Welcome...

February, 2016

INSIDE THIS ISSUE

Greetings Fellow Greater Cincinnati ISACA Members,

The 2016 ISACA membership renewal period is in progress. The Greater Cincinnati ISACA Chapter Board has set a goal of achieving an 88% renewal rate by 3/31/2016. To show the Chapter Board's appreciation to all Chapter members, I am pleased to announce that the Chapter will offer a free dinner meeting with 1 CPE to members for our September 2016 meeting. In addition, if the Chapter meets the renewal goal, members will be eligible for receiving special prizes ISACA International's Membership Page during the September meeting. We encourage you to visit ISACA International's Membership Page to renew today! Don't risk losing your membership benefits due to the accelerated purge date. We value you expertise and hope you will take time to renew your 2016 ISACA® membership.

Our annual general meeting will be held May 3, 2016. At that meeting we will be electing officers for the next two-year term. We will also be asking for approval of our amended bylaws. The bylaws and the slate of officers will be sent to all members before the end of March.

Damon Hacker provided an informative and entertaining discussion of the use of digital evidence and how to use digital forensics for an investigation.

Our March meeting will be held March 1, 2016 at the Montgomery Inn. Our speaker, Shannon Glass will be discussing How to Build a Cyber Security Approach When You're starting at Ground Zero

CPEs for Greater Cincinnati ISACA training events are uploaded to ISACA International. Members need to logon to the ISACA web site and apply the CPEs to their certifications. These CPEs are not subject to audit, if you get selected for an audit of your training.

I encourage you to join our LinkedIn group if you are not a member. I post training opportunities in the group that I learn about from other ISACA chapters. This will give you additional options for earning CPEs. We also have a Facebook page. If you know anyone in the audit or security profession who might benefit from ISACA membership, please invite them to one of our meetings or put them in touch with our board so they can find out more!

Do you have any coworkers that are not receiving this newsletter and would like to? If so, have them send an e-mail to our Newsletter Editor, Kyle Schutte and request to be included on the e-mail distribution list. If you are interested in becoming a member of the chapter, please contact our VP of Membership, Mike Smith. As a reminder, our website is the best place to learn about upcoming events and available job opportunities in the Greater Cincinnati ISACA area! Check it out at: www.isaca-cincinnati.org! As always, I am happy to hear any comments you have, so feel free to e-mail me at rkrickisaca@gmail.com.

Russell Krick, CISA,

Greater Cincinnati ISACA President

Monthly Meeting

Digital Evidence and How Digital Forensics is Used

Date: March 1, 2016
Location: Montgomery Inn, Montgomery
Time: Networking 5:30; Presentation 6pm; Dinner 7pm.

Topic: How to Build a Cyber Security Approach When You're starting at Ground Zero

Speaker: Shannon Glass

Topics:

- Understanding Cybercrime and How to Protect Yourself
- Privacy and Data Security
- Scams and Fraud
- Network Security
- Website Security
- Email
- Mobile Devices
- Employees
- Facility Security
- Operational Security
- Payment Cards
- Incident Response and Reporting
- Policy Development Management

Speaker:
As the information security and compliance practice director at AfidenceIT, Shannon Glass is an accomplished leader in building and managing high-performance teams in information security, governance, and regulatory compliance. She provides transformational leadership consulting for IT operational outsourcing initiatives. Skilled in helping clients develop and articulate organizational vision and strategy across their enterprise, Shannon is responsible for engaging, overseeing the delivering exceptional quality to her clients. She has years of experience in risk-based security assessments, vulnerability scanning, penetration testing, security awareness training, security programs, and regulatory compliance standards such as PCI, ISO 27000 and NIST based frameworks that meet the needs of individual customers. Shannon's experience spans many industries, but she is considered a subject matter expert in the financial services and healthcare industries.

Members and non-members should register by using this link .
For those who prefer to pay at the door, please select that option when you register at the link above.

ISACA 2016 Certification Exam Review Courses

Are you planning on taking an ISACA certification exam in the future? If you answered yes, did you know that ISACA offers CISA, CISM, CGEIT, CSX and CRISC Exam Review Courses? These review courses are one of the many ways to prepare for the ISACA's exams. There is also a CISA review course offered online.

Go to this page to find out more details or find a review course near you.

Upcoming Webinars

ISACA Members can earn free CPEs by attending a 60 minute ISACA webinar. Increasing your knowledge of important and relevant IT and IS topics is just a bonus.

Here are the upcoming Webinars:

Topic: **PCI DSS: Developing Robust Trojan Defenses**

Presenter: **Jim Seaman,** *Security Consultants Team Lead,* Nettitude Group

Date: Thursday, 31 March 2016

Time: 12PM (EST) / 11AM (CST) / 9:00AM (PST) / 17:00 (UTC)

Overview: Legend has it that in 1200 B.C., King Agamemnon of Mycenae, led a coalition of Greek forces to lay siege against the City of Troy. The goal was to reclaim Menelaus's wife, Helen (a queen from Sparta), who had been abducted by the Trojan Prince Paris. Troy was subjected to 10 years of hostile activities from a determined enemy, applying numerous different methods to identify and exploit any vulnerability in the city's defenses. However, despite the best efforts of the attacking Greek forces, an array of physical defenses stood up to these actions. The barrage of attacks lasted for over 10 years, without success, and even led to the death of Achilles. This was until they exploited the failings of the human factor, where the Greeks delivered an attractive gift, containing an unknown and dangerous payload.

The secret to the success of the City of Troy's defensive measures was not created overnight; in fact, it was the result of nine layers of development spanning over five layers of improving architecture and 1,300 years (2,500 B.C. – 1,200 B.C.). The result was a comprehensive suite of Defense in Depth (DiD) security countermeasures, including:

- Strategic placement of access/egress gates
- Strict restriction of inbound and outbound traffic flows
- Secure residence for Helen of Troy
- Escorted convoys
- Entry/exit searches
- Vulnerability assessments
- Robust access controls
- Authentication
- Segmentation
- Internal patrols
- External patrols
- Perimeter defenses

Click on this link to find out more details or to register

You can register ahead of time for up to two new webinars each month; presented live by subject matter experts and accessible to you free of charge. Enjoy interaction with the presenter in the live format or view the entire webinar after the event on your schedule. These brief, yet extremely informative, web-based, education sessions are available in ISACA archives for up to a year after the event.

Upcoming Webinars

ISACA Members can earn free CPEs by attending a 60 minute ISACA webinar. Increasing your knowledge of important and relevant IT and IS topics is just a bonus.

Here are the upcoming Webinars:

Topic: Understanding How Machine Learning Defends Against 0-Day Threats

Speaker: **Vinoo Thomas,** *Senior Product Manager,* Intel Security

Date: **Thursday**, 10 March 2016

Time: 12PM (EST) / 11AM (CST) / 9AM (PST) / 17:00 (UTC)

Overview:

Bypassing antivirus software has been an arms race that's been played out for over three decades with security vendors always trying to stay ahead of the bad guys. From monthly .DAT file updates shipped on floppy disks by snail mail to customers, to today's cloud-based reputation systems – the Anti-Malware industry has come a long way in responding to new threats quickly. However, for authoring generic or heuristic signatures, many Anti-Malware vendors still require a copy of the actual file to analyze, replicate and reverse engineer threats in order to author signatures.
In this session we will cover machine learning as a solution for detecting 0-day threats. In particular, we will look at how:

• machine learning can be used to overcome gaps left by traditional approaches

• signature-less, cloud-based detection technologies leverage automated static and behavior-based classification to protect against zero-day malware

• how to best leverage this approach in your environment.

Click on this link to find out more details or to register

You can register ahead of time for up to two new webinars each month; presented live by subject matter experts and accessible to you free of charge. Enjoy interaction with the presenter in the live format or view the entire webinar after the event on your schedule. These brief, yet extremely informative, web-based, education sessions are available in ISACA archives for up to a year after the event.

Job Opportunities

Company: Clark Schaefer Consulting
Position: IT Audit Consultant
Location: Cincinnati and Columbus, OH

About the Company :

Clark Schaefer Consulting is an established professional services firm associated with Clark, Schaefer, Hackett CPAs, one of the top public accounting firms in the region. As a firm, we have been performing consulting services within the Cincinnati business community and surrounding area for 10 plus years and prior to that time, as part of our CPA firm affiliate for 75 years. Due to increased demand from our clients and the outlook for our services in2016, we are currently seeking information systems professionals as consultants for full-time, salaried positions at our Cincinnati and Columbus locations.

By design, we serve a diverse set of regional clients ranging from the Fortune 1000 to privately held corporations. As a regionally based firm, we believe we offer an ideal work-life balance for those who enjoy client service work, but want to avoid the extensive travel and time requirements of the national firms. If you are interested in having
diversity in your work experience; expanding your personal knowledge base; and being part of assisting the top companies in your community as they improve their operations, this is a great opportunity for you.

Job Description:

Based upon skills and experience, the successful candidates will join a team of professionals performing a range of IT audit, internal audit, and other related information system services. These services could include IT audits, process improvement, policy/procedure development, disaster recovery reviews, network architecture assessments, IT risk assessments, application control reviews, systems implementation assistance, and a wide variety of other technology related services. For more details on specific potential projects, please visit our website for a listing of the services we typically perform which might fit your background and skills.

Primary Responsibilities:

• Provide IT auditing and other technology related services to fulfill individual engagement requirements.
• Assist with the development of project plans, methodologies and client proposals as needed.
• Maintain a consistent level of chargeable hours to fulfill annual billable expectations.
• Travel to client locations as required throughout the year.
• Maintain a commitment to continuing education and professional development.

Education & Experience:

• Bachelor's degree in technology or related field.
• Relevant IT audit or information technology experience.
• Professional certifications such as CISA, CISM, CIA, CISSP are a plus.
• Excellent written and verbal communication skills.
• Ideal candidate would have 1-4 years of experience.

To Apply:

Please e-mail your resume, cover letter and salary history to recruiting@clarkschaefer.com . For more information concerning our Firm and services, please visit www.clarkschaefer.com.

Company: Cincinnati Insurance Company
Position: IT Governance Risk & Compliance Service Manager
Location: Fairfield, OH

About the Company :

The Cincinnati Insurance Company, a subsidiary of Cincinnati Financial Corporation, stands among the nation's top 25 property casualty insurer groups, based on net written premiums. Our commitment to the independent agency system began in 1950 and is our company's core strength and competitive advantage. We excel by offering agents and policyholders a local presence, unparalleled claims service, loss control consultation services, work-saving technology initiatives, and competitive products, rates and compensation. Selected associates receive a comprehensive salary and benefits package, including a matching 401(k). Equal Opportunity Employer.

Job Description:

We are currently seeking an IT GRC Service Manager to lead our Information Technology Governance, Risk and Compliance service area. This includes oversight and evaluation of the management controls within our IT Department to determine whether our systems are safeguarding assets, maintaining data integrity and operating effectively to achieve the organization's goals and objectives.

Specific Responsibilities:

- lead the IT GRC Service area by developing, creating and maintaining procedures, processes, and standards for the service area and IT, including the IT GRC audit plan, IT GRC business continuity plan and team's internal system access
- define team objectives, set goals and track progress to ensure objectives are met
- inform director of status in a timely and accurate fashion
- coordinate service area workload by managing the work intake process by prioritizing and assigning tasks to associates.
- conduct detailed reviews of IT auditor projects and facilitate appropriate documentation; leverage director guidance as needed
- partner with Resource Manager(s) to continually evaluate service area team members and provide real-time, constructive feedback
- provide oversight and leadership in the planning, design and execution of general IT control audit programs including operational process reviews, reviews of records retention policies, vendor management, change management, system implementations, applications, databases, IT infrastructure and other IT related risk areas
- function as the IT GRC subject matter expert in support of IT and operational audits and regulatory audits such as HIPAA, PCI and SOX
- independently manage the audit of departmental or specific service area systems
- review audit documentation to determine information technology system risks and the potential impact of risks on the organization
- perform root cause analysis on exceptions identified during audits including the composition of memos to address the remediation efforts
- communicate with and educate other service area directors, service managers and process owners on the importance of controls, an effective control environment and the role of IT GRC
- track status and results of current and prior audits, identify audit themes across departments, propose practical solutions and determine whether appropriate corrective actions have been designed and implemented to address IT audit concerns
- participate on varied teams or committees as an IT GRC representative

… Continued from page 5

Specific Responsibilities (Continued)

- work effectively with associates at all levels in varying departments and service areas
- actively monitor the regulatory environment for new laws and regulations that impact technology; leverage findings to assist with ongoing maintenance of annual audit plan and to ensure compliance
- assist in the research of new technologies and provide recommendations based on benefits or impacts on current systems
- execute audits of programs and projects ensuring they are effectively and efficiently managed and in alignment with organizational objectives
- improve risk management of corporate priority projects by conducting and facilitating risk assessments
- lead by example and gain influence by demonstrating humility and respect for others

Job Requirements:

- excellent oral and written communication skills
- ability to work independently and within a team environment
- excellent time management and prioritization skills
- excellent negotiation and conflict management skills
- strong analytical skills
- detail oriented
- ability to adapt and quickly understand a new and complex environment
- comfortable in relationships with all levels of management and associates
- bachelor's degree required in related field of study (e.g., Management Information Systems, Information Technology, and Computer Science).
- professional certification required (i.e., CISA, CISSP, CIA, CISM, CPA, etc.).

Preferred:

- three or more years of "Big Four" technology audit experience, post Sarbanes Oxley
- demonstrated experience writing reports of control descriptions, internal control findings and recommendation
- demonstrated experience with internal controls, risk assessments, business process and internal IT control testing or operational auditing

To find out more or to apply for this position, contact :
Stephanie Kolodzjieski, Corporate Recruiter
Stephanie_Kolodziejski@cinfin.com
513.603.5380

Company: Fifth Third Bank
Position: IT Audit Staff or Senior
Location: Cincinnati, OH

About the Company :

Fifth Third Bancorp is a diversified financial services company headquartered in Cincinnati, Ohio. As of December 31, 2014, the Company had $139 billion in assets and operated 15 affiliates with 1,302 full-service Banking Centers, including 101 Bank Mart® locations, most open seven days a week, inside select grocery stores and 2,638 ATMs. Fifth Third operates four main businesses: Commercial Banking, Branch Banking, Consumer Lending, and Investment Advisors.

Job Description:

Conducts IT governance, infrastructure & support, integrated business process and application audits for various lines of business/functional areas within the Bancorp. Primary responsibilities include performing IT audit activities in the planning, fieldwork, reporting and wrap-up phases in accordance with established standards. Seniors will be responsible for supervision of assigned staff personnel (typically leads 1-2 staff per audit) and ensuring that the execution of all audit phases is conducted in accordance with established standards.

Specific Responsibilities:

- Ensure execution of all audit activities in the planning, testing, reporting and wrap-up phases are in compliance with the Audit Division's methodology /standards and within the timeframes to support department metrics
- Challenge, validate and execute test strategies to determine the effectiveness of internal controls and compliance with regulations; incorporating appropriate tools, techniques and technology.
- Establish, foster and maintain working relationships with peers and supervisory management within the business line and cross-functional lines to support an effective workflow, continuous communication and value to customer.
- Participate in departmental processes and initiatives that promote team effectiveness, employee engagement and resource development.
- Attend Bancorp sponsored and other training to build industry knowledge and technical capabilities.

<u>Additional Responsibilities for Senior Auditor:</u>

- Develop audit scope and objectives, risk and control assessments, work programs, and other deliverables of audit work.
- Delegate responsibilities to audit staff members, and review audit work papers providing coaching feedback on work prepared by staff auditors.
- Communicate information to management through presentations and internal audit reports.

Job Requirements:

- Bachelors degree required; Computer Science or Management Information Systems preferred. Other related academic majors (e.g., Accounting or Audit) should be accompanied by relevant experience in IT or IT Audit.
- Encouraged to pursue CISA certification and/or related professional certifications such as CISSP, CPA or CIA.
- IT or Financial services industry experience and/or public accounting firm experience desirable.
- Proficient with MS-Windows and other related PC applications. Possess the desire and ability to learn mainframe and distributed applications as well as automated data analysis tools and Techniques
- Strong written and verbal communication skills required.
- Senior candidates will demonstrate coaching, leadership and project management skills.

To find out more or to apply for this position, contact :
Reese Gable, Talent Acquisition Consultant
Reese.Gable@53.com
513-534-7527

Company: Hillenbrand, Inc.
Position: IT Internal Auditor III - 1500000131
Location: Batesville, IN

Job Description:
The IT Internal Auditor will work closely with the business unit management, finance and IT leadership, external audit firms and, as needed, co-sourcing firms. The IT Internal Auditor must be able to execute the assigned audit areas to timely and successful completion.

Essential Duties and Responsibilities include the following**:**
- Conduct more complex audit activities to analyze and evaluate the performance of the organization's financial, operational, managerial, and IT processes and systems to identify risks, areas for improvement, and to ensure that the organization complies with all relevant regulations, laws, and standards.
- Conduct routine and complex audit projects independently; plan, organize, and schedule own workload so that audit activities are completed accurately and on time.
- Collect, examine, analyze, and verify information about the organization's systems and processes by reviewing manuals, policies, reports, financial statements, and other written materials, and by interviewing organizational members where required.
- Develop recommendations for changes to processes and systems that will minimize risk, improve performance and productivity and ensure that the organization complies with all relevant regulations, laws, and standards.
- Prepare audit reports that accurately document the audit process and its findings.
- Partner with and build strong working relationships with business line management
- Participate in the risk assessment process;
- Mentor and train junior auditors and/or business line guest auditors;
- Participate in development of internal audit policy and procedure documentation;
- Other duties may be assigned.

Supervisory Responsibilities
This position does not have any direct supervisory responsibilities.

Education
Bachelor's degree (B.A./B.S.) or equivalent from a college or university in Accounting, Finance, IT or MIS; and a minimum of 5 years IT audit and/or IT experience in a corporate environment, or with a Big 4 firm; or equivalent combination of education and experience with an emphasis in IT audit.

A professional security, audit, or control-related professional certification such as CISA, CIA, or CISSP is preferred.

Skills/Experience
- Basic Microsoft Office skills required
- Sarbanes Oxley compliance experience required
- Experience interacting with all levels of management required
- German or Chinese Mandarin language skills preferred
- Public accounting experience preferred
- Manufacturing industry experience preferred
- Basic experience in the assessment of internal controls and communicating findings and recommendations to others clearly and accurately in non-technical terms preferred

… Continued from page 8

Skills/Experience (Continued)

- Intermediate understanding of IT processes and technology, with demonstrated proficiency in one or more of these applications (JD Edwards, SAP, Hyperion) required
- Expert understanding of controls related to information security, program/project management, and/or infrastructure services (operating systems, databases, and network) required

Travel
Employee must be able to travel 20% of the time.

Physical Demands
To perform this job successfully, the physical demands listed are representative of those that must be met by an employee. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this job, the employee is regularly required to sit, stand, walk, use hands to handle and feel, reach with hands and arms, talk and hear. The employee may occasionally be required to crouch. The employee may occasionally lift items as heavy as 25lbs. Specific vision abilities may include the employee's ability to see near and far distances.

DISCLAIMER:
The above information on this job description has been designed to indicate the general nature and level of work performed by the employee within this classification. It is not designed to contain or be interpreted as a comprehensive inventory of all duties, responsibilities and qualifications required of any employee assigned to this job. Nothing in this job description restricts management's right to assign duties and responsibilities to this job at any time.

View all of our career opportunities at http://hillenbrandcareers.com

At Hillenbrand, we strive to build a diverse work force through equal opportunity employment that embraces and leverages the differences each individual has to offer.

To find out more or to apply for this position, contact:
Deanna Havron, Manager, Global Talent Acquisition & Development
deanna.havron@hillenbrand.com

M/F/D/V

Job Opportunities

Company: KPMG, LLP
Position: IT Audit Advisory Associate or Senior Associate
Location: Cincinnati, OH

About the Company :

Do you have a passion for solving complex business problems? KPMG's Advisory Services Practice focuses on fundamental business issues — managing risk, increasing revenues, controlling costs that organizations, across various industries, should address in order to help them flourish. We help companies to identify and manage risks inherent in business processes and technology systems that support business objectives, and provide them with the information needed to help them meet their strategic and financial goals. Services are specialized to help clients mitigate risks across an overall risk spectrum. We are currently seeking an IT Audit Advisory Associate/Senior Associate to join us in our Cincinnati Ohio office.

Job Description:

As an IT Attestation professional, you will work with clients whose business processes and use of technology have external stakeholders. Our team delivers independent third party assessments that can provide comfort to clients and their business partners through seals and distributable reports such as reports such as SysTrust and SSAE16.

Specific Responsibilities:

- Plan and execute the day-to-day activities of IT audit engagements for a variety of clients including system development, package implementation and/or platform reviews
- Evaluate the design and effectiveness of technology controls throughout the business cycle
- Identify and communicate IT audit findings to senior management and clients
- Help identify performance improvement opportunities for assigned clients

Additional Responsibilities for Senior Associate:

- Supervise Associates and Interns on engagements
- Supervise and provide performance management for IT audit staff working on assigned engagements
- Serve as a liaison between clients and upper management

Job Requirements:

- Qualifications for both positions:
  One year of experience in any of the following areas: internal or external IT audit, risk assessment, business process reengineering, Enterprise Resource Planning 'ERP" packages such as SAP Oracle Financials, Hyperion and Cognos, Customer Relationship Management (CRM) packages such as Siebel, IT security, project management, IT outsourcing or off shoring, and/or IT strategy
- Bachelor's degree in an appropriate field from an accredited college/university
- Exceptional interpersonal skills with ability to gain the confidence and respect of senior level executives
- Willingness and ability to travel

Additional Qualifications for Senior Associate:

- Three years of advisory services experience in any of the following areas: internal or external IT audit, risk assessment, business process reengineering, ERP packages such as SAP, Oracle Financials, Hyperion and Cognos, CRM packages such as Siebel, IT security, project management, IT outsourcing or off shoring, and/or IT strategy
- Project or team lead experience
- Strong leadership and communication skills, technical knowledge, and the ability to write at a publication quality level in order to communicate findings and recommendations to the client's senior management team

To find out more or to apply for this position, contact :

Brett Ballinger, Director, Risk Consulting

bballinger@kpmg.com

Company: Fifth Third Bank
Position: Senior IT Risk Analyst (one openings)
Location: Cincinnati, OH

About the Company :

Fifth Third Bancorp is a diversified financial services company headquartered in Cincinnati, Ohio. As of December 31, 2014, the Company had $139 billion in assets and operated 15 affiliates with 1,302 full-service Banking Centers, including 101 Bank Mart® locations, most open seven days a week, inside select grocery stores and 2,638 ATMs in Ohio, Kentucky, Indiana, Michigan, Illinois, Florida, Tennessee, West Virginia, Pennsylvania, Missouri, Georgia and North Carolina. Fifth Third operates four main businesses: Commercial Banking, Branch Banking, Consumer Lending, and Investment Advisors. Fifth Third also has a 22.8% interest in Vantiv Holding, LLC. Fifth Third is among the largest money managers in the Midwest and, as of December 31, 2014, had $308 billion in assets under care, of which it managed $27 billion for individuals, corporations and not-for-profit organizations. Investor information and press releases can be viewed at www.53.com. Fifth Third's common stock is traded on the NASDAQ® Global Select Market under the symbol "FITB."

Job Description:

This position is responsible for implementing information technology risk management strategies identified by the IT Risk Manager. In this role, the Senior IT Risk Analyst will be assigned overall responsibility for key areas and will have accountability for proper planning, prioritization and execution of supporting IT risk responsibilities. This position is responsible for hands-on execution of control/risk assessments and the development of control enhancement recommendations.

Specific Responsibilities:

- Support the IT Risk Manager in the execution of responsibilities to conduct risk assessments, implement self-assessment programs, perform technical research on risk topics, and other activities that support risk management goals for the IT Division. Some of the primary responsibilities include:
- Support the IT Risk Manager on the implementation of information technology risk management strategy and operating priorities.
- Support the integration of the IT Risk Management practices into key Information Technology and business areas.
- Build effective relationships with key individuals who own and support processes you are responsible for evaluating, including the appropriate line-of-business risk managers.
- Perform ongoing planning and prioritization of key projects and activities to ensure that resources are applied to the most critical areas. Communicate with the IT Risk Manager, as needed, to ensure proper prioritization and management of workload.
- Participate on projects and ensure that key IT risks are being adequately addressed. Coordinate with project managers to ensure that issues are identified, action plans are in place and that PLC requirements are being met.
- Perform risk assessments on key IT processes or assets, identify vulnerabilities and propose solutions to mitigate risk. Perform due diligence and risk assessments on IT service providers.
- Work with IT areas in developing an effective self-assessment process for proactively identifying risks associated with processes, applications and technical infrastructure components.
- Support compliance with applicable regulations, which include, but is not limited to the following: the FDIC Improvement Act, the Sarbanes-Oxley Act of 2002 and the Gramm-Leach-Bliley Act of 1999.
- Support the resolution of Internal Audit, regulatory, or Risk Management related issues that could impact the confidentially, availability or integrity of data or processes.
- Create effective risk assessment documentation supporting work performed, including formal communication on risk assessment results. Be able to deliver effective presentations to management on summary of work performed and findings.

…..Continued from page 10

Job Requirements:

Two to four years of information technology experience required. Desired experience should include a foundation in IT security and controls. While experience in a number of IT disciplines may provide a solid framework for this position, hands-on results from performing IT risk assessments, information security consulting or IT audits are most beneficial. At least one relevant technical or professional certification, such as CISA or CISSP, is required.

Bachelor's degree required, preferably in computer science or information systems. Must possess excellent written and verbal communication skills, with a proven track record of interacting effectively with end-users and technology professionals. Able to work on multiple projects concurrently, manage time effectively and require minimal supervision in the execution of IT Risk Analyst responsibilities. Must possess strong analytical capabilities and have a desire to learn new things. Less than 10% travel required.

To apply for this position, visit https://www.53.com/careers/index.html

Requisition #: 146609

To find out more, contact :

Justin Hedric, VP – Senior IT Risk Manager

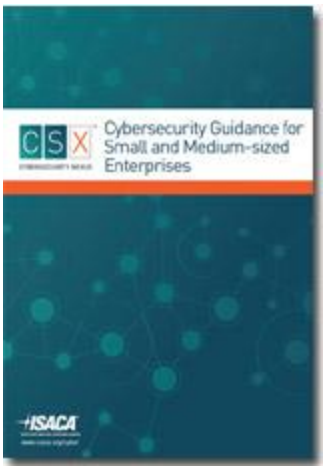
Justin.hedric@53.com

513.534.8648

Cybersecurity Guidance for Small and Medium-sized Enterprises

Cybersecurity is rapidly becoming a critical activity in many enterprises, due to the increasing number of cyberattacks and cybercrime. Cyberattacks often target small and medium-sized enterprises, because cybercriminals expect information in SMEs to be less protected than in large enterprises. Protection against cyberattacks is an important element in ensuring that SMEs can protect their economic interests, reputation and intellectual property, and the information assets of their customers and business partners.

This guidance for implementation publication provides practical advice on how to implement cybersecurity governance, risk management, assurance and compliance using the Cybersecurity Standard for SMEs and its COBIT 5 foundation. SMEs do not need to apply to the full extent the recommendations in this guidance for implementation publication. Examples and cases give SMEs insights into implementing the standard. However, the implementation guidance should not be read as prescriptive.



ISACA Members and Non-Members can purchase a hard copy or download the eBook at the following prices:

Members- Downloadable Book Format for US $35.00 each **here**

Non-members—Join ISACA today to get your $35.00 Book, or purchase the book for US $60.00 each.

How to Earn and Report CPE

Did you know that ISACA certified members can earn up to 72 FREE CPEs per year!

ISACA offers opportunities to earn CPE through participation in a variety of programs and events. Several of these choices are listed below with specific instructions.

Webinars and Virtual Conferences: Up to 36 free CPEs per year. CPE quizzes are for members only.

Journal quizzes: Earn one CPE for each of six journals per year. 6 FREE CPEs per year

Serving as an ISACA Volunteer: Participate on an ISACA or ITGI board, committee, task force or as an officer of an ISACA chapter, and gain one CPE credit (up to 20 per year) for each hour of active participation. (Consult Qualifying Educational Activities for CISA, CISM, CGEIT and CRISC members.) 20 FREE CPEs per year

Mentoring: Earn one CPE for each hour of mentoring efforts directly related to coaching, reviewing or assisting an individual with CISA/CISM/CGEIT/CRISC exam preparation or providing career guidance through the credentialing process. 10 FREE CPEs per year

TOTAL Possible FREE CPEs for ISACA Certified Members: 72 FREE CPEs per year

How to Report CPEs in your Profile

CPEs are reported annually during the renewal process. CPEs earned in the current year may be entered in your profile once the next year's renewal period opens. Reporting of CPEs can be done online or by submitting the information on the annual renewal invoice.

To update CPE hours through the ISACA website, log on using your personalized log in credentials and follow the steps below.

Click on the **MY ISACA** tab at the top of the page

Click on the **MY CERTIFICATIONS** tab

Click on the **EDIT MY CPE Hours** link

The CPE reporting is located on the My Demographic, Certification CPE and Other Information tab. Scroll to the bottom of the page to view and edit the appropriate CPE fields. If you do not see a CPE section, CPE hours are not being accepted or you are not required to report CPEs yet.

Enter CPE hours – then click SAVE at the bottom of the page

For more information about the specific Continuing Professional Education (CPE) requirements for your certification, please see the following link.

Editor's Corner

Dear Cincinnati ISACA member,

As we look to improve communication with all members and individuals who are interested in our Chapter, we appreciate any and all feedback to changes in regards to emails, newsletters and reminders.

Our goal as a Chapter is to continually provide useful information to our community. With this in mind, submissions for CPE, Job Opportunities, Events, etc. are always welcome.

Submissions, feedback and questions can all be directed to Kyle Schutte (kschutte@clarkschaefer.com).

Thank You!

Kyle Schutte, CISA
VP of Communications

About Our Chapter

Founded in 1973, the Greater Cincinnati ISACA Chapter is a not-for-profit professional organization serving IT Audit, Risk, Security, and Governance professionals in the Greater Cincinnati market. The chapter consists of over 450 professionals that represent a diverse mix of public, private, and not-for-profit business sectors at all levels within those industries. Members of the Greater Cincinnati ISACA Chapter have the opportunity to earn 36 CPE hours annually through various events and seminars. The greatest asset to the Greater Cincinnati ISACA Chapter is its membership community.

Purpose
To promote the education of individuals for the improvement and development of their capabilities relating to IT Audit, Security, Risk, and Governance in the field of Information Technology audit and control.

Please visit the chapter website at www.isaca-cincinnati.org to learn more.
Connect with other chapter members by joining the Greater Cincinnati ISACA LinkedIn group.

Visit www.isaca.org to learn more about the organization.