybersecurity risk. The above discussion clearly brings out the need to understand behavioural influences on CyC, assess and monitor it.

## 4. Existing models on organisational culture/risk culture

COBIT (ISACA's IT governance framework) recognises that "Culture, ethics and behaviour of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities". It identifies 'culture and behaviour' as a governance component to achieve AP001: Managed IT Management Framework; as information security processes and procedures will not be effective if the enterprise's and personnel's culture and ethics are not appropriate. However, it does not discuss CyC in detail(ISACA, 2019).

Some of the other common models and frameworks used to measure 'risk culture' in organisations:

**Attitude-Behaviour-Culture model** (A-B-C model) by Hillson, David (Hillson, 2013)–describes the relationship between attitude, behaviour, and culture (**Figure 2**).

- Pros - Robust conceptual model, helps high level understanding
- Cons - Does not have components for practical application

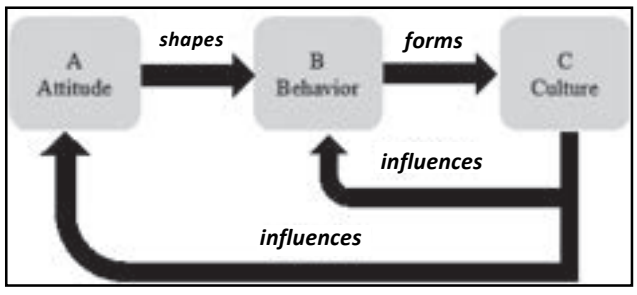



*Figure 2: A-B-C model*

**IRM Risk Culture Aspects Model** by IRM (IRM, n.d.) - proposes 8 aspects, grouped into 4 themes, that need to be in place to ensure a healthy risk culture, aligned to the organisation's strategic objectives and business model (**Figure 3**).

- Pros - Extensive coverage, includes diagnostic questionnaire
- Cons - Behavioural aspects not fully captured, focussed on governance & controls

| **Tone at the Top** | **Decisions** |
|---|---|
| Risk Leadership | Informed risk decisions |
| Dealing with bad news | Reward |
| **Governance** | **Competency** |
| Accountability | Risk resources |
| Transparencey | Risk Skills |

***Figure 3: IRM Risk Culture Aspects Model***

**Risk culture framework by McKinsey & Co** (Mckinsey & Co, 2010)- identifies 10 key cultural factors which contribute to failures. These are mapped to four dimensions and measures them in a continuum from weak to strong (**Figure 4**).

- Pros - Based on research on risk culture failure case studies, considers behavioural aspects
- Cons - Presupposes existence of robust risk management, difficult to apply for smaller organisations

There are models by other top consulting companies aligned to one or more of above.

| **Groups** | **Dimension** | **High Risk** → | **Low Risk** |
|---|---|---|---|
| Transparency of Risk | Communication | Poor | Good |
| | Tolerance | Unclear | Clear |
| | Level of insight | Lack of insight | Good insight |
| Acknowledgement of risk | Confidence | Overconfidence | Confident but careful |
| | Challenge | No Challenge | Constructive challenge |
| | Openness | Fear of bad news | Reward Honesty |
| Responsiveness to risk | Level of care | Indifference | Diligence |
| | Speed of response | Slow | Fast |
| Resect for risk | Cooperation | Gaming | Coordinating |
| | Adherence to rules | Beat the system | Play by rules |

***Figure 4: McKinsey's Risk culture framework***

**Cultural Webby Gerry Johnson and Kevan Scholes**

Organisational culture is tricky to assess as it is unique to each entity. The Cultural Web, developed by Gerry Johnson and Kevan Scholes, is one approach which provides a means to understand and change an organization's culture. It can help identify the gaps and highlight areas that need alignment to organisational strategy. The Cultural Web identifies six interrelated elements (**Figure 5**) that help to make up the "paradigm" - the pattern or model - of the work environment. By analyzing the factors in each, one can begin to see the bigger picture of what is working, what isn't working, and what needs to be changed. The six elements are: Stories, Rituals and Routines, Symbols, Organizational Structure, Control Systems, and Power Structures (Johnson & Scholes, 2012).


*Figure 5: Cultural Web*

An SAI computing conference paper by Adéle Da Veiga, provides Cybersecurity culture research methodology (CSeCRM)(Da Veiga, 2016), which describes the methodology to develop CyC. In a research paper, based on an analysis of 69 papers, the authors describe cybersecurity culture and safety culture as two distinct sub-components of organizational culture. Further they identify certain Cybersecurity culture practices around Management support, Cybersecurity Policy, Cybersecurity awareness and training, Involvement and communication, and learning from experience (Blackett, et al., 2019).A literary review work on user behaviour infers that personality traits and individual differences in procrastination, impulsivity, and risk-taking behaviours, are related to cyber security behaviours (Moustafa, et al., June 2021).

COBIT (ISACA's IT governance framework) recognises that "Culture, ethics and behaviour of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities". It identifies 'culture and behaviour' as a governance component to achieve AP001: Managed IT Management Framework; as information security processes and procedures will not be effective if the enterprise's and personnel's culture and ethics are not appropriate. However, it does not discuss CyC in detail (ISACA, 2019).

The above discussion on available literature reveals that there is limited work on precisely measuring CyC.Moreover, available frameworks are either too generic/conceptual or not focussed on CyC.

## 5. Proposed CyC framework

The gap is predominantly due to an approach of mitigating cybersecurity risks using process and technological solutions that focus on compliance rather than on commitment to risk management. While compliance is rule-based, commitment to risk management can only be achieved through behavioural changes. To address this perceptible gap, the author has ideated a framework to understand and assess cybersecurity culture that is based on The Cultural Web model. The Cultural Web model was chosen since it is simple to follow and focusses on behavioural aspects. The framework provides six behavioural elements that impact CyC.Under each element, its objective and attributes have been defined totailorit for CyC (shown in **Figure 6**). This resulting model has been namedthe Cybersecurity Culture (CyC) Framework.

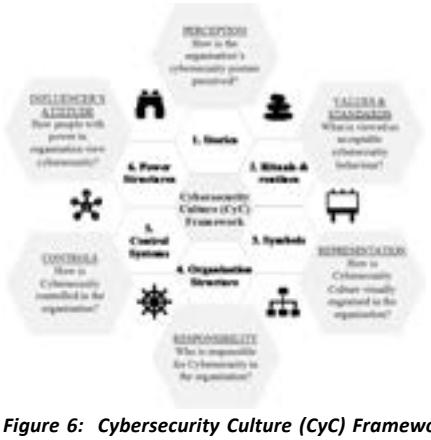



*Figure 6: Cybersecurity Culture (CyC) Framework*

Description of each element, its key attributes, and examples of desirable & undesirable behaviour areprovided below:

| **1. Stories** | | |
|---|---|---|
| **PERCEPTION – How is the organisation's cybersecurityposture perceived?** | | |
| **Description:** Stories element reflects the perceptions about the organisation's Cybersecurity risk exposure, appetite, policies, and practices both within and outside the organisation. Perceptions could comprise of past events, key people (heroes, villains, mavericks in respect of cybersecurity matters), what is viewed as good cybersecurity practice, tenacity in handling bad cybersecurity practices, etc. | | |
| **Attributes** | ***Examples of Undesirable behaviour reflecting unhealthy CyC*** | ***Examples of Desirable behaviour reflecting healthy CyC*** |
| 1.1. Perception (Reputation) of Cybersecurity position | *Careless, not taking cybersecurity seriously, inaction/delay in action, misunderstood as not IT dependent* | *Cyber security conscious, strict and immediate action on incidents/undesirable behaviour, close monitoring, and robust controls* |
| 1.2. Awareness of impact of breaches/incidents to organisation | *Mentality that breaches/incidents will not/have not happened to us; my job will not affect security* | *Awareness of breaches/possible incidents that organisation is exposed to and its impact (financial & non-financial)* |
| 1.3. Awareness of IS policy and practices | *Lack of clarity on acceptable and unacceptable behaviour, Unaware of policy* | *Existence of clear policy, awareness of acceptable and unacceptable behaviour among users* |
| 1.4. Impulse control/Alertness to prevent oversight resulting in breach/incident | *Users fall prey to Clickbaits and phishing, Not cautious* | *High user awareness and alertness* |
| 1.5. Mindful of surroundings and ability to report suspicion | *Unaware or indifferent to suspicious activity in work environment* | *High user awareness and alertness* |

| 2. Rituals and Routines | | |
|---|---|---|
| **VALUES & STANDARDS – What is viewed asacceptable cybersecurity behaviour?** | | |
| **Description:** Rituals and Routines reflects the core values and addresses the baseline acceptable behaviour. It also encompasses the aspects that contribute to decision making when there are no clear cut guidelines. | | |
| **Attributes** | ***Examples of Undesirable behaviour reflecting unhealthy CyC*** | ***Examples of Desirable behaviour reflecting healthy CyC*** |
| 2.1. Attitude towards adherence to IS Policy | *Lack of knowledge. Low compliance* | *High compliance to IS Policy* |
| 2.2. Ability to inculcate adherence in new joinees, subordinates, other users (Contractors, Vendors, Customers) | *High variance in degree of compliance among different user groups/locations* | *Consistent compliance to IS Policy across user groups/locations* |
| 2.3. Channel to report/escalate suspicious incidents | *Lack of IT helpdesk/hotline to report incidents, complex process – not being used* | *Clear/easy to remember process to report suspicious incidents, being used regularly* |
| 2.4. Response to business changes | *Cybersecurity risks not evaluated/considered when making business changes* | *Cybersecurity risks due to business changes are evaluated/considered in decision making* |
| 2.5. Application of IS policy/its principles to new scenarios | *New scenarios exposed to risks, or gets bottled necked till clear policy is issued* | *Dynamic environment where decision makers are able employ the principles of IS Policy when handling business changes* |

| **3. Symbols** | | |
|---|---|---|
| **REPRESENTATION ⍰ How is Cybersecurity Culture visually engrained in the organisation?** | | |
| **Description:** Visual representation to inculcate and embed Cybersecurity Culture both physically and virtually. | | |
| **Attributes** | ***Examples of Undesirable behaviour reflecting unhealthy CyC*** | ***Examples of Desirable behaviour reflecting healthy CyC*** |
| 3.1. Physical location/work space demarcation | *Weak physical access controls* | *Areas with restricted access clearly marked and labelled, physical access controls in place* |
| 3.2. Colour coding and labelling different data classification | *No data classification, lack of clarity/standardisation across organisation* | *Sensitive and confidential information clearly marked and labelled in red, Internal documents labelled in green* |
| 3.3. Labelling for easy identification of IT Assets, quick troubleshooting | *Unlabelled, not standard* | *Clear labelling physical assets, cables, ports, etc.* |
| 3.4. Different badges/ID cards for personnel with different access rights | *No mechanism to identify employees/visitors, or prescribed process not followed* | *Admins wear blue badges, Visitors wear green badges* |
| 3.5. Visual display of Cybersecurity good practices /precautions | *No such practice* | *Regular email alerts on security incidents, alerts when opening email to outsiders, Posters in strategic places, intranet* |
| 3.6. Reward good behaviour and Punish undesirable behaviour | *No such practice* | *Awards, recognition, contests to encourage food practices. Warnings, disciplinary action to discourage poor practices.* |

| 4. Organizational Structure | | |
|---|---|---|
| **RESPONSIBILITY – Who is responsible for Cybersecurity in the organisation?** | | |
| **Description:** Organizational Structure represents the formal and informal lines of authority and responsibility for cybersecurity. It encompasses role clarity of each user in respect of cybersecurity. | | |
| **Attributes** | ***Examples of Undesirable behaviour reflecting unhealthy CyC*** | ***Examples of Desirable behaviour reflecting healthy CyC*** |
| 4.1. Cybersecurity is a key consideration in routine, non-IT decision making | *Cybersecurity is seen as the sole responsibility of IT function* | *Cybersecurity is seen as the sole responsibility of every user* |
| 4.2. Importance of Cybersecurity emphasised through formal communication | *Top Management lacks understanding of cybersecurity risks, weak tone at the top on cybersecurity matters* | *Emphasis through written directions, orders, wide-spread sharing of learning from breaches* |
| 4.3. Importance of Cybersecurity emphasised through informal communication | *Poor user awareness and /alertness* | *Undesirable behaviour is quickly pointed out by peers, cybersecurity importance discussed in casual chats& discussions* |
| 4.4. Employees (including Board, Management, & Independent Directors) are clear on their role in cybersecurity, impact of their actions/decisions to cybersecurity | *Lack of clarity on role in cybersecurity* | *Job descriptions clarify role of each position in cybersecurity, clear understanding of how one's job is likely to impact cybersecurity of organisation* |
| 4.5. Ensuring Users (other than employees) understand impact of their actions/decisions to organisation's cybersecurity | *Lack of clarity on role in cybersecurity* | *Third party Contracts have clear terms enforcing requisite IT policy/practices* |

| **5. Control Systems** | | |
|---|---|---|
| **CONTROLS – How is Cybersecurity controlled in the organisation?** | | |
| **Description:** Control Systems reflect established process controls and reporting to manage cybersecurity risks. | | |
| **Attributes** | ***Examples of Undesirable behaviour reflecting unhealthy CyC*** | ***Examples of Desirable behaviour reflecting healthy CyC*** |
| 5.1. Internal Control Environment | *Weak internal controls* | *Strong internal controls – maker-checker, clear authority, good document trail* |
| 5.2. Reviewof performanceand action on deviations/alarms | *Poor reporting mechanism, lack of action on reports* | *Regular reports on key metrics from the hardware, software, network monitoring tools; Action taken on outliers* |
| 5.3. Competency of employeesto manage cybersecurity risk | *Ineffective initiatives* | *Effective training and awareness campaigns, use of qualified resources* |
| 5.4. Performance monitoring of third parties (vendors, contractors) | *Ineffective measures* | *Evaluation of vendors on cybersecurity aspects* |

| 6. Power Structures | | |
|---|---|---|
| **INFLUENCER□S ATTITUDE□ How people with power in organisation view cybersecurity?** | | |
| **Description:** Power Structures represent the group of people wielding the real power in the organisation. This set of people exert the most influence on organisational decision making. How these power centres view cybersecurity impacts cybersecurity culture. | | |
| **Attributes** | ***Examples of Undesirable behaviour reflecting unhealthy CyC*** | ***Examples of Desirable behaviour reflecting healthy CyC*** |
| 6.1. Outlook of influential decision makers towards cybersecurity | *Unaware, indifferent to cybersecurity* | *Understand criticality, supportive, consciously consider cybersecurity in decision making* |
| 6.2. Influential decision makers□attitude towardsdeviation from prescribed IS Policy/processes | *Indifferent, frequent incidents of workaround being approved* | *Deviations actively discouraged* |

*CyC framework lends itself for use in entities of all sizes. Assessment can be made more objective by defining pertinent indicators for each attribute that drawsinputs from ERP transaction logs, firewalls that use User and entity behaviour analytics (UEBA), Security Information and Event Management (SIEM), attendance records, employee surveys, audit reports/observations, etc.*

## 6. Scoring CyC health

CyC frameworkfacilitates assessment ofcultural health against the different attributes under each of the elements (say from 1 to 5 with 1 representing very poor cultural health and 5 representing excellent cultural health). The element-level score can be arrived at by averaging the score of the attributes.[1]

Thesum of scores of all elementsrepresents the organisation's **CyC Health Score.** This is represented as a web diagram for application - **CyC Health Score Web** (shown in **Figure 7**). Each axis represents one element. The concentric hexagons represent increasing health (innermost hexagon indicates very poor health with score of 1, and outermost hexagon represents excellent health with score of 5).

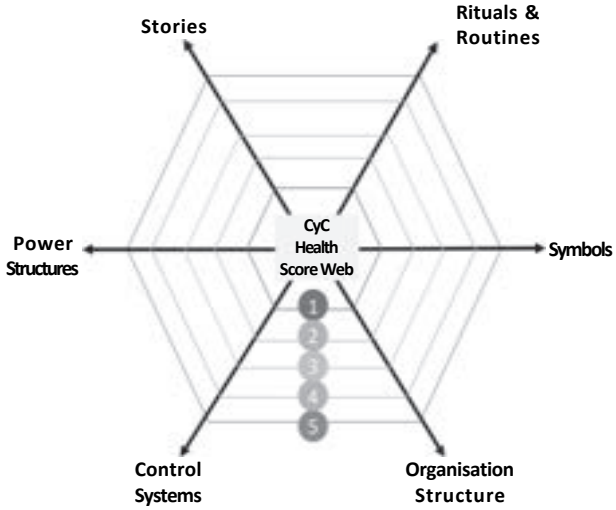



*Figure 7: CyC Health Score Web template*

[1]*Alternatively, attributes may be assigned weights and weighted average score can be arrive at.*

The filled example shown in **Figure 8** may be interpreted as follows:

- Power structures & Organisation Structure elements are assessed to be in good health (average of attribute scores is 4 on 5),
- Stories element is assessed to be in poor health (average of attribute scores is of 2 on 5),
- Overall health is moderate at 63% (score of 19 over a total of 30),
- Organisation needs to focus measures to improve the Stories element, interventions to improve each attribute under Stories element to be devised.

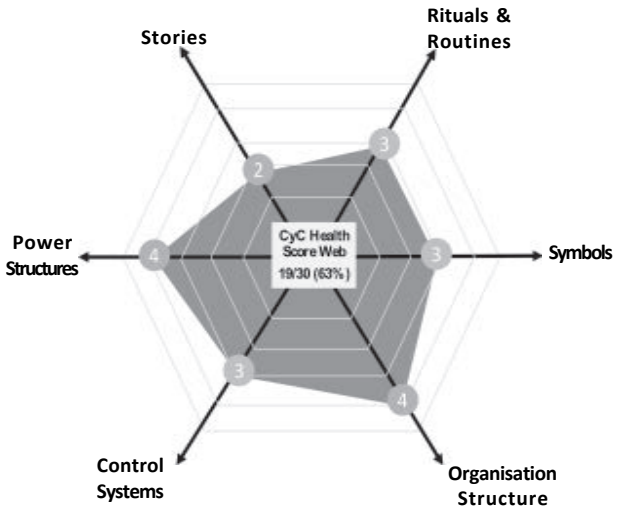



*Figure 8: CyC Health Score Web example*

**7. Applicability of CyC framework**

CyC Framework will complement and enhance existing cybersecurity frameworks. It will help demonstrate how behavioural aspectsimpact the cybersecurity ofthe organisation.

i. It can be used by organisations as part of their IT Governance framework. CyC Health score can help measure and quantify improvement/deterioration of CyC.

ii. Determining CyC Health score can be automated by mapping data for metrices. It will lend itself to potential Artificial Intelligence/Machine Learning (AI/ML) solutions for continual behavioural tracking.

iii. CyC Health Score Web can assist in explaining behavioural aspects to Board/Governing body level stakeholders.

iv. It can be a component of organisation's Enterprise Risk Management (ERM) framework.

v. Internal/External/IS Auditors can use the CyC Health Score as input for risk assessment and assertion on general controls.

**8. Scope for further research in this area**

The CyC framework conceptualises the need for CyC assessment tool. The framework needs to be tested and subjected to empirical analysis. Some questions that require further research in respect of CyC are:

i. Can attributes proposed in the CyC framework be refined with inputs from industry?

ii. How can Industry specific peculiarities (for ex: IT industry, defence, financial services, aviation, ecommerce) be embedded in the Framework?

iii. Detailed mapping of CyC framework to existing cybersecurity frameworks/standards like COBIT, ITIL, & Information Security Management System (ISO 27001 -ISMS).

iv. Critical Success Factors and Key Performance Indicators across the six dimensions of the CyC Web: What are they sensitive to?

v. CyC Web as a Corporate Governance tool – what are the profits and pitfalls?

## 9. Concluding remarks

This white paper attempts to conceptualise a framework that can facilitate structured consideration of behavioural influences on Cybersecurity Culture. It envisages the building blocks to construct an assessment cum governance tool that can help organisations measure the health of their Cybersecurity Culture. Further research can help finetune this work for the same.

***References***

*(ENISA), E. U. A. f. N. a. I. S., 2017. Cyber Security Culture in organisations, s.l.: ENISA.*

*ISACA, 2019. COBIT , s.l.: ISACA.*

*Hillson, D., 2013. The A-B-C of risk culture: how to be risk-mature. North America, New Orleans, Paper presented at PMI® Global Congress.*

*Verizon, 2021. Data Breach Investigations Report, s.l.: Verizon.*

*pwc, 2009. Auditing risk culture Art or science?. [Online]*
*Available at: https://www.pwc.com.au/assurance/assets/auditingriskculture_feb09.pdf*
*[Accessed Aug 2021].*

*Da Veiga, A., 2016. A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. s.l., SAI Computing Conference (SAI).*

*Blackett, C., Katta, V. & Reegard, K., 2019. The Concept of Cybersecurity Culture. s.l., ResearchGate - 29th European Safety and Reliability Conference.*

*IRM, I. o. R. M., n.d. Risk culture. [Online]*
*Available at: https://www.theirm.org/what-we-say/thought-leadership/risk-culture/*
*[Accessed 25 August 2021].*

*IRM, T. I. o. R. M., n.d. Risk culture Resources for Practitioners. [Online]*
*Available at: https://www.theirm.org/media/7236/risk-culture-resources-for-practitioners.pdf*
*[Accessed August 2021].*

*Weiss, J., Perkins, E. & Walls, A., June 2013. Definition: Cybersecurity, s.l.: Gartner.*

*Reegard, K., Blackett, C. & Katta, V., 2019. The Concept of Cybersecurity Culture, s.l.: Researchgate.*

CMMI & ISACA, 2018. *Cybersecurity Culture Study,* s.l.: ISACA & CMMI Institute.

Mckinsey&Co, 2010. *Taking Control of Organisational Risk Culture.* [Online]
Available at: https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/working%20papers/16_taking_control_of_organizational_risk_culture.pdf
[Accessed August 2021].

Johnson, G. & Scholes, K., 2012. *Fundamentals of Strategy.* s.l.:Pearson Education.

Moustafa, A. A., Bello, A. & Maurushat, A., June 2021. The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology.*


# Three Programs, One Vision

Our programs are based on the One In Tech vision that technology knows no gender, no color, no age, and makes no assumptions, holds no biases and has no bounds. To combat barriers commonly based on these, we built a suite of programs focused on children, women, and people of color, and those under-served socioeconomically and due to bias. Our objectives are to build equity and diversity in the digital space.

| ONE IN TECH WeLeadTech | ONE IN TECH SheLeadsTech | ONE IN TECH YOUNG LEADERS IN TECH |
|---|---|---|
| *Creating pathways for a racially and culturally diverse workforce* | *Building avenues to achieve a workforce free of gender-bias* | *Preparing the next generation to be healthy digital citizens* Young Leaders |
| WeLeadTech empowers groups who, due to racial or cultural bias or exclusion, are underrepresented in the tech industry with opportunities to build leadership skills, find and be mentors, gain career guidance, and achieve certifications leading to stronger equity in technology fields. | SheLeadsTech empowers women, a highly underrepresented percentage in the tech workforce, to not only enter into tech careers, but to stay in the field, serving in leadership roles and achieving their highest potential. | In Tech provides under-resourced and under-represented children with the knowledge and skills to help them avoid online risks, build online skills, and explore cybersecurity fields to begin a pipeline of a diverse workforce. Initiatives within this program include: |

# Certifications of ISACA


Certified Information Systems Auditor®

An ISACA® Certification

The CISA certification is world-renowned as the standard of achievement for those who audit, control, monitor and assess an organization's information technology and business systems. The recent quarterly IT Skills and Certifications Pay Index (ITSCPI) from Foote Partners ranked CISA among the most sought-after and highest-paying IT certifications. This certification is a must have for entry to mid-career IT professionals looking for leverage in career growth.

ISACA's Certified Information Security Manager® (CISM®) certification indicates expertise in information security governance, program development and management, incident management and risk management. If you are a mid-career IT professional aspiring to senior management roles in IT security and control, CISM can get you the visibility you need.


Certified Information Security Manager®

An ISACA® Certification


Certified in the Governance of Enterprise IT®

An ISACA® Certification

ISACA's Certified in the Governance of Enterprise IT® (CGEIT®) is unique and framework agnostic. It is the only IT governance certification that can give you the mindset to assess, design, implement and manage enterprise IT governance systems aligned with overall business goals. Get visibility at the executive level with CGEIT!

# Certifications of ISACA

CRISC™

Certified in Risk and Information Systems Control™

An ISACA® Certification

ISACA's Certified in Risk and Information Systems Control™ (CRISC®) certification indicates expertise in identifying and managing enterprise IT risk and implementing and maintaining information systems controls. Gain instant recognition and credibility with CRISC and boost your career! If you are a mid-career IT professional with a focus on IT and cyber risk and control, CRISC can get you the leverage you need to grow in your career.

Modern privacy laws and regulations require organizations to implement privacy by design and by default into IT systems, networks, and applications. To do so, privacy professionals must partner with software developers, system and network engineers, application and database administrators, and project managers to build data privacy and protection measures into new and existing technology environments.

CDPSE™

Certified Data Privacy Solutions Engineer™

An ISACA® Certification

ISACA

COBIT® 5

CSX™

CYBERSECURITY NEXUS

# ISACA®

# RECENT GRADUATE MEMBERSHIP APPLICATION

**www.isaca.org/join**

*Please complete both sides*
U.S. Federal I.D. No. 23-7067291
Phone: +1.847.660.5505 • Fax: +1.847.253.1443
Email: *recentgraduates@isaca.org*

☐ MR. ☐ MS. ☐ MRS. ☐ MISS ☐ OTHER _____ Date _____
MONTH/DAY/YEAR

Name _____
FIRST MIDDLE LAST/FAMILY

*PRINT NAME AS YOU WANT IT TO APPEAR ON MEMBERSHIP CERTIFICATE*

Residence address _____
STREET

_____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Residence phone _____ Email address _____
AREA/COUNTRY CODE AND NUMBER

Birth Year _____ College or University recently graduated from: _____

Date of Graduation: _____ Degree program: ☐ Undergraduate ☐ Graduate ☐ Doctoral ☐ Other _____

**Verification of your Recent Graduate Status**
To become a recent graduate member, you must have graduated from a recognized college or university within the last two (2) years, with a minimum four (4) year degree. You will need to attach one of the following as verification: copy of your unofficial transcript indicating your date of graduation; a copy of your college diploma; or a letter from the Registrar on university letterhead specifying your date of graduation

**NOTE:** Both your printed application form and verification document are required for processing. Please allow 3-5 business days to obtain the member rate on exams, conference registrations, or other purchases.

**Please note:** Membership in the association requires you to belong to a chapter when you live or work within 50 miles/80 km of a chapter territory. The name of the chapter is indicative of its territory. If you live farther than 50 miles/80 km from a chapter territory, select member at large. Chapter selection is subject to verification by ISACA International Headquarters. Cities listed in parentheses are a reference to where the majority of chapter meetings are held. Please contact your local chapter at *www.isaca.org/chapters* for other meeting locations.

**Chapter Affiliation**
☐ Chapter Number *(see reverse)* _____
*or*
☐ Member at large *(no chapter within 50 miles/80 km)*

**How did you hear about ISACA?**
☐ ISACA Chapter ☐ Do not remember ☐ Postal Mail ☐ Tradeshow/Seminar
☐ ISACA Event ☐ Email ☐ Professor/Teacher ☐ Web Advertisement
☐ ISACA Journal ☐ Employer ☐ Publication ☐ Web Site Reference
☐ Career Centre ☐ Friend/Colleague ☐ Social Media ☐ Other

**Member Get A Member Referral Information**
If you have been referred by an ISACA member, please enter the ISACA Member ID# that was provided to you.
Referring Member ID# _____

**If employed, please provide the following:**

Company name _____

Title _____

Business address _____
STREET

_____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Business phone _____
AREA/COUNTRY CODE AND NUMBER

ISACA requires members to provide certain demographic information to help us understand and better serve our constituents, and to ensure that we deliver information that is relevant to you.

**Current field of employment** *(check one)*
☐ Advertising/Marketing/Media
☐ Aerospace
☐ Education/Student
☐ Financial/Banking
☐ Government/Military—National/State/Local
☐ Health Care/Medical
☐ Insurance
☐ Legal/Law/Real Estate
☐ Manufacturing/Engineering
☐ Mining/Construction/Petroleum/Agriculture
☐ Not applicable
☐ Pharmaceutical
☐ Public Accounting
☐ Retail/Wholesale/Distribution
☐ Technology Services/Consulting
☐ Telecommunications/Communications
☐ Transportation
☐ Utilities
☐ Other _____

**Level of education achieved** *(indicate degree achieved, or number of years of university education if degree not obtained)*
☐ one year or less ☐ five years ☐ MS/MBA/Masters
☐ two years ☐ six years or more ☐ Ph.D
☐ three years ☐ AS Degree ☐ Not applicable
☐ four years ☐ BS/BA Degree ☐ Other _____

**Certifications obtained (other than CISA, CISM, CGEIT, CRISC)**
☐ ACA ☐ CIA ☐ MCSE
☐ CA ☐ CISSP ☐ PMP
☐ CFE ☐ CPA ☐ Other _____

**Work experience**
*(check the number of years of information systems related work experience)*
☐ No Experience ☐ 7-9 years ☐ Not applicable
☐ 1-3 years ☐ 10-12 years
☐ 4-6 years ☐ 13 years or more

**Current professional activity** *(if not your title, please select the BEST match)*
☐ CEO, President, Owner, General/Executive Manager
☐ CAE, General Auditor, Partner, Audit Head/VP/EVP
☐ CISO/CSO, Security Executive/VP/EVP
☐ CIO/CTO, Info Systems/Technology Executive/VP/EVP
☐ CFO, Controller, Treasurer, Finance Executive/VP/EVP
☐ Chief Compliance/Risk/Privacy Officer, VP/EVP
☐ IT Audit Director/Manager/Consultant
☐ Security Director/Manager/Consultant
☐ IT Director/Manager/Consultant
☐ Compliance/Risk/Privacy Director/Manager/Consultant
☐ IT Senior Auditor (External/Internal)
☐ IT Auditor (External/Internal Staff)
☐ Non-IT Auditor (External/Internal)
☐ Security Staff
☐ IT Staff
☐ IT/IS Compliance/Risk/Control Staff
☐ Professor/Teacher
☐ Student
☐ Other

**Birth Year** _____

**Payment due**
- International dues $ 68.00 (US)
- Chapter dues *(see reverse)* $ _____ (US)
- New member processing fee $ 0.00 (US)*

PLEASE PAY THIS TOTAL $ _____ (US)

* Membership dues consist of international dues, chapter dues, and new member processing fee. The processing fee is waived for Recent Graduates.

Membership dues are nonrefundable and nontransferable.

**Mail your application and check to:**
ISACA • 1055 Paysphere Circle • Chicago, IL 60674 • USA

**Method of payment**
☐ Check payable to "ISACA" in US dollars, drawn on US bank
☐ Send invoice (Applications cannot be processed until dues payment is received.)
☐ MasterCard ☐ VISA ☐ American Express ☐ Diners Club ☐ Discover

All payments by credit card will be processed in US dollars

Credit Card # _____

Print name of cardholder _____

Expiration date _____
MONTH/YEAR

Signature _____

By applying for membership in ISACA, members agree to hold the association and its chapters, and the IT Governance Institute, and their respective officers, directors, members, trustees, employees and agents, harmless for all acts or failures to act while carrying out the purposes of the association and the institute as set forth in their respective bylaws, and they certify that they will abide by the association's Code of Professional Ethics (*www.isaca.org/ethics*). Full payment entitles new members to membership from the date payment is processed by International Headquarters through 31 December 2019. No rebate of dues is available upon early resignation of membership. Contributions, dues or gifts to ISACA are not tax deductible as charitable contributions in the United States. However, they may be tax deductible as ordinary and necessary business expenses. Your contact information will be used to fulfill your request to become an ISACA member, and may also be used by ISACA to send you information about related ISACA goods and services, and other information in which we believe you may be interested. As an ISACA member, we will be sure to keep you up-to-date on the latest products and services that are available to our community. By applying for membership, you confirm the information provided on this form is complete and accurate, and you authorize ISACA to contact you at the address and numbers you have provided, including to provide you with marketing and promotional communications. You further represent that the information you provided is yours and is accurate. To learn more about how we use the information you have provided on this form, please read our Privacy Policy, available at *www.isaca.org*. Should you elect to attend one of our events or purchase other ISACA programs or services, information you submit may also be used as described to you at that time.

**The dues amounts on this application are valid 1 August 2019 through 31 May 2020.**

**US dollar amounts listed below are for local chapter dues. While correct at the time of printing, chapter dues are subject to change without notice. Please include the appropriate chapter dues amount with your remittance.**

**For current chapter dues, or if the amount is not listed below, please visit the web site, *www.isaca.org/chapdues*, or contact your local chapter at *www.isaca.org/chapters*.**

| Chapter Name | Chapter Number | Dues |
|---|---|---|
| **ASIA** | | |
| Bahrain | 208 | $25 |
| Dhaka, Bangladesh | 207 | $20 |
| China Hong Kong | 64 | $70 |
| Ahmedabad, India | 247 | $20 |
| Bangalore, India | 138 | $20 |
| Cochin, India | 176 | $15 |
| Coimbatore, India | 155 | $20 |
| Hyderabad, India | 164 | $20 |
| Kolkata, India | 165 | $20 |
| Chennai, India | 99 | $15 |
| Mumbai, India | 145 | $40 |
| New Delhi, India | 140 | $20 |
| Pune, India | 159 | $20 |
| Trivandrum, India | 242 | $15 |
| Vijayawada, India | 200 | $20 |
| Baghdad, Iraq | 244 | $40 |
| Indonesia | 123 | $45 |
| Fukuoka, Japan | 219 | $70 |
| Nagoya, Japan | 118 | $60 |
| Osaka, Japan | 103 | $80 |
| Tokyo, Japan | 89 | $30 |
| Amman, Jordan | 246 | $35 |
| Astana, Kazakhstan | 240 | $10 |
| Korea | 107 | $65 |
| Lebanon | 181 | $35 |
| Macao | 190 | $10 |
| Malaysia | 93 | $15 |
| Muscat, Oman | 168 | $40 |
| Islamabad, Pakistan | 224 | $30 |
| Karachi, Pakistan | 148 | $25 |
| Lahore, Pakistan | 196 | $30 |
| Manila, Philippines | 136 | $40 |
| Jeddah, Saudi Arabia | 163 | $0 |
| Riyadh, Saudi Arabia | 154 | $0 |
| Singapore | 70 | $40 |
| Sri Lanka | 141 | $15 |
| Taiwan | 142 | $50 |
| Bangkok, Thailand | 109 | $10 |
| UAE | 150 | $20 |
| **LATIN AMERICA** | | |
| Buenos Aires, Argentina | 124 | $30 |
| LaPaz, Bolivia | 173 | $25 |
| Belo Horizonte, Brazil | 245 | $0 |
| Brasília, Brazil | 202 | $5 |
| Rio de Janeiro, Brazil | 203 | $20 |
| São Paulo, Brazil | 166 | $25 |
| Santiago, Chile | 135 | $40 |
| Bogotá, Colombia | 126 | $25 |
| Medellín, Colombia | 229 | $25 |
| Costa Rica | 31 | $40 |
| Santo Domingo, Dominican Republic | 226 | $30 |
| Quito, Ecuador | 179 | $30 |
| San Salvador, El Salvador | 232 | $30 |
| Guatemala City, Guatemala | 215 | $25 |
| Guadalajara, México | 201 | $40 |
| Mexico City, México | 14 | $40 |
| Monterrey, México | 80 | $50 |
| Panamá | 94 | $30 |
| Asunción, Paraguay | 184 | $40 |
| Lima, Perú | 146 | $30 |
| Puerto Rico | 86 | $45 |
| Montevideo, Uruguay | 133 | $100 |
| Venezuela | 113 | $0 |
| **EUROPE/AFRICA** | | |
| Austria | 157 | $45 |
| Belgium | 143 | $75 |
| Gaborone, Botswana | 228 | $50 |
| Sofia, Bulgaria | 189 | $40 |
| Croatia | 170 | $50 |
| Cyprus | 210 | $30 |
| Czech Republic | 153 | $130 |
| Denmark | 96 | $60 |
| Cairo, Egypt | 230 | $35 |
| Estonia | 162 | $25 |
| Finland | 115 | $15 |
| France (Paris) | 75 | $140 |
| Germany | 104 | $80 |
| Accra, Ghana | 205 | $35 |
| Athens, Greece | 134 | $30 |
| Budapest, Hungary | 125 | $65 |
| Ireland | 156 | $30 |
| Israel | 40 | $60 |
| Milan, Italy | 43 | $53 |
| Rome, Italy | 178 | $35 |
| Venice, Italy | 216 | $30 |
| Kenya | 158 | $40 |
| Latvia | 139 | $20 |
| Lithuania | 180 | $40 |
| Luxembourg | 198 | $60 |
| Malta | 186 | $50 |
| Mauritius | 211 | $70 |
| Casablanca, Morocco | 239 | $30 |
| Windhoek, Namibia | 238 | $50 |
| Netherlands | 97 | $50 |
| Abuja, Nigeria | 185 | $35 |
| Ibadan, Nigeria | 222 | $30 |
| Lagos, Nigeria | 149 | $40 |
| Port Harcourt, Nigeria | 234 | $30 |
| Norway | 74 | $75 |
| Katowice, Poland | 220 | $30 |
| Warsaw, Poland | 218 | $25 |
| Lisbon, Portugal | 209 | $40 |
| Moscow, Russia | 167 | $10 |
| Romania | 172 | $25 |
| Belgrade, Serbia | 236 | $40 |
| Slovenia | 137 | $50 |
| Slovakia | 160 | $100 |
| South Africa | 130 | $70 |
| Barcelona, Spain | 171 | $100 |
| Madrid, Spain | 183 | $85 |
| Valencia, Spain | 182 | $40 |
| Sweden | 88 | $50 |
| Switzerland | 116 | $45 |
| Tanzania | 174 | $50 |
| Tunis, Tunisia | 225 | $30 |
| Ankara, Turkey | 217 | $10 |
| Istanbul, Turkey | 204 | $50 |
| Kampala, Uganda | 199 | $50 |
| Kyiv, Ukraine | 206 | $10 |
| London, UK | 60 | $45 |
| Central UK | 132 | $45 |
| Northern England, UK | 111 | $45 |
| Scotland, UK | 175 | $50 |
| Winchester, UK | 212 | $45 |
| Lusaka, Zambia | 223 | $50 |
| Harare, Zimbabwe | 241 | $30 |
| **NORTH AMERICA** | | |
| **Canada** | | |
| Calgary, AB | 121 | $25 |
| Edmonton, AB | 131 | $25 |
| Vancouver, BC | 25 | $25 |
| Victoria, BC | 100 | $15 |
| Winnipeg, MB | 72 | $20 |
| Atlantic Provinces | 105 | $20 |
| Ottawa Valley, ON | 32 | $20 |
| Toronto, ON | 21 | $25 |
| Montreal, PQ | 36 | $30 |
| Quebec City, PQ | 91 | $45 |
| Regina, SK | 231 | $25 |
| **Islands** | | |
| Bermuda | 147 | $45 |
| Curacao | 227 | $30 |
| Kingston, Jamaica | 233 | $30 |
| Trinidad & Tobago | 106 | $50 |
| **Midwestern United States** | | |
| Central Indiana (Indianapolis) | 56 | $30 |
| Chicago, IL | 02 | $50 |
| Illini (Springfield, IL) | 77 | $30 |
| Illowa | 169 | $25 |
| Iowa (Des Moines) | 110 | $25 |
| Kentuckiana (Louisville, KY) | 37 | $40 |
| Detroit, MI | 08 | $40 |
| Western Michigan | 38 | $30 |
| Minnesota | 07 | $35 |
| Omaha, NE | 23 | $30 |
| Central Ohio (Columbus) | 27 | $55 |
| Greater Cincinnati, OH | 03 | $35 |
| Northeast Ohio (Cleveland) | 26 | $30 |
| Northwest Ohio | 188 | $30 |
| Milwaukee, WI | 57 | $60 |
| Madison, WI | 243 | $50 |
| **Northeastern United States** | | |
| Greater Hartford, CT | 28 | $30 |
| Central Maryland (Baltimore) | 24 | $25 |
| New England | 18 | $30 |
| New Jersey | 30 | $40 |
| Central New York (Syracuse) | 29 | $0 |
| Hudson Valley, NY (Albany) | 120 | $0 |
| New York Metropolitan | 10 | $50 |
| Western New York (Buffalo/Rochester) | 46 | $30 |
| Harrisburg, PA | 45 | $25 |
| Philadelphia, PA | 06 | $40 |
| Pittsburgh, PA | 13 | $30 |
| Rhode Island | 197 | $25 |
| Greater Washington, D.C. | 05 | $40 |
| **Southeastern United States** | | |
| Birmingham, AL | 65 | $35 |
| Huntsville, AL | 221 | $30 |
| Central Florida (Orlando) | 67 | $45 |
| Jacksonville, FL | 58 | $30 |
| South Florida | 33 | $50 |
| Tallahassee, FL | 213 | $25 |
| West Florida (Tampa) | 41 | $50 |
| Atlanta, GA | 39 | $50 |
| Charlotte, NC | 51 | $35 |
| Research Triangle (Raleigh, NC) | 59 | $35 |
| South Carolina Midlands (Columbia, SC) | 54 | $30 |
| Memphis, TN | 48 | $65 |
| Middle Tennessee (Nashville) | 102 | $45 |
| Virginia | 22 | $35 |
| **Southwestern United States** | | |
| Central Arkansas (Little Rock) | 82 | $70 |
| Fayetteville, Arkansas | 235 | $50 |
| Denver, CO | 16 | $40 |
| Baton Rouge, LA | 85 | $35 |
| Greater New Orleans, LA | 61 | $35 |
| Greater Kansas City, MO | 87 | $40 |
| Springfield, MO | 214 | $35 |
| St. Louis, MO | 11 | $25 |
| New Mexico (Albuquerque) | 83 | $25 |
| Central Oklahoma (OK City) | 49 | $30 |
| Tulsa, OK | 34 | $40 |
| Austin, TX | 20 | $25 |
| Greater Houston Area, TX | 09 | $40 |
| North Texas (Dallas) | 12 | $40 |
| San Antonio/So. Texas | 81 | $30 |
| **Western United States** | | |
| Anchorage, AK | 177 | $20 |
| Phoenix, AZ | 53 | $45 |
| Tucson, AZ | 237 | $30 |
| Los Angeles, CA | 01 | $25 |
| Orange County, CA (Anaheim) | 79 | $35 |
| Sacramento, CA | 76 | $35 |
| San Francisco, CA | 15 | $45 |
| San Diego, CA | 19 | $40 |
| Silicon Valley, CA (Sunnyvale) | 62 | $45 |
| Hawaii (Honolulu) | 71 | $40 |
| Boise, ID | 42 | $40 |
| Las Vegas, NV | 187 | $25 |
| Portland, OR | 50 | $35 |
| Utah (Salt Lake City) | 04 | $35 |
| Mt. Rainier, WA (Olympia) | 129 | $20 |
| Puget Sound, WA (Seattle) | 35 | $35 |
| **OCEANIA** | | |
| Adelaide, Australia † | 68 | $22 |
| Brisbane, Australia † | 44 | $33 |
| Canberra, Australia † | 92 | $33 |
| Melbourne, Australia † | 47 | $22 |
| Perth, Australia † | 63 | $33 |
| Sydney, Australia † | 17 | $38.50 |
| Auckland, New Zealand | 84 | $50 |
| Wellington, New Zealand | 73 | $21 |
| Papua New Guinea | 152 | $30 |

† Cost includes AUS GST.

**To receive your copy of the *ISACA Journal*, please complete the following subscriber information:**

**Size of ENTIRE organization**
- ☐ Fewer than 50 employees
- ☐ 50 - 149 employees
- ☐ 150 - 499 employees
- ☐ 500 - 1,499 employees
- ☐ 1,500 - 4,999 employees
- ☐ 5,000 - 9,999 employees
- ☐ 10,000 - 14,999 employees
- ☐ 15,000 or more employees
- ☐ Not applicable

**Size of IT audit staff** *(local office)*
- ☐ 0 individuals
- ☐ 1 individual
- ☐ 2-5 individuals
- ☐ 6-10 individuals
- ☐ 11-25 individuals
- ☐ More than 25 individuals
- ☐ Not applicable

**Size of information security staff** *(local office)*
- ☐ 0 individuals
- ☐ 1 individual
- ☐ 2-5 individuals
- ☐ 6-10 individuals
- ☐ 11-25 individuals
- ☐ More than 25 individuals
- ☐ Not applicable

**Your level of purchasing authority**
- ☐ Recommend Products/Services
- ☐ Approve Purchases
- ☐ Recommend and Approve
- ☐ Not applicable

# ISACA®

## MEMBERSHIP APPLICATION

**Join online and save US $20.00**
***www.isaca.org/join***

*Please complete both sides*
U.S. Federal I.D. No. 23-7067291
Phone: +1.847.660.5505 • Fax: +1.847.253.1443
Email: *membership@isaca.org*

☐ MR. ☐ MS. ☐ MRS. ☐ MISS ☐ OTHER _____ Date _____
MONTH/DAY/YEAR

Name _____
FIRST MIDDLE LAST/FAMILY

*PRINT NAME AS YOU WANT IT TO APPEAR ON MEMBERSHIP CERTIFICATE*

Residence address _____
STREET

CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Residence phone _____ Residence facsimile _____
AREA/COUNTRY CODE AND NUMBER AREA/COUNTRY CODE AND NUMBER

Company name _____

Title _____

Business address _____
STREET

CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Business phone _____ Business facsimile _____
AREA/COUNTRY CODE AND NUMBER AREA/COUNTRY CODE AND NUMBER

E-mail _____

**Send mail to**
☐ Home ☐ Business

**Chapter Affiliation**
☐ Chapter Number *(see reverse)* _____
*or*
☐ Member at large *(no chapter within 50 miles/80 km)*

**How did you hear about ISACA?**
☐ ISACA Chapter
☐ ISACA Event
☐ ISACA Journal
☐ Career Centre
☐ Do not remember
☐ Email
☐ Employer
☐ Friend/Colleague
☐ Postal Mail
☐ Professor/Teacher
☐ Publication
☐ Social Media
☐ Tradeshow/Seminar
☐ Web Advertisement
☐ Web Site Reference
☐ Other

**Member Get A Member Referral Information**
If you have been referred by an ISACA member, please enter the ISACA Member ID# that was provided to you.
Referring Member ID# _____

**Please note:** Membership in the association requires you to belong to a chapter when you live or work within 50 miles/80 km of a chapter territory. The name of the chapter is indicative of its territory. If you live farther than 50 miles/80 km from a chapter territory, select member at large. Chapter selection is subject to verification by ISACA International Headquarters. Cities listed in parentheses are a reference to where the majority of chapter meetings are held. Please contact your local chapter at *www.isaca.org/chapters* for other meeting locations.

ISACA requires members to provide certain demographic information to help us understand and better serve our constituents, and to ensure that we deliver information that is relevant to you.

**Current field of employment** *(check one)*
☐ Advertising/Marketing/Media
☐ Aerospace
☐ Education/Student
☐ Financial/Banking
☐ Government/Military—National/State/Local
☐ Health Care/Medical
☐ Insurance
☐ Legal/Law/Real Estate
☐ Manufacturing/Engineering
☐ Mining/Construction/Petroleum/Agriculture
☐ Not applicable
☐ Pharmaceutical
☐ Public Accounting
☐ Retail/Wholesale/Distribution
☐ Technology Services/Consulting
☐ Telecommunications/Communications
☐ Transportation
☐ Utilities
☐ Other _____

**Level of education achieved** *(indicate degree achieved, or number of years of university education if degree not obtained)*
☐ one year or less
☐ two years
☐ three years
☐ four years
☐ five years
☐ six years or more
☐ AS Degree
☐ BS/BA Degree
☐ MS/MBA/Masters
☐ Ph.D
☐ Not applicable
☐ Other _____

**Certifications obtained**
**(other than CISA, CISM, CGEIT, CRISC)**
☐ ACA
☐ CA
☐ CFE
☐ CIA
☐ CISSP
☐ CPA
☐ MCSE
☐ PMP
☐ Other _____

**Work experience**
*(check the number of years of information systems related work experience)*
☐ No Experience
☐ 1-3 years
☐ 4-6 years
☐ 7-9 years
☐ 10-12 years
☐ 13 years or more
☐ Not applicable

**Current professional activity** *(If not your title, please select the BEST match)*
☐ CEO, President, Owner, General/Executive Manager
☐ CAE, General Auditor, Partner, Audit Head/VP/EVP
☐ CISO/CSO, Security Executive/VP/EVP
☐ CIO/CTO, Info Systems/Technology Executive/VP/EVP
☐ CFO, Controller, Treasurer, Finance Executive/VP/EVP
☐ Chief Compliance/Risk/Privacy Officer, VP/EVP
☐ IT Audit Director/Manager/Consultant
☐ Security Director/Manager/Consultant
☐ IT Director/Manager/Consultant
☐ Compliance/Risk/Privacy Director/Manager/Consultant
☐ IT Senior Auditor (External/Internal)
☐ IT Auditor (External/Internal Staff)
☐ Non-IT Auditor (External/Internal)
☐ Security Staff
☐ IT Staff
☐ IT/IS Compliance/Risk/Control Staff
☐ Professor/Teacher
☐ Student
☐ Other

**Birth Year** _____

**Payment due**
- International dues † $ 135.00 (US)
- Chapter dues *(see reverse)* $ _____ (US)
- New member processing fee $ 30.00 (US)*

PLEASE PAY THIS TOTAL $ _____ (US)

† For student membership information please visit *www.isaca.org/student*

* Membership dues consist of international dues, chapter dues and new member processing fee. Join online and save US $20.00.

Membership dues are nonrefundable and nontransferable.

**Mail your application and check to:**
ISACA • 1055 Paysphere Circle • Chicago, IL 60674 • USA

**Method of payment**
☐ Check payable to "ISACA" in US dollars, drawn on US bank
☐ Send invoice (Applications cannot be processed until dues payment is received.)
☐ MasterCard ☐ VISA ☐ American Express ☐ Diners Club ☐ Discover

All payments by credit card will be processed in US dollars

Credit Card # _____

Print name of cardholder _____

Expiration date _____
MONTH/YEAR

Signature _____

By applying for membership in ISACA, members agree to hold the association and its chapters, and the IT Governance Institute, and their respective officers, directors, members, trustees, employees and agents, harmless for all acts or failures to act while carrying out the purposes of the association and the institute as set forth in their respective bylaws, and they certify that they will abide by the association's Code of Professional Ethics (*www.isaca.org/ethics*).

Full payment entitles new members to membership from the date payment is processed by International Headquarters through 31 December 2019. No rebate of dues is available upon early resignation of membership.

Contributions, dues or gifts to ISACA are not tax deductible as charitable contributions in the United States. However, they may be tax deductible as ordinary and necessary business expenses.

Your contact information will be used to fulfill your request to become an ISACA member, and may also be used by ISACA to send you information about related ISACA goods and services, and other information in which we believe you may be interested. As an ISACA member, we will be sure to keep you up-to-date on the latest products and services that are available to our community. By applying for membership, you confirm the information provided on this form is complete and accurate, and you authorize ISACA to contact you at the address and numbers you have provided, including to provide you with marketing and promotional communications. You further represent that the information you provided is yours and is accurate. To learn more about how we use the information you have provided on this form, please read our Privacy Policy, available at www.isaca.org. Should you elect to attend one of our events or purchase other ISACA programs or services, information you submit may also be used as described to you at that time.

**The dues amounts on this application are valid 1 August 2019 through 31 May 2020.**

# ISACA®

## STUDENT MEMBERSHIP APPLICATION

www.isaca.org/students

*Please complete both sides*
U.S. Federal I.D. No. 23-7067291
Phone: +1.847.660.5505 • Fax: +1.847.253.1443
Email: *students@isaca.org*

☐ MR. ☐ MS. ☐ MRS. ☐ MISS ☐ OTHER _____ Date _____
MONTH/DAY/YEAR

Name _____
FIRST MIDDLE LAST/FAMILY

Address at school _____
STREET

_____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Phone at school _____ Facsimile at school _____
AREA/COUNTRY CODE AND NUMBER AREA/COUNTRY CODE AND NUMBER

University Name _____

Field of study/major of concentration _____ Expected date of graduation _____

Home address _____
STREET

_____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Home phone _____ Home facsimile _____
AREA/COUNTRY CODE AND NUMBER AREA/COUNTRY CODE AND NUMBER

E-mail _____

ISACA requires members to provide certain demographic information to help us understand and better serve our constituents, and to ensure that we deliver information that is relevant to you.

**Send mail to**
- ☐ Home
- ☐ School

**Degree Program**
- ☐ Undergraduate
- ☐ Graduate

**How did you hear about ISACA?**
- ☐ ISACA Chapter
- ☐ ISACA Event
- ☐ ISACA Journal
- ☐ Career Centre
- ☐ Do not remember
- ☐ Email
- ☐ Employer
- ☐ Friend/Colleague
- ☐ Postal Mail
- ☐ Professor/Teacher
- ☐ Publication
- ☐ Social Media
- ☐ Tradeshow/Seminar
- ☐ Web Advertisement
- ☐ Web Site Reference
- ☐ Other

**Verification of Student Status**

To become a student member, you must attach one of the following:
- Current university issued class schedule
- Copy of your transcript showing the courses you are taking
- Letter from the College or University stating that you are currently enrolled at the school

**NOTE:** Both your printed application form and document verifying your student status are required for processing. Please allow 3-5 business days to obtain the student member rate on exams, conferences or purchases.

All International Association benefits will be provided electronically.

**Payment due**
- International dues for students $ 25.00 (US)
- Chapter dues #____ (see following page) $ _____ (US)

PLEASE PAY THIS TOTAL* $ _____ (US)

* Membership dues consist of international dues and chapter dues.
Membership dues are non-refundable and non-transferable.

**Mail your application and check to:**
ISACA • 1055 Paysphere Circle • Chicago, IL 60674 • USA

**Method of payment**
- ☐ Check payable to "ISACA" in US dollars, drawn on US bank
- ☐ Send invoice (Applications cannot be processed until dues payment is received.)
- ☐ MasterCard ☐ VISA ☐ American Express ☐ Diners Club ☐ Discover

All payments by credit card will be processed in US dollars

Credit Card # _____
Print name of cardholder _____
Expiration date _____
MONTH/YEAR

Signature _____

By applying for membership in ISACA, members agree to hold the Association and its chapters, and the IT Governance Institute, and their respective officers, directors, members, trustees, employees and agents, harmless for all acts or failures to act while carrying out the purposes of the Association and the Institute as set forth in their respective bylaws, and they certify that they will abide by the Association's Code of Professional Ethics (www.isaca.org/ethics).

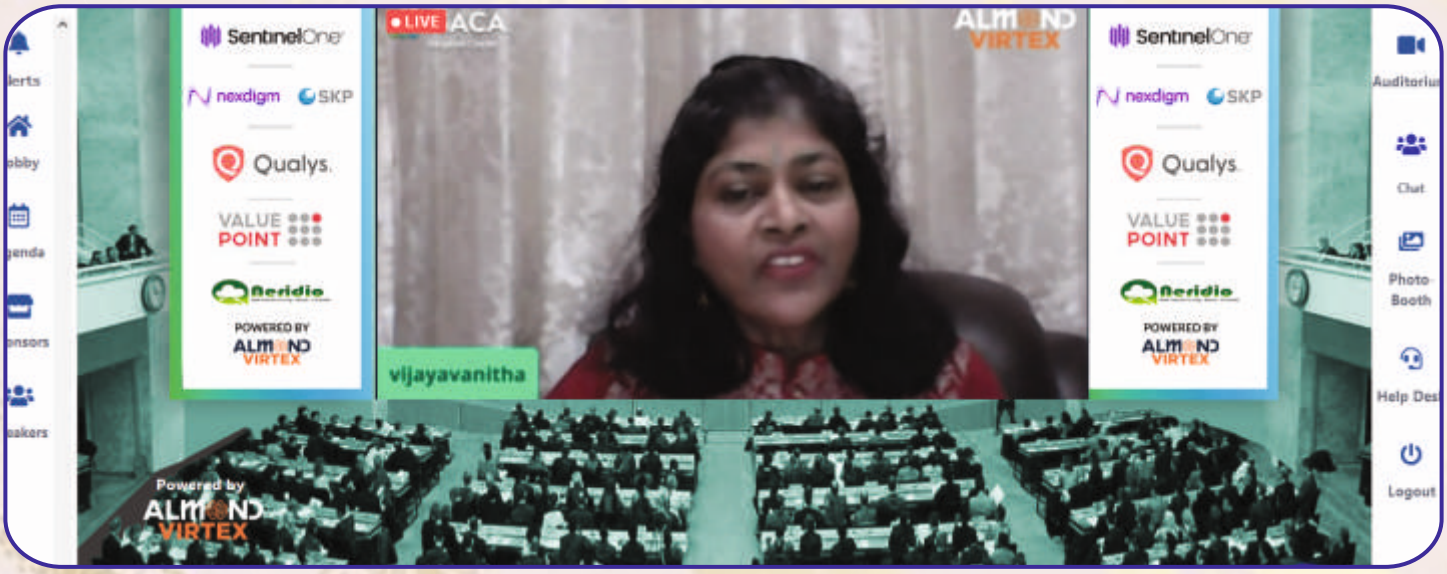
Full payment entitles new members to membership from the date payment is processed by International Headquarters through 31 December 2018. No rebate of dues is available upon early resignation of membership.

Contributions, dues or gifts to the Information Systems Audit and Control Association are not tax deductible as charitable contributions in the United States. However, they may be tax deductible as ordinary and necessary business expenses.

Your contact information will be used to fulfill your request to become an ISACA member, and may also be used by ISACA to send you information about related ISACA goods and services, and other information in which we believe you may be interested. As an ISACA member, we will be sure to keep you up-to-date on the latest products and services that are available to our community. By applying for membership, you confirm the information provided on this form is complete and accurate, and you authorize ISACA to contact you at the address and numbers you have provided, including to provide you with marketing and promotional communications. You further represent that the information you provided is yours and is accurate. To learn more about how we use the information you have provided on this form, please read our Privacy Policy, available at www.isaca.org. Should you elect to attend one of our events or purchase other ISACA programs or services, information you submit may also be used as described to you at that time.

**The dues amounts on this application are valid 1 June 2019 through 31 July 2020.**


*Message from ISACA, CEO - Mr. David Samuelson*

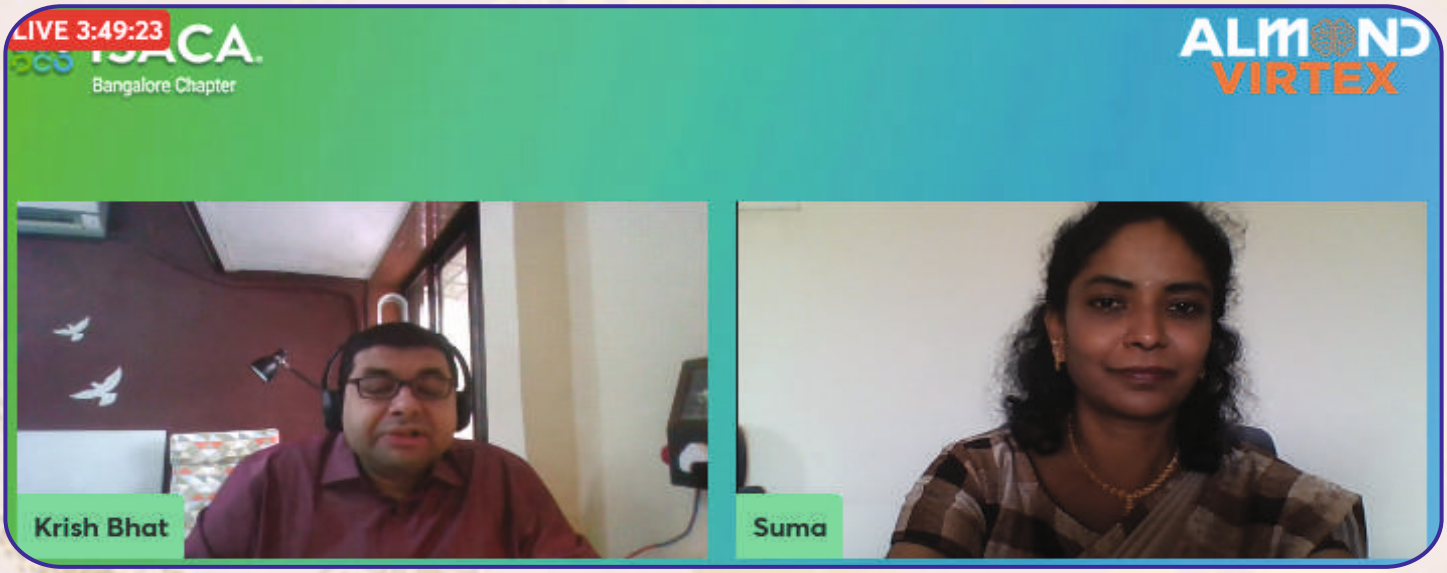

*The remote workforce Cyber problem – Resistance to adoption by Mr. Debashish Jyotiprakash , CTSO, Qualys Inc*



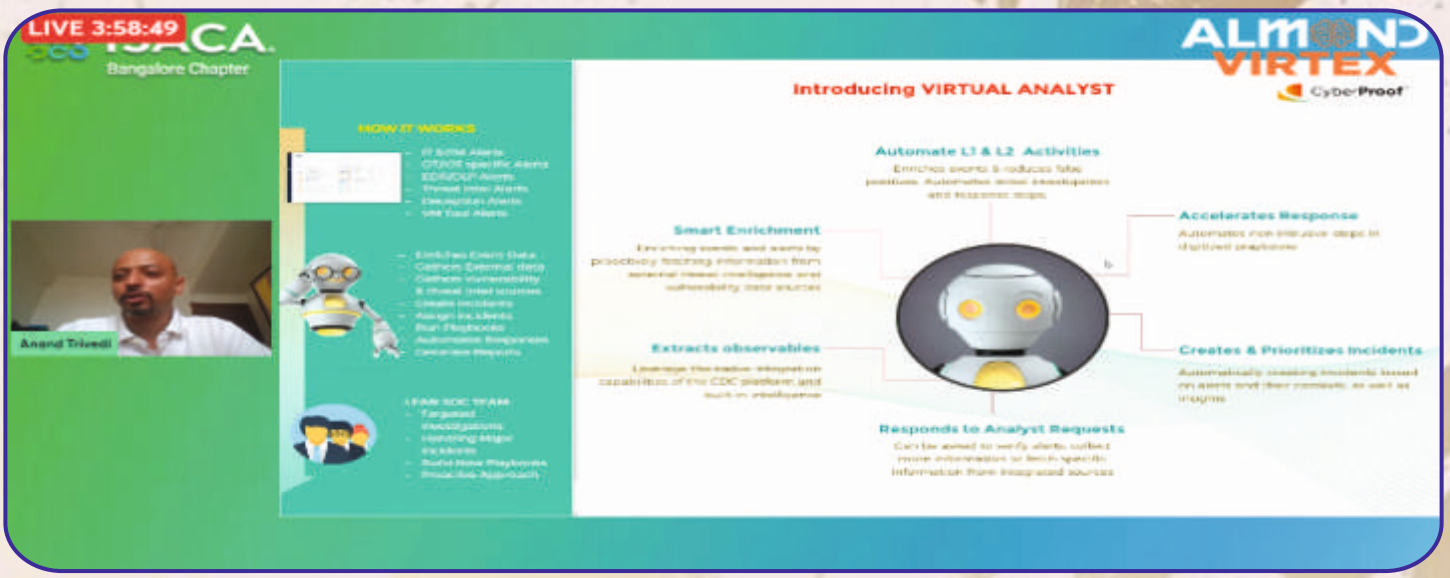
*1st Prize winner of Whitepaper Contest*

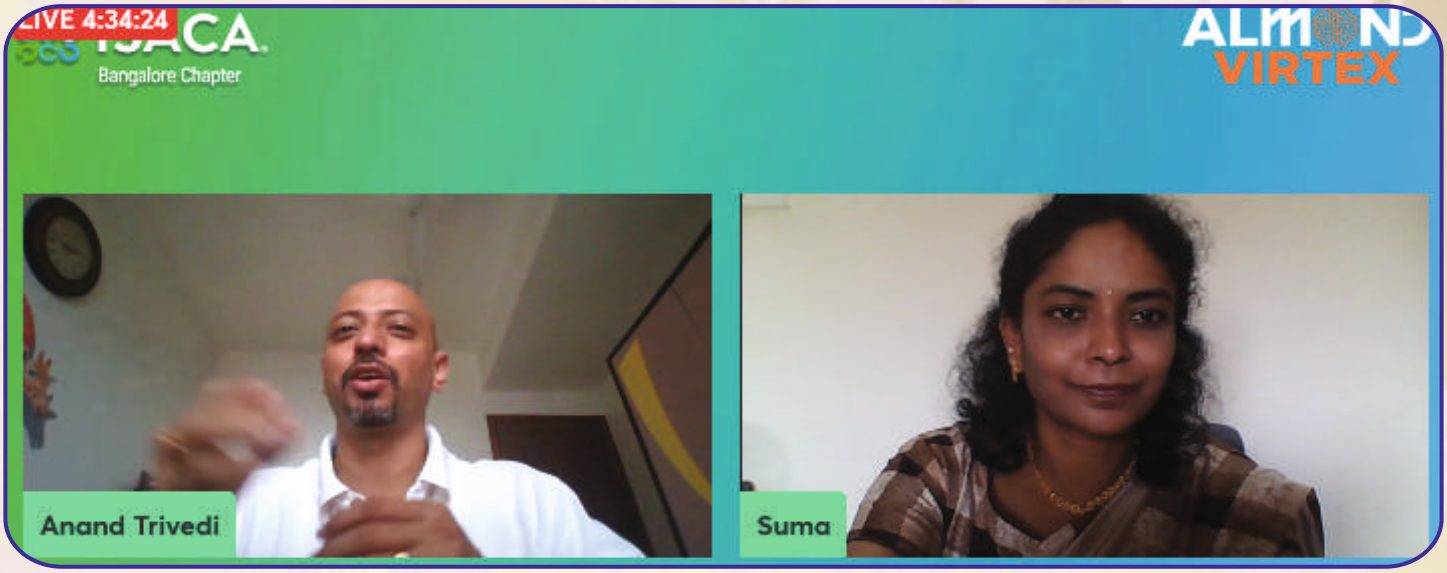

*1st & 2nd Prize winners of Whitepaper Contest*


*All the three prize winners of Whitepaper Contest*




*Cyber Risk in a Post Pandemic Era - Trust Nothing, Distrust Nothing*
*Mr. Krishnanand N. Bhat, Director, Technology advisor, Nexdigm (SKP),*




*Building a Next Generation Cloud Native Smarter SOC - Mr. Anand Trivedi, APAC - Business Head, UST Global*


*No more Ransomware Strike – With SuperHuman AI Cybersecurity Defense - Mr. Yashaswi Mudumbai, Technical Director - India & SAARC, Sentinel One*


*Key Inflection Points on your Journey to XDR - Mr. Setu Kulkarni, VP Corporate Strategy & BD - Whitehat security US / NTTS*


*Building a Next Generation Cloud Native Smarter SOC - Mr. Anand Trivedi, APAC - Business Head, UST Global*


*Preparing the Next Generation of Cybersecurity Professionals, Sidharth Mutreja, Cyberbit, Regional Director- SE- South Asia & ASEAN*


Panel Discussion - **Security transformation for digital transformation - Challenges and approach**

**Vaidyanathan Iyer, COO IBM Cybersecurity Command Center (Moderator)**

**1. Mr. Pawan Desai, CEO Mitkat Advisory**

**2. Mrs. Seema Bangera, Independent Cyber Security Consultant**

**3. Mr. Damanjit S. Uberoi,, Executive Director, Grant Thornton**

**4. Mr. P C Joseph, Independent Consultant & Academic Researcher**


*Wrap-up & Vote of Thanks by Vanitha (Secretary of ISACA Bangalore Chapter)*

ISACA COMMUNITY DAY

PEOPLE | SERVICE | PURPOSE

## ISACA CommunITy Day - 2nd October 2021

*It gives immense pride to the ISACA Bangalore chapter for having participated in the 3rd Annual ISACA CommunITy Day on the 2nd October 2021. Another incredible way to give back to the community and make a positive impact in the world.*

*The EC members of the ISACA Bangalore chapter and volunteers visited NGO Sparsha located at Hesarughatta, Tumkur Road.*

*It was indeed a privilege to visit this institution which is contributing towards the society with the objective of creating a **safe** home for every child with **free** access to basic facilities like food, health, education, and clothing, providing skills-oriented **education** to empower underprivileged children and youth.*

*As part of the program, the EC team had the opportunity to share their thoughts, with the children, on how to be secure when engaged in online activities, as all the children are now attending online classes and remote learning.*

*It was a treat to the eyes to witness all the creativity of the children which bloomed in the form of wonderful artifacts, green house, and gardening.*

*The chapter had also distributed a few goodies as a gesture of giving back to the community which was warmly accepted and appreciated by the institution.*

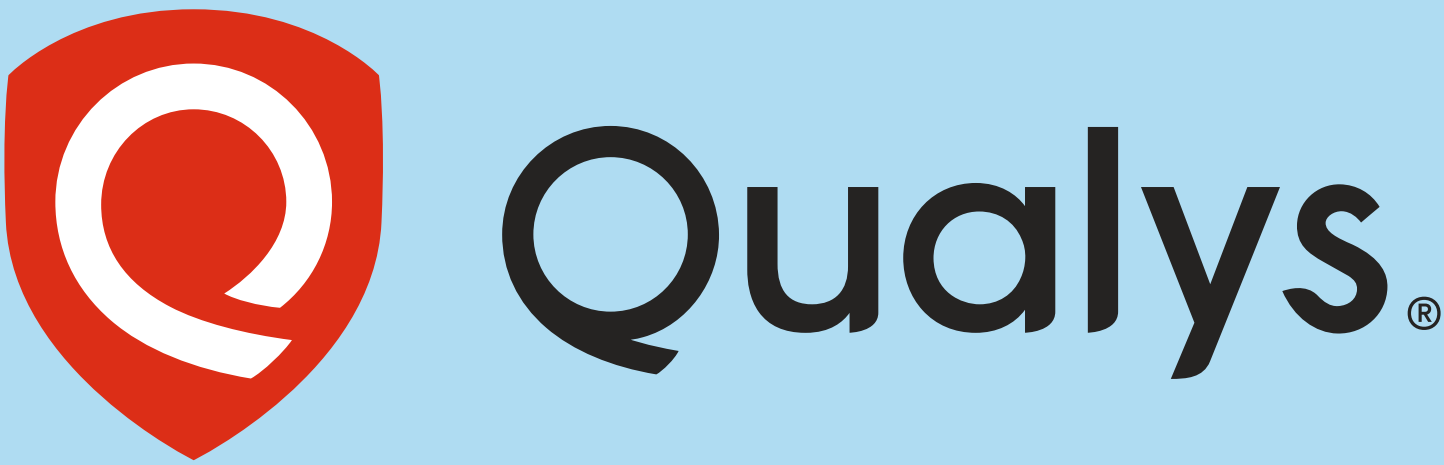
*ISACA Bangalore Chapter appreciates the opportunity given to "give back to the world", through the CommunITy day program.*

*ISACA Bangalore chapter once again has demonstrated " making a positive impact in the world" through their active participation and commitment.*


Move Your
Career Forward
with an ISACA
Certification
Get certified and get ahead.
ISACA
Move Your
Career Forward
with ISACA
Certification
Get certified and get ahead.
ISACA


Move Your
Career Forward
with an ISACA
Certification
Get certified and get ahead.
ISACA
Move Your
Career Forward
with ISACA
Certification
Get certified and get ahead.
ISACA


Neridio
Rationalizing Data Clouds


Qualys®

*Book Post*

# VALUE POINT®

**If undelivered please return to :**

ISACA
Bangalore Chapter

*# S.13, 531A, 2nd Floor, Priya Chambers*
*Dr. Rajkumar Road, 2nd Stage, Rajajinagar*
*Opp. St. Theresa's Hospital, Bangalore - 560 010.*
*Ph. : 23377956, Email : chapter@isacabangalore.org*

Printed @ Cauvery Ent. © 22128682

**Chapter Reg No : 433/2002-2003**