APRIL - 2021 ISSUE

ISACA
Bangalore Chapter

INFOCITY AUDITOR

ISACA Bangalore Chapter - News Letter

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!

ISACA Bangalore Chapter

InfoclTy Auditor

April - 2021

From The Desk Of The President

Dear Members,

Greetings and thanks for renewing your 2021 membership. Every year your membership elevates you to a new tier (Bronze, Silver, Gold and Platinum) with greater rewards and access to exclusive tools and insights which helps you to excel even more in your role.

It is with great pride, we bring to you that we have completed 25 successful years post inception of ISACA Bangalore Chapter. We have seen various phases during the last 25 years. We have ensured we excel year after year and increase the quality of delivery and value to our Members, that is you. All of you have been a pillar towards the growth of our Chapter. We will continue to provide you value add in all forms and means and expect your active participation on a continous basis. We wanted to have a gala time for our Silver Jubilee Celebrations, however due to the current pandemic conditions, we are unable to host any physical meeting. We are continuously looking at the situation and will look for an opportunity to celebrate in a grand style.

We have already concluded two rounds of the Review Classes for our ISACA Certifications in this term. The first batch concluded in Feb 2021 and the 2nd batch training started effective March 2021 with good number of participation for CISA, CISM & CRISC training helping the members collaborate and prepare for the Examinations.

We had rolled out the survey to all of you and we got good participation and we from the Executive Committee are working towards implementing certain suggestions that you all have provided. We are happy to see the participation.

We re-lauched the SheLeadsTech program and conducted an event which was actively participated by many of you. We also introduced Short Learning Bytes (SLB) and have plans to conduct focused group workshop in the coming months.

Building Committee kept meeting regularly and have shortlisted two properties. Reviews are on and post all due diligence, a decision would be taken.

Planning and preparations for the Annual Conference has started. This year the theme of the conference is **"Digital transformation - Saviour for Pandemic and Cyber Security".** This year's conference will be on the virtual platform keeping the safety of the members in mind and ensuring no physical movement happens during this pandemic time. Please watch out for more information in our regular communication.

We all are going through a difficult phase due to the serge in the COVID cases, hence request all of you to take proper care of yourself, your family, your near and dear ones and stay safe in this pandemic situation.

As always, we solicit your active participation in the Chapters events and initiatives including monthly CPE meetings, SLB, Newsletter article contribution, Review Classes for aspiring students and more.

Looking forward to meeting you all in the next event either Physically or Virtually !!!

Warm Regards,

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

Message From the Vice President

Dear Members,

Greetings!!

Many thanks for the renewal your 2021 membership and certification(s), we are sure that all of you are getting continuous benefits and support from ISACA HQ and our chapter.

As you all aware that ISACA's Privacy technologist CDPSE certification's early adoption is closed and now you can go through the exam route to get certified with relevant privacy domain experience.

Three outstanding sessions delivered as part of CPE on 5G - The Cyber Security Approach, Security in the World of Containers and Hybrid Cloud, and Third-party risk management and we are sure you have enjoyed the sessions.

We are happy to inform you that our first SLB (Short learning bytes) session, 'Practical approach to containing Ransomware', showed very good response among members. A series of SLB sessions will be delivered in the coming months.

We also re-launched the program SheLeadsTech in March in the online event with leading women speakers from various industriesas part of the International Women's Day celebrations.

ISACA launched a new Modular, Stackable, Knowledge & Performance-affirming New Credential - under ITCA. The ISACA® **Information Technology Certified Associate™ (ITCA™)** assesses and affirms both knowledge and the ability to perform IT-related tasks that the real-world workplace demands. Through five IT-career-related certificate programs, ITCA will jump-start and fast track your professional journey or add skills and knowledge you can apply immediately to your IT audit, risk, security, governance, or privacy role. We would encourage you to spread this new certification awareness among your friends, colleagues, Students or fresh Graduates, Individuals with little or zero years' experience in IT, and Individuals seeking to get into an IT career or career changers seeking to switch to a new field of IT. For more details kindly visit our web site.

Thank you once again for the renewal of your ISACA membership and certification and for supporting the chapter to maintain the "number one chapter in India" in terms of membership.

Now the pandemic came back with double strength as part second wave. We all have been working from home to save the world.While we do this, we are also fighting another threat like'Damocles Sword' hanging on the head of the cyber world, called cybercrime. I am sure we will be able to overcome both threats and achieve our goals

I'd like to take this moment to thank all for your support.

Regards,

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

Message From Secretary

Dear Friends,

During current times it is virtually impossible to think, write or speak about anything without mentioning COVID-19. It is so truewith the ISACA Bangalore Chapter too.

The work of Executive Committee involves considerable effort&responsibility,andthe service of members is essential to the success of the Chapter.The inability to follow the usual procedures due to the COVID-19 pandemic protocols and the dire economic situation has made the functioning of the Committee even more challenging than ever before.

I feel that being able to contribute to the functioning of the Committee is a worthy goal and as Secretary, I am doing my best to facilitate it.

In terms of meetings, the Executive Committee has probably spent at least twice as much time attempting to strike a balance between virtual, in-person, and postponed events.We anticipate a lively and interesting Virtual Annual Conference in 2021.We have held meetings in this format before.We've made an effort to take notes from them.Although we will all miss the social contacts, it is at times like these that it is even more crucial to support the needs and safety of our members.

Whatever the case may be, I am confident that we will have a fantastic Annual Conference 2021.Your President has already organized the Annual Conference program that is packed with Technological innovation and sessions that address your career/professional developments.

I am determined to connect with you Whether I see you on my computer or in-person. Do not forget to say hello to us. See you in August 2021!

I wish you all the bestand stay safe.

Regards,

VIJAYAVANITHA, CISA, CIA, MBA, M Com
Secretary

Chapter Highlights for the period from January to March 2021

CPE Meetings:

1. **Topic : "Security in the World of Containers and Hybrid Cloud"**
   Venue : Web-based ONLINE session via Zoom Webinar Platform
   Date : 23-Jan-2021 (Saturday) Time : 5:30 PM - 7:30 PM IST
   Free Attendance - 2 CPE Credits offered

Topic Summary:

Security in the World of Containers and Hybrid Cloud: Containers and hybrid cloud technologies have made the security landscape much more complex. Security teams are increasingly finding it challenging to keep up with the changing risks, compliance requirements, tools, and architectural changes introduced by these technologies. As traditional infrastructure evolves to a mix of bare metal, virtual, cloud, and container environments, how can you maintain security, governance, compliance and reduce risk amid this growing complexity? Traditional perimeter-based network security is no longer effective on its own, and security teams must rethink their approach.

Speaker: Ameeta Roy

Speaker profile: Ameeta Roy, Director, Solutions Architecture, Red Hat, Urban Bangalore. Ameeta has 30 + years of experience in IT having worked across technology and services in leading organizations. Ameeta has varied experience in Leadership, SDLC and Pre-Sales in her professional career.

Members/Non Members participated from various countries, the meetings was well appreciated by all the participants.

2. **Topic : "5G - The Cyber Security Approach"**
   Venue : Web-based ONLINE session via Zoom Webinar Platform
   Date : 20-Feb-2021 (Saturday) Time : 5:30 PM - 7:30 PM IST
   Free Attendance - 2 CPE Credits offered

Topic Summary:

5G - The Cyber Security Approach: 5G is a very fast moving combination of technology and business. The need for ubiquitous fast connectivity and mobility are pushing the delivery of 5G faster than anyone imagined. In this session, we will go over the architecture for 5G, and its applications .We will focus on infrastructure security plus threats and concerns as mobility and IoT continue to come together delivered in the evolved data center and network. And finally will detail security concerns and threats that come with this new evolution to the network infrastructures we operate today.

Speaker: Mr. Rajesh seshan.

Speaker profile: Rajesh Seshan, Head, Cybersecurity Advisory Services division at Cisco. A technophile having approximately 30 years of IT related experience ranging from Security to programming to systems to networking to virtualization to handling operations and services for his own start-up across various geographies. He is a 20 year old CCIE in routing and switching. Rajesh currently heads the Cybersecurity advisory services division at Cisco for India and SAARC.

151 Members/ Non Members participated from various countries, the meetings was well appreciated by all the participants.

3. Topic : "Cyber Security Due Diligence during Mergers and Acquisitions"
Launch / Relaunch : "She leads Tech" with a speaker session
Topic for Panel Discussion : Women Empowerment - Support, Challenges, Way Forward
Venue : Web-based ONLINE session via Zoom Webinar Platform
Date : 6-Mar-2021 (Saturday) Time : 5:30 PM - 7:30 PM IST
Free Attendance - 2 CPE Credits offered

Speaker: Mr. Runa Dalal, Director - Risk Advisory - Cyber Risk, Deloitte.

Panelists are:
- **Satyavathi Divadari,** Chief Cyber Security Architect - Microfocus
- **Priya Madhavan**, Consultant at Nasscom Futureskills
- **Jamuna Swamy**, Strategic Advisor at Infomine S/w Solu LLP, Sr Advisor and Mentor at Vault Infosec
- The Panel discussion moderated by Ms. **Suma K Venkatesh,** Director SIG, ISACA Bangalore Chapter.

116 Members/ Non Members participated from various countries, the meetings was well appreciated by all the participants.

4. Topic : "Third Party Risk Management"
Venue : Web-based ONLINE session via Zoom Webinar Platform
Date : 27-Mar-2021 (Saturday) Time : 5:30 PM - 7:30 PM IST
Free Attendance - 2 CPE Credits offered

Topic Summary:

Third Party Risk Management: Coverage Areas: • Scope of TPRM • Types of TPRM • Differentiate between Traditional RM and TPRM • Components of TPRM

Speaker: Dr. Mahesh

Speaker profile: Dr. Mahesh is an experienced Information Security Professional having 25 + years of experience in Security Governance, Policy Management, GRC management, GRC, Compliance, Risk Assessment, Third Party Risk Management, Technical Security assurance.

Dr. Mahesh is currently working as "Director - Corporate Security" in Cognizant. He is also serving as "Vice President" of ISACA Chennai Chapter.

212 Members/ Non Members participated from various countries, the meetings was well appreciated by all the participants.

Intro Seminar:

1. 'Introductory Seminar' - conducted on ISACA Certification Courses.
Venue : Web-based ONLINE session via Zoom Webinar Platform
Date : 13-Mar-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 Quarter (April to June 2021)

The Chapter announced the Review Classes in the New Year 2021 as per the below training calendar and the registrations are open now.

ISACA Bangalore Chapter

CISA, CISM, CRISC – Online Review Classes – 2021

Registrations Open – Register Now !!

Full Day: 9:30 am to 5:30 pm IST – live online via Zoom Platform
Fees (per course): Members INR 8,500 | Non-members: INR 9,500
Key features: Industry Faculty, Official ISACA Presentations, Q&A discussion and more

CISA Certified Information Systems Auditor | CISM Certified Information Security Manager | CRISC Certified in Risk and Information Systems Control

CISA – 5 Days		CISM – 4 Saturdays		CRISC – 4 Sundays	
27-Mar	Domain 1: Information Systems (IS) Auditing Process	17-Apr	Domain 1: Information Security (IS) Governance	18-Apr	Domain 1: IT Risk Identification
28-Mar	Domain 2: Governance and Management of IT	24-Apr	Domain 2: Information Risk Management	25-Apr	Domain 2: IT Risk Assessment
03-Apr	Domain 3: IS Acquisition, Development and Implementation	01-May	Domain 3: IS Program Development and Management	02-May	Domain 3: Risk Response Mitigation
04-Apr	Domain 4: IS Operations and Business Resilience	08-May	Domain 4: IS Incident Management	09-May	Domain 4: Risk and Control Monitoring and Reporting
10-Apr	Domain 5: Protection of Information Assets				

Registration Link: https://www.meraevents.com/event/isaca-blr **Queries:** please write to chapter@isacabangalore.org

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

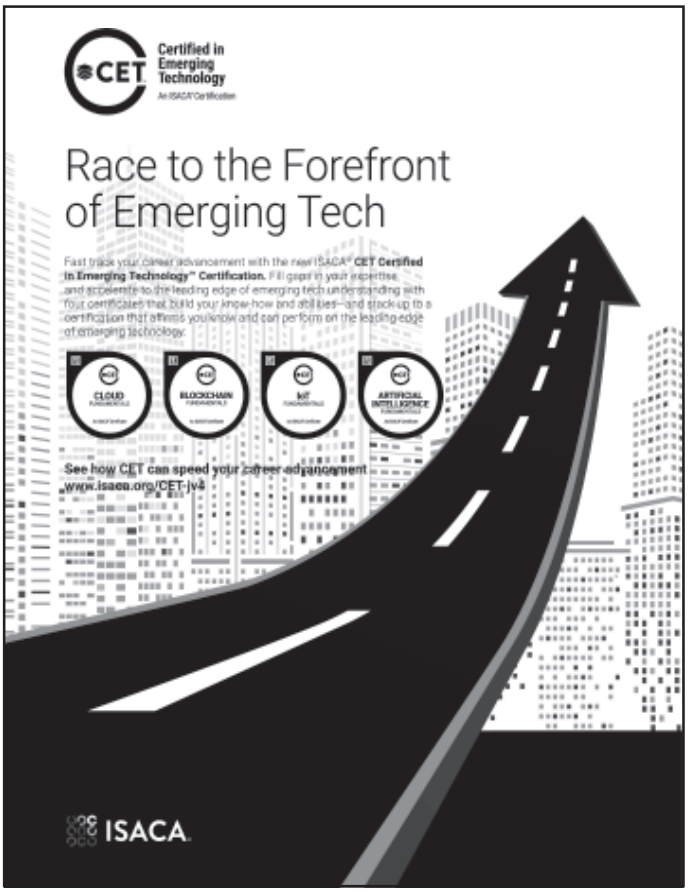
In case you need any assistance, please do not hesitate to reachout to me or Chapter Office at chapter@isacabangalore.org

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: **$20.00**
Total Dues for 2020 membership renewal: **US$ 155.00**

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



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

FEATURE

Security Discipline and Hygiene Mean Healthy, Naturally

In this time of the COVID-19 pandemic, personal cleanliness and hygiene are discussed more frequently than ever before. It is essential to maintain hygiene to stay safe and prevent the spread of COVID-19. Even from a cost perspective, the cost of being cautious is lower than the cost associated with COVID-19 infection and the psychological costs. The root of hygiene is discipline. It drives maintaining hygiene. Good hygiene is everyone's responsibility to protect themselves and the community.

How does this relate to IT or IT security? If every employee is disciplined in understanding and maintaining secure IT functions and security hygiene, many IT security issues would never occur. For example, employees should understand all of the following concepts to maintain IT security hygiene:

- Use of strong passwords
- Not sharing passwords with anyone
- Not leaving their personal laptop or desktop without locking it
- Use of the facility (i.e., workplace) only for the purpose provided
- Not using enterprise-provided devices for personal purposes
- Avoiding inappropriate websites
- Not installing unapproved software on any work-related device
- Not allowing unauthorized users to access enterprise devices
- Using the most recent security software versions
- Not allowing piggy backing while accessing facilities. Piggy backing refers to when a person tags along with another person who is authorized to gain entry into a restricted area or passed a certain checkpoint. It can be either electronic or physical. There would be no record for the person's entry into the facility, which creates a security issue.

Security hygiene means:

- Focus on the basics (e.g., timely patching, moving away from unsupported versions).
- Security resources are scarce and limited, so security implementation should be prioritized based on business criticality.
- There are numerous security solutions and services available in the market. Choose security

Sundaresan Ramaseshan, CISM, ITIL Foundation, ITIL Service Operations Specialist
Is an IT and security services professional at Ford Motor Private Limited, in Chennai, India. He has more than 27 years of IT industry experience working in various roles in the software development life cycle. He is interested in enhancing his depth of knowledge of the security domain and sharing his knowledge gained from his day-to-day work in operations to benefit the IT community.

products and services based on the business scenario. There is no one-size-fits-all solution.

- Perform security assessments and actions based on the organization's current state. For example, some vulnerabilities may be rated high risk, but the scenario may not be applicable to the organization. On the other hand, there are some vulnerabilities that may be rated medium or low risk in the market but would be high priorities for the organization.
- In this new age of digitalization and business advancement, security teams should engage seamlessly with the business to enable the release of products and services without compromising security.

One way to understand IT security hygiene is to use a bottom-up approach based on the seven layers of security as well as a top-down approach from the leadership perspective.

Per the Open System Interconnection (OSI), as developed by the International Organization for Standardization (ISO), any IT system should have seven layers of security architecture, with each layer having a specific functionality to perform.[1] All seven layers work collaboratively to transmit data from one person to another across the globe.

Security Rule Book: Information Security Policy

For any organization to be successful in establishing security, it should have an information security policy (ISP) to ensure the foundation of security and the appropriate use of resources.

In the complex world of IT, classifying information by the ISO OSI model could be the starting point. As previously stated, there are seven layers of architecture that split the communication system into abstraction layers. For example, a layer that provides error-free communications across a network provides the path needed by applications in layers above it, while it calls the next layer to send and receive packets that constitute the contents of that path.

"FOR ANY ORGANIZATION TO BE SUCCESSFUL IN ESTABLISHING SECURITY, IT SHOULD HAVE AN INFORMATION SECURITY POLICY (ISP) TO ENSURE THE FOUNDATION OF SECURITY AND THE APPROPRIATE USE OF RESOURCES."

Understanding the OSI model helps in understanding the seven layers of security:

1. Physical—This is the lowest level of security. At this layer, systems are locked to keep them safe (e.g., adding physical access restrictions for workstations, restricting access to data centers, restricting access to racks where servers are kept). Having strong security measures implemented at this layer can eliminate issues such as direct wiretapping, signal jamming, tailgating and unauthorized access.
2. Data link—At this layer, data are moved from software to hardware and back. Security at this layer keeps data moving to where they are supposed to go.
3. Network—This layer is also called the Internet layer, as it connects different networks. Security at this layer protects attackers from accessing logins and passwords sent over the network, prevents flooding attacks, and prevents sniffing/snooping attacks.
4. Transport—This layer predominantly transports the workload from point A to point B and makes sure it is delivered securely and without any alteration. Strong security implementation at this layer could avoid denial of service (DoS) and man-in-the-middle (MitM) attacks.
5. Session—The session layer provides the mechanism for opening, closing and managing a session between end user application processes (i.e., a semi-permanent dialog). It adds synchronization points or checkpoints in data streams for long communications. Success of security at this layer means prevention of attacks such as DoS and spoofing.

Enjoying this article?

- Read *Conducting an IT Security Risk Assessment. www.isaca.org/conducting-an-IT-security-risk-assessment*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

6. Presentation—The presentation layer is responsible for presenting the data to the application layer. This may include some form of format or character translation.
7. Application—This layer is the closest to the end users. Some examples are web browsers and email clients. Securing this layer means preventing browser hijacking or spam outbursts.

Each of the layers are vulnerable to direct and indirect attacks. The layers must be continuously monitored and adjusted so the ecosystem is protected, the attack surface is minimized and business runs as usual. Even if the security of one of the layers is compromised, it could destabilize and render the entire ecosystem insecure. Adhering to IT security hygiene could ensure the elimination/avoidance of weakness, which can result in solid foundational security for the organization.

IT ISP

An ISP identifies the rules and procedures for all individuals accessing and using an organization's IT assets and resources. The objectives of an ISP are preservation of the confidentiality, integrity and availability of systems and information used by an organization's members.

To successfully adopt an ISP, the policy should:

- Be simple to understand. Policies need to be stated in a way that the audience can understand, and they need to reflect and convey the reason the policies exist.
- Be enforceable, but flexible. Policies should be broad enough to be able to achieve common understanding across technologies.
- Be measurable in a consistent manner
- Minimize unintended consequences

An information security framework consists of a number of documents that clearly define the adopted policies, procedures and processes by which an organization abides. It effectively explains to all parties (i.e., internal, tangential, external) how information, systems and services are managed within the organization.

For an organization to demonstrate it is secure, it needs to have a solid ISP derived from a recommended framework as deemed fit with respect to the organization.

Some examples of popular ISP frameworks include:

- Payment Card Industry Data Security Standard (PCI DSS)—A set of requirements intended to ensure that all organizations that process, store or transmit credit card information maintain a secure environment
- ISO/International Electrotechnical Commission (IEC) ISO/IEC 27001—An international standard that describes best practice for implementing an information security management system (ISMS)
- Center for Internet Security (CIS) Critical Security Controls—This is a list of 20 actions designed to mitigate the threat of the majority of common cyberattacks. The controls were designed by a group of volunteer experts from a range of fields, including cyberanalysts, consultants, academics and auditors.
- US National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Security—This is a voluntary framework primarily intended for critical infrastructure organizations to manage and mitigate cybersecurity risk based on existing standards, guidelines and practices.

People, Processes and Technology

It is helpful to view IT security hygiene with respect to people, processes and technology (**figure 1**).

People

Security is incomplete without "u." Security is every employee's responsibility, regardless of whether said employee is full time or part time, a contractor or in a leadership position, IT or non-IT, or works on the shop floor or at corporate headquarters. Every employee of an enterprise must be disciplined in following their job responsibilities, thereby ensuring hygiene in their physical and virtual workplace environment. Untrained employees can be the weakest link in the chain.[2] All it takes is for one employee to inadvertently click on an attachment of a malicious email, allowing attackers to take advantage of the enterprise. Proper training,

Figure 1—People, Process and Technology Framework

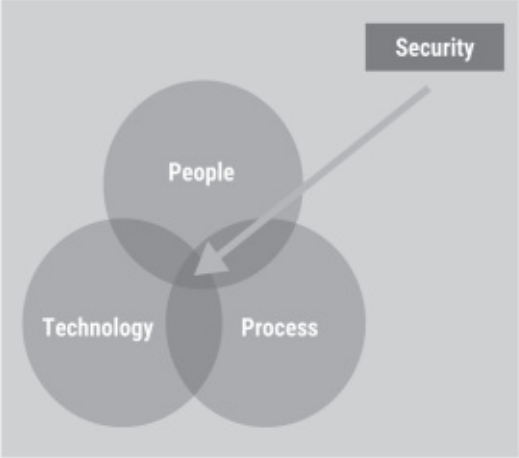
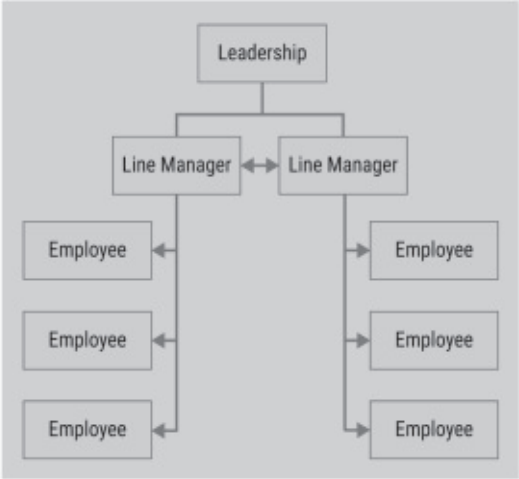


Figure 2—Organizational Structure



frequent communication and surprise evaluations can help employees to be vigilant. In short, it is the responsibility of each of the employees, which includes the leadership team, line managers and all other employees in the team structure of the organization (**figure 2**), to know of and abide by security policies mandated by the organization.

Managers

Middle managers are in positions to interface between employees and leadership. The manager is tasked with ensuring that employees develop the skills needed to maintain, sustain and propagate good hygiene. They play a crucial role in enforcing objectives and expectations and act as a bridge to help keep employees in alignment with management expectations. It is crucial to identify the most suitable person for these positions.

Because managers have a certain amount of authority in making day-to-day decisions, they have direct impact on the day-to-day functioning of enterprise operations. In short, managers are responsible for their teams adhering to the security mandates without any let up.

Leadership

C-suite personnel and leadership are directly responsible and accountable for the overall well-being of the organization and its employees. The phrase "tone at the top" refers to the leadership's take on a variety of things. For security, it is very crucial that any actions align with leadership objectives. If the leadership team is portraying confidence and support of IT actions, it will automatically mean the message resonates further into the ranks of employees and departments.

It is not enough to formulate a policy and approve it. It is how the policy is implemented and the value it delivers that determines the success of its intent.

For example, during an audit, there is a condition that is flagged as a major comment by the auditor. The product line manager then involves the leadership and other required stakeholders in this particular vertical to assess the impact, assess the time needed to fix the condition and ensure the sustenance of the controls implemented.

Management should encourage employees when employees alert them to issues and guide employees to use this experience so that issues are identified and can be addressed. This will motivate employees to be vigilant in looking for any opportunities to eliminate security concerns in the future.

Employees should be motivated to bring security issues to the attention of management. There should never be a situation where employees are afraid to do so, as it would be counterproductive.

The seriousness and importance of leadership to the discipline and hygiene of the organization is directly reflected in their buy-in and requires support from the

> "IT IS MUCH EASIER TO ENSURE PROPER SECURITY MEASURES THAT COMPLY WITH LEADERSHIP OBJECTIVES AND REGULATIONS IN THE FIRST PLACE RATHER THAN TRYING TO FIX THINGS RETROACTIVELY."

employees. For any major security gaps, an organization's culture is reflected in the presence of leadership in the related discussions. It is much easier to ensure proper security measures that comply with leadership objectives and regulations in the first place rather than trying to fix things retroactively.

At the end of the day, if there are any issues, concerns or violation of processes, leadership stakeholders are directly accountable. In some situations, they could be legally liable and punished by court of law. Take, for example, the accounting scandal of US energy, commodities and services enterprise Enron Corporation and the dissolution of Arthur Andersen LLP, which had been one of the largest auditing and accounting enterprises in the world in 2000. Enron's estimated losses totaled around US$74 billion and the chief executive officer of Enron was convicted of federal felony charges and sentenced to prison.[3]

It may be a struggle for non-IT professionals in an enterprise to understand IT terminology, risk and complexities. At a security summit, there was a skit about delivery at market speed. There was a product built for public use that needed to be deployed in a couple of hours. However, the required security evaluations were not conducted, as the security team was separate and was only to be involved once development teams engaged it to verify security. In this scenario, the enterprise wanted to release the product for consumer use, but the security team was against it and was asking for time to evaluate the security of the product. The security team asked enterprise leadership to fill out a form to understand the risk and sign the document as part of "risk acceptance." For enterprises, this risk acceptance may seem simple, as it removes the obstructions to rolling out the product, but many times the document is signed without understanding the depth of the risk and its implications. The skit then demonstrated a better solution, which is to have a security consultant involved from the initiation of the project and review/rectify at an early stage to ensure that there is no separate lead time for security checks. The non-IT team should be able to ask questions to satisfy the risk conditions or take the escalation route. This is also an opportunity for organizations operating in silos to see and align business strategy and security, which creates a more lean, agile environment and ensures that hygiene is sustained.

Technology

Technology refers to software and hardware. It is important to understand how to ensure that installed software is the correct version and legally sound (i.e., obtained through proper purchasing processes) and to know how secure an organization's systems are (i.e., having the proper amount of security tools, ensuring that the servers are onboarded with proper configuration and versions, properly renewing security certificates).

Patches and upgrades are extremely important steps that are often not paid due attention.

For example, in a well-known data breach, the issue was that the organization did not complete patching on time. The need for patching and what to patch was identified, and recommendations were provided to the required teams. However, the final actions of initiating and completing the patches and audit verification did not happen. Vulnerability scans, which are supposed to uncover these issues, failed to do so. The process of monitoring and ensuring patching completion did not work as intended. These errors are due to a lack of discipline.

Processes

Every security policy should have required processes that align with respective timelines. For example, a policy around change management would say: "Each of the changes has to be adequately tested and test results verified and signed-off on before releasing to production." This could well be ensured by documenting change management processes and following those processes in a disciplined manner.

Disaster Recovery
Another example of process documentation in alignment with security policy would be availability. Technology disaster recovery processes should be in place, reviewed to ensure up-to-date information, and tested adequately and frequently to ensure that the purpose is served. The purpose is the ability of the technology or application(s) to be recovered and return to normal operations (RTNO) within the agreed-upon time and based on the classification. Depending on the availability requirement from the organization, these applications should be architected and hosted accordingly, including recovery sites. Where an availability requirement is very high with no expected downtime, the required architecture should be different. It may even have mirroring solutions and, if there are any issues with the primary environment, the control will seamlessly be transferred to the secondary environment. Business or end users would not even be aware of a transfer. At end of the day, based on business needs and availability requirements, infrastructure must be provisioned. In short, the more the availability requirements, the more the cost involved in the setup.

> "EVERY SECURITY POLICY SHOULD HAVE REQUIRED PROCESSES THAT ALIGN WITH RESPECTIVE TIMELINES."

There have been several IT outages, particularly in the airline industry, that have lasted more than one week, causing massive disruption to travel, inconvenience to passengers and financial loss. Because the impact of these events is critical, processes must be in place to bring the system/technology back to operational within a stipulated time. If the processes had been tested adequately and frequently, the systems would have returned to normal operations within a specified time. This is a discipline issue impacting security hygiene.

Business Continuity Outcomes Due to COVID-19
The COVID-19 pandemic has led many businesses to move toward nearly 100 percent remote work and connectivity. Until now, work from home for many enterprises was a dreaded concept because it increases opportunities for security risk for employees and stakeholders when they connect to the organization's network through their personal laptops or desktops. However, in many cases, there is no other option. In fact, the pandemic has led to people looking at new ways of operating organizations more effectively. For example, many organizations find that having employees work remotely cuts down facility and maintenance cost and are, therefore, shifting to this model for more and more employees.

Conclusion

IT security is everyone's responsibility, whether employees are part of an IT team or a business team. Strongly sticking to the basic hygiene in IT and IT security as identified by the organization is of foundational importance. Untrained employees are the weakest link in the chain. Employees across the organization should be trained periodically on key elements of security, such as how to keep up with security hygiene, either as part of onboarding or via refresher courses. Necessary audits should be conducted on a periodic basis to assess the knowledge level of employees and successful implementation of security practices. It is very important to have the right people in the right places who are willing to go above and beyond and are disciplined to ensure that security hygiene is developed and sustained in the workplace. Input from leadership is extremely important. It should resonate in each and every aspect of communication so employees throughout the organization understand and are able to deliver on the expectations of IT and IT security team hygiene practices to keep the organization secure.

Endnotes

1 International Organization for Standardization (ISO), 35.100 Open Systems Interconnection (OSI), *https://www.iso.org/ics/35.100/x/*
2 Kress, B.; "Why Humans Are Still Security's Weakest Link," Accenture, 8 May 2019, *https://www.accenture.com/us-en/blogs/blogs-why-humans-still-securitys-weakest-link*
3 Corporate Finance Institute, "Enron Scandal," *https://corporatefinanceinstitute.com/resources/knowledge/other/enron-scandal/*

FEATURE

Risk Assessment and Analysis Methods: Qualitative and Quantitative

A risk assessment determines the likelihood, consequences and tolerances of possible incidents. "Risk assessment is an inherent part of a broader risk management strategy to introduce control measures to eliminate or reduce any potential risk-related consequences."[1] The main purpose of risk assessment is to avoid negative consequences related to risk or to evaluate possible opportunities.

It is the combined effort of:

- "...[I]dentifying and analyzing possible future events that could adversely affect individuals, assets, processes and/or the environment (i.e., risk analysis)"
- "...[M]aking judgments about managing and tolerating risk on the basis of a risk analysis while considering influencing factors (i.e., risk evaluation)"[2]

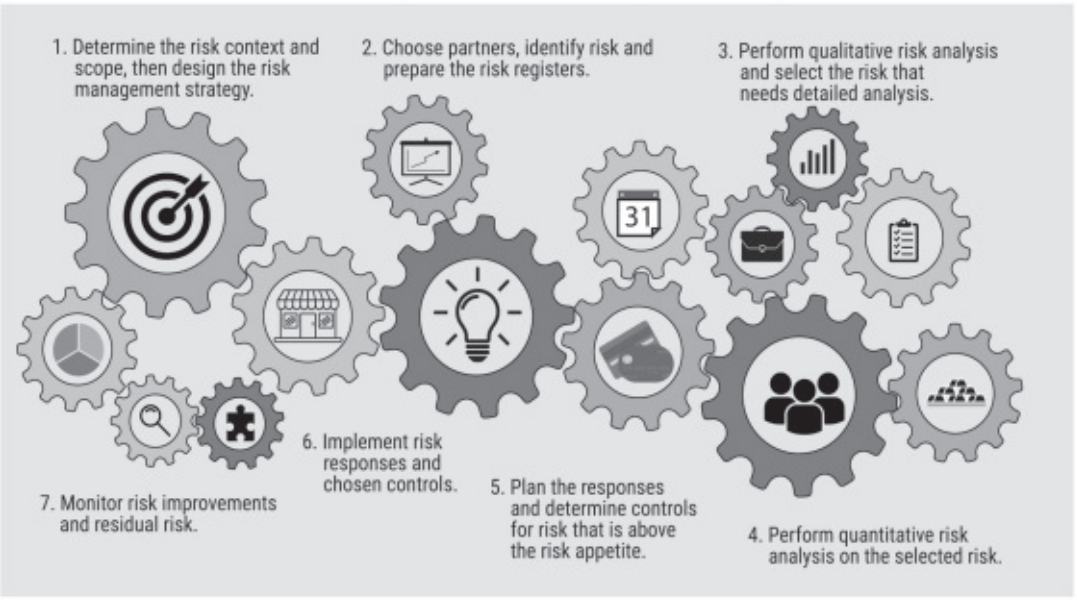
Relationships between assets, processes, threats, vulnerabilities and other factors are analyzed in the risk assessment approach. There are many methods available, but quantitative and qualitative analysis are the most widely known and used classifications. In general, the methodology chosen at the beginning of the decision-making process should be able to produce a quantitative explanation about the impact of the risk and security issues along with the identification of risk and formation of a risk register. There should also be qualitative statements that explain the importance and suitability of controls and security measures to minimize these risk areas.[3]

In general, the risk management life cycle includes seven main processes that support and complement each other (**figure 1**):

1. Determine the risk context and scope, then design the risk management strategy.
2. Choose the responsible and related partners, identify the risk and prepare the risk registers.
3. Perform qualitative risk analysis and select the risk that needs detailed analysis.
4. Perform quantitative risk analysis on the selected risk.
5. Plan the responses and determine controls for the risk that falls outside the risk appetite.
6. Implement risk responses and chosen controls.
7. Monitor risk improvements and residual risk.

Volkan Evrin, CISA, CRISC, COBIT 2019 Foundation, CDPSE, CEHv9, ISO 27001-22301-20000 LA
Has more than 20 years of professional experience in information and technology (I&T) focus areas including information systems and security, governance, risk, privacy, compliance, and audit. He has held executive roles on the management of teams and the implementation of projects such as information systems, enterprise applications, free software, in-house software development, network architectures, vulnerability analysis and penetration testing, informatics law, Internet services, and web technologies. He is also a part-time instructor at Bilkent University in Turkey; an APMG Accredited Trainer for CISA, CRISC and COBIT 2019 Foundation; and a trainer for other I&T-related subjects. He can be reached at volkan@evrin.net.

Figure 1—The Risk Management Life Cycle



Qualitative and Quantitative Risk Analysis Techniques

Different techniques can be used to evaluate and prioritize risk. Depending on how well the risk is known, and if it can be evaluated and prioritized in a timely manner, it may be possible to reduce the possible negative effects or increase the possible positive effects and take advantage of the opportunities.[4] "Quantitative risk analysis tries to assign objective numerical or measurable values" regardless of the components of the risk assessment and to the assessment of potential loss. Conversely, "a qualitative risk analysis is scenario-based."[5]

Qualitative Risk

The purpose of qualitative risk analysis is to identify the risk that needs detail analysis and the necessary controls and actions based on the risk's effect and impact on objectives.[6] In qualitative risk analysis, two simple methods are well known and easily applied to risk:[7]

1. Keep It Super Simple (KISS)—This method can be used on narrow-framed or small projects where unnecessary complexity should be avoided and the assessment can be made easily by teams that lack maturity in assessing risk. This one-dimensional technique involves rating risk on a basic scale, such as very high/high/medium/low/very low.
2. Probability/Impact—This method can be used on larger, more complex issues with multilateral teams that have experience with risk assessments. This two-dimensional technique is used to rate probability and impact. Probability is the likelihood that a risk will occur. The impact is the consequence or effect of the risk, normally associated with impact to schedule, cost, scope and quality. Rate probability and impact using a scale such as 1 to 10 or 1 to 5, where the risk score equals the probability multiplied by the impact.

Qualitative risk analysis can generally be performed on all business risk. The qualitative approach is used to quickly identify risk areas related to normal business functions. The evaluation can assess whether peoples' concerns about their jobs are related to these risk areas. Then, the quantitative approach assists on relevant risk scenarios, to offer more detailed information for decision-making.[8] Before making critical decisions or completing complex tasks, quantitative risk analysis provides more objective information and accurate data than qualitative analysis. Although quantitative analysis is more objective, it should be noted that there is still an estimate or inference. Wise risk managers consider other factors in the decision-making process.[9]

Although a qualitative risk analysis is the first choice in terms of ease of application, a quantitative risk analysis may be necessary. After qualitative analysis, quantitative analysis can also be applied. However, if qualitative analysis results are sufficient, there is no need to do a quantitative analysis of each risk.

Quantitative Risk

A quantitative risk analysis is another analysis of high-priority and/or high-impact risk, where a numerical or quantitative rating is given to develop a probabilistic assessment of business-related issues. In addition, quantitative risk analysis for all projects or issues/processes operated with a project management approach has a more limited use, depending on the type of project, project risk and the availability of data to be used for quantitative analysis.[10]

The purpose of a quantitative risk analysis is to translate the probability and impact of a risk into a measurable quantity.[11] A quantitative analysis:[12]

- "Quantifies the possible outcomes for the business issues and assesses the probability of achieving specific business objectives"
- "Provides a quantitative approach to making decisions when there is uncertainty"
- "Creates realistic and achievable cost, schedule or scope targets"

Consider using quantitative risk analysis for:[13]

- "Business situations that require schedule and budget control planning"
- "Large, complex issues/projects that require go/no go decisions"
- "Business processes or issues where upper management wants more detail about the probability of completing on schedule and within budget"

The advantages of using quantitative risk analysis include:[14]

- Objectivity in the assessment
- Powerful selling tool to management
- Direct projection of cost/benefit
- Flexibility to meet the needs of specific situations
- Flexibility to fit the needs of specific industries
- Much less prone to arouse disagreements during management review
- Analysis is often derived from some irrefutable facts

> "THE MOST COMMON PROBLEM IN QUANTITATIVE ASSESSMENT IS THAT THERE IS NOT ENOUGH DATA TO BE ANALYZED."

To conduct a quantitative risk analysis on a business process or project, high-quality data, a definite business plan, a well-developed project model and a prioritized list of business/project risk are necessary. Quantitative risk assessment is based on realistic and measurable data to calculate the impact values that the risk will create with the probability of occurrence. This assessment focuses on mathematical and statistical bases and can "express the risk values in monetary terms, which makes its results useful outside the context of the assessment (loss of money is understandable for any business unit)."[15] The most common problem in quantitative assessment is that there is not enough data to be analyzed. There also can be challenges in revealing the subject of the evaluation with numerical values or the number of relevant variables is too high. This makes risk analysis technically difficult.

There are several tools and techniques that can be used in quantitative risk analysis. Those tools and techniques include:[16]

- Heuristic methods—Experience-based or expert-based techniques to estimate contingency
- Three-point estimate—A technique that uses the optimistic, most likely and pessimistic values to determine the best estimate
- Decision tree analysis—A diagram that shows the implications of choosing various alternatives

Enjoying this article?

- Read *Risk IT Framework, 2nd Edition. www.isaca.org/risk-it-f2*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

- Expected monetary value (EMV)—A method used to establish the contingency reserves for a project or business process budget and schedule
- Monte Carlo analysis—A technique that uses optimistic, most likely and pessimistic estimates to determine the business cost and project completion dates
- Sensitivity analysis—A technique used to determine the risk that has the greatest impact on a project or business process
- Fault tree analysis (FTA) and failure modes and effects analysis (FMEA)—The analysis of a structured diagram that identifies elements that can cause system failure

There are also some basic (target, estimated or calculated) values used in quantitative risk assessment. Single loss expectancy (SLE) represents the money or value expected to be lost if the incident occurs one time, and an annual rate of occurrence (ARO) is how many times in a one-year interval the incident is expected to occur. The annual loss expectancy (ALE) can be used to justify the cost of applying countermeasures to protect an asset or a process. That money/value is expected to be lost in one year considering SLE and ARO. This value can be calculated by multiplying the SLE with the ARO.[17] For quantitative risk assessment, this is the risk value.[18]

> "USING BOTH APPROACHES CAN IMPROVE PROCESS EFFICIENCY AND HELP ACHIEVE DESIRED SECURITY LEVELS."

By relying on factual and measurable data, the main benefits of quantitative risk assessment are the presentation of very precise results about risk value and the maximum investment that would make risk treatment worthwhile and profitable for the organization. For quantitative cost-benefit analysis, ALE is a calculation that helps an organization to determine the expected monetary loss for an asset or investment due to the related risk over a single year.

For example, calculating the ALE for a virtualization system investment includes the following:

- Virtualization system hardware value: US$1 million (SLE for HW)
- Virtualization system management software value: US$250,000 (SLE for SW)
- Vendor statistics inform that a system catastrophic failure (due to software or hardware) occurs one time every 10 years (ARO = 1/10 = 0.1)
- ALE for HW = 1M * 0.1 = US$100,000
- ALE for SW = 250K * 0.1 = US$25,000

In this case, the organization has an annual risk of suffering a loss of US$100,000 for hardware or US$25,000 for software individually in the event of the loss of its virtualization system. Any implemented control (e.g., backup, disaster recovery, fault tolerance system) that costs less than these values would be profitable.

Some risk assessment requires complicated parameters. More examples can be derived according to the following "step-by-step breakdown of the quantitative risk analysis":[19]

1. Conduct a risk assessment and vulnerability study to determine the risk factors.
2. Determine the exposure factor (EF), which is the percentage of asset loss caused by the identified threat.
3. Based on the risk factors determined in the value of tangible or intangible assets under risk, determine the SLE, which equals the asset value multiplied by the exposure factor.
4. Evaluate the historical background and business culture of the institution in terms of reporting security incidents and losses (adjustment factor).
5. Estimate the ARO for each risk factor.
6. Determine the countermeasures required to overcome each risk factor.
7. Add a ranking number from one to 10 for quantifying severity (with 10 being the most

severe) as a size correction factor for the risk estimate obtained from company risk profile.

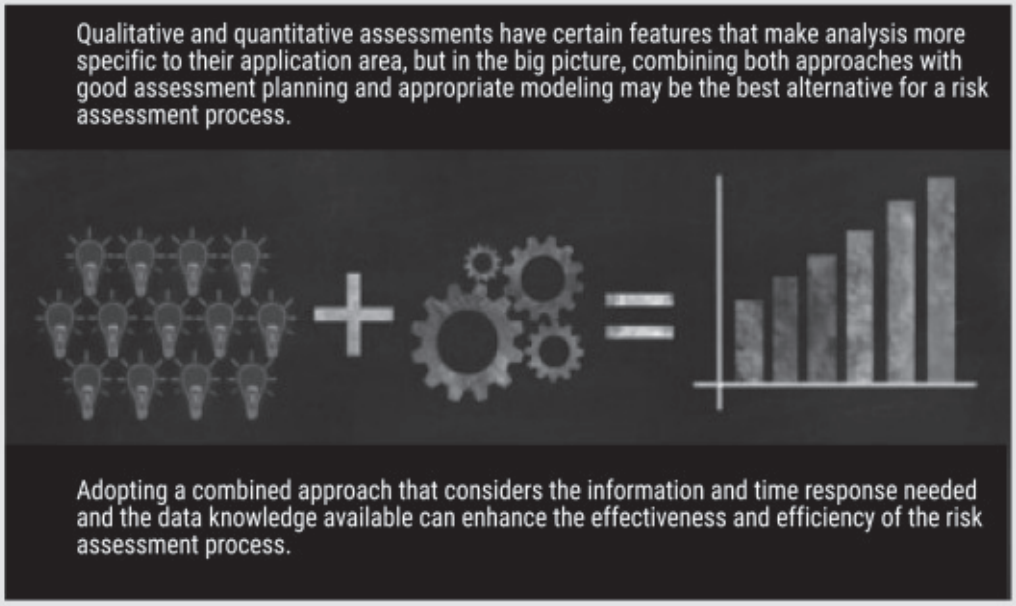
8. Determine the ALE for each risk factor. Note that the ARO for the ALE after countermeasure implementation may not always be equal to zero. ALE (corrected) equals ALE (table) times adjustment factor times size correction.
9. Calculate an appropriate cost/benefit analysis by finding the differences before and after the implementation of countermeasures for ALE.
10. Determine the return on investment (ROI) based on the cost/benefit analysis using internal rate of return (IRR).
11. Present a summary of the results to management for review.

Using both approaches can improve process efficiency and help achieve desired security levels. In the risk assessment process, it is relatively easy to determine whether to use a quantitative or a qualitative approach. Qualitative risk assessment is quick to implement due to the lack of mathematical dependence and measurements and can be performed easily. Organizations also benefit from the employees who are experienced in asset/processes; however, they may also bring biases in determining probability and impact. Overall, combining qualitative and quantitative approaches with good assessment planning and appropriate modeling may be the best alternative for a risk assessment process (**figure 2**).[20]

Conclusion

Qualitative risk analysis is quick but subjective. On the other hand, quantitative risk analysis is optional and objective and has more detail, contingency reserves and go/no-go decisions, but it takes more time and is more complex. Quantitative data are difficult to collect, and quality data are prohibitively expensive. Although the effect of mathematical operations on quantitative data are reliable, the accuracy of the data is not guaranteed as a result of being numerical only. Data that are difficult to collect or whose accuracy is suspect can lead to inaccurate results in terms of value. In that case,

Figure 2—A Combination Approach to Risk Assessment



business units cannot provide successful protection or may make false-risk treatment decisions and waste resources without specifying actions to reduce or eliminate risk. In the qualitative approach, subjectivity is considered part of the process and can provide more flexibility in interpretation than an assessment based on quantitative data.[21]

For a quick and easy risk assessment, qualitative assessment is what 99 percent of organizations use. However, for critical security issues, it makes sense to invest time and money into quantitative risk assessment.[22] By adopting a combined approach, considering the information and time response needed, with data and knowledge available, it is possible to enhance the effectiveness and efficiency of the risk assessment process and conform to the organization's requirements.

Endnotes

ISACA®, *CRISC Review Manual, 6th Edition*, USA, 2015, *https://www.isaca.org/bookstore/crisc-exam-resources/crr6ed*
Ibid.
Schmittling, R.; A. Munns; "Performing a Security Risk Assessment," *ISACA® Journal*, vol. 1, 2010, *https://www.isaca.org/archives*
Bansal, S.; "Differentiating Quantitative Risk and Qualitative Risk Analysis," iZenBridge, 12 February 2019, *https://www.izenbridge.com/blog/differentiating-quantitative-risk-analysis-and-qualitative-risk-analysis/*
Tan, D.; *Quantitative Risk Analysis Step-By-Step*, SANS Institute Information Security Reading Room, December 2020, *https://www.sans.org/reading-room/whitepapers/auditing/quantitative-risk-analysis-step-by-step-849*
Op cit Bansal
Hall, H.; "Evaluating Risks Using Qualitative Risk Analysis," Project Risk Coach, *https://projectriskcoach.com/evaluating-risks-using-qualitative-risk-analysis/*
Leal, R.; "Qualitative vs. Quantitative Risk Assessments in Information Security: Differences and Similarities," 27001 Academy, 6 March 2017, *https://advisera.com/27001academy/blog/2017/03/06/qualitative-vs-quantitative-risk-assessments-in-information-security/*
Op cit Hall
Goodrich, B.; "Qualitative Risk Analysis vs. Quantitative Risk Analysis," PM Learning Solutions, *https://www.pmlearningsolutions.com/blog/qualitative-risk-analysis-vs-quantitative-risk-analysis-pmp-concept-1*
Meyer, W. G.; "Quantifying Risk: Measuring the Invisible," PMI Global Congress 2015—EMEA, London, England, 10 October 2015, *https://www.pmi.org/learning/library/quantitative-risk-assessment-methods-9929*
Op cit Goodrich
Op cit Hall
Op cit Tan
Op cit Leal
Op cit Hall
Tierney, M.; "Quantitative Risk Analysis: Annual Loss Expectancy," Netwrix Blog, 24 July 2020, *https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative-risk-analysis/*
Op cit Leal
Op cit Tan
Op cit Leal
ISACA®, *Conducting an IT Security Risk Assessment*, USA, 2020, *https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpcit*
Op cit Leal

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 ☐ 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# _____

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 ☐ 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	$ 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.

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

Book Post

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