Business Continuity Tabletop Exercise Scenarios

When somebody should go to the books stores, search foundation by shop, shelf by shelf, it is in fact problematic. This is why we provide the books compilations in this website. It will no question ease you to look guide **Business Continuity Tabletop Exercise Scenarios** as you such as.

By searching the title, publisher, or authors of guide you truly want, you can discover them rapidly. In the house, workplace, or perhaps in your method can be all best area within net connections. If you goal to download and install the Business Continuity Tabletop Exercise Scenarios , it is very easy then, before currently we extend the connect to buy and make bargains to download and install Business Continuity Tabletop Exercise Scenarios thus simple!

Business Continuity Management in Construction - Leni Sagita Riantini Supriadi 2017-08-19
This book provides an understanding of Business Continuity Management (BCM) implementation for local/international construction operations, with a primary focus on Indonesian construction firms as an illustrative example. It reviews the whole spectrum of work relating to organizational culture (OC) and the institutional framework (IF) as one of the key ways for companies to evaluate and implement BCM in construction operations. Once readers have acquired a sound understanding of BCM, OC and IF linkages in construction firms, the lessons learned can be extended to other companies. This is facilitated through a systematic assessment framework presented in the book using a Knowledge Based Decision Support System (BCM-KBDSS), which allows these companies to evaluate their current status quo with respect to BCM, OC and IF, and then make informed decisions on how and to what extent BCM should be implemented in their operations. As such, the book offers a unique blend of theory and practice, ensuring readers gain a far better understanding of BCM implementation in the construction industry.
Tabletop and Full-scale Emergency Exercises for General Aviation, Non-hub, and Small Hub Airports - James Fielding Smith 2016

Developing Your Pandemic Influenza Business Continuity Plan - Dr Goh Moh Heng 2006-03-01
The flu pandemic continues to threaten organizations with unimaginable disastrous impact. This book provides the principles of the BCM planning methodology and shows how they can be applied to prepare an effective and detailed pandemic flu business continuity plan. It is a comprehensive guide book that includes a practical 'fast track' how-to-do-it template so that even those without previous experience in business continuity planning, can develop their own pandemic flu business continuity plans.
The Official (ISC)2 Guide to the CISSP CBK Reference - John Warsinske 2019-04-04
The only official, comprehensive reference guide to the CISSP All new for 2019 and beyond, this is the authoritative common body of knowledge (CBK) from (ISC)2 for information security professionals charged with designing, engineering, implementing, and managing the overall information security program to protect organizations from increasingly sophisticated attacks. Vendor neutral and backed by (ISC)2, the CISSP credential meets the stringent requirements of ISO/IEC Standard 17024. This CBK covers the new eight domains of CISSP with the necessary depth to apply them to the daily practice of information security. Written by a team of subject matter experts, this comprehensive reference covers all of the more than 300 CISSP objectives and sub-objectives in a structured format with: Common and good practices for each objective Common vocabulary and definitions References to widely accepted computing standards Highlights of successful approaches through case studies Whether you've earned your CISSP credential or are looking for a valuable resource to help advance your security career, this comprehensive guide offers everything you need to apply the knowledge of the most recognized body of influence in information security.
CSO - 2006-12
The business to business trade publication for information and physical Security professionals.
A Risk Management Approach to Business Continuity - Julia Graham 2015-02-20
Julia Graham and David Kaye, two globally recognized risk management experts with experience in 50 countries, were among the first to recognize the interrelationship of Risk Management and Business Continuity and demonstrate how to integrate them with Corporate Governance enterprise-wide. They focus on all the factors that must be considered when developing a comprehensive Business Continuity Plan, especially for multi-location or multinational companies. Endorsed by The Business Continuity Institute, Institute for Risk Management, and Disaster Recovery Institute International, the book includes: • Chapter objectives, summaries and bibliographies; charts, sample forms, checklists throughout. • Plentiful case studies, in boxed text, sourced globally in the UK, US, Europe, Australia, Asia, etc. • Boxed inserts summarizing key concepts. • Glossy of 150 risk management and business continuity terms. • Wide range of challenges, including supply chain disruptions, media and brand attack, product contamination and product recall, bomb threats, chemical and biological threats, etc. • Instructions for designing/executing team exercises with role playing to rehearse scenarios. • Guidance on how to develop a business continuity plan, including a Business Impact Analysis. Downloadable Instructor Materials are available for college and professional developement use, including PowerPoint slides and syllabus for 12-week course with lecture outlines/notes, quizzes, reading assignments, discussion topics, projects "Provides clear guidance, supported with a wide range of memorable and highly relevant case studies, for any risk or business continuity manager to successfully meet the challenges of today and the future." --Steven Mellish, Chairman, The Business Continuity Institute
Handbook of Water and Wastewater Systems Protection - Robert M. Clark 2011-09-01
Following the events of 9/11, the Administrator of the US Environmental Protection Agency created the Water Protection Task Force (WPTF), which identified water and wastewater systems as a major area of vulnerability to deliberate attack. The WPTF suggested that there are steps that can be taken to reduce these vulnerabilities and to make it as difficult as possible for potential saboteurs to succeed. The WPTF recommended that be scrutinized with renewed vigor to secure water and wastewater systems against these possible threats. It also recommended that water and wastewater systems have a response plan in place in the event an act of terrorism occurs. The WPTF identified water distribution networks as an area of special vulnerability and highlighted the need for rapid on-line detection methods that are accurate and have a wide detection range. As a result of these recommendations novel technologies from various fields of science and engineering are now addressing water security issues and water and wastewater utilities are looking for innovative solutions. Once such technologies are available, there will be a rapid implementation process that will present many business opportunities for the private sector. However, in addition to terrorist threats water and wastewater systems are inherently vulnerable to natural disasters such as earthquakes and floods. This volume will address the problems associated with both intended terrorist attacks and natural disasters affecting water or wastewater systems. The book is divided into parts based on the kinds of threats facing water and wastewater systems: (1) a direct attack on water and wastewater infrastructure storage reservoirs, and distribution and collection networks; (2) a cyber attack disabling the functionality of the water and wastewater systems or taking over control of key components which might result in system failures; and (3) a deliberate chemical or biological contaminant injection at one of the water distribution system’s nodes. It will examine unique plans, technological and managerial innovations for protecting such systems, and includes descriptions of projects that were implemented to respond to

natural disasters. Case studies are presented that discuss existing projects and evaluate their performance, with an emphasis on providing guidelines and techniques that can be implemented by water and wastewater planners and managers to deal with natural and manmade disasters should they occur.
The NICE Cyber Security Framework - Izzat Alsmadi 2019-01-24
This textbook is for courses in cyber security education that follow National Initiative for Cybersecurity Education (NICE) KSAs work roles and framework, that adopt the Competency-Based Education (CBE) method. The book follows the CBT (KSA) general framework, meaning each chapter contains three sections, knowledge and questions, and skills/labs for Skills and Abilities. The author makes an explicit balance between knowledge and skills material in information security, giving readers immediate applicable skills. The book is divided into seven parts: Securely Provision; Operate and Maintain; Oversee and Govern; Protect and Defend; Analysis; Operate and Collect; Investigate. All classroom materials (in the book an ancillary) adhere to the NICE framework. Mirrors classes set up by the National Initiative for Cybersecurity Education (NICE) Adopts the Competency-Based Education (CBE) method of teaching, used by universities, corporations, and in government training Includes content and ancillaries that provide skill-based instruction on compliance laws, information security standards, risk response and recovery, and more
Risk Analysis and the Security Survey - James F. Broder 2011-12-07
As there is a need for careful analysis in a world where threats are growing more complex and serious, you need the tools to ensure that sensible methods are employed and correlated directly to risk. Counter threats such as terrorism, fraud, natural disasters, and information theft with the Fourth Edition of Risk Analysis and the Security Survey. Broder and Tucker guide you through analysis to implementation to provide you with the know-how to implement rigorous, accurate, and cost-effective security policies and designs. This book builds on the legacy of its predecessors by updating and covering new content. Understand the most fundamental theories surrounding risk control, design, and implementation by reviewing topics such as cost/benefit analysis, crime prediction, response planning, and business impact analysis--all updated to match today's current standards. This book will show you how to develop and maintain current business contingency and disaster recovery plans to ensure your enterprises are able to sustain loss are able to recover, and protect your assets, be it your business, your information, or yourself, from threats. Offers powerful techniques for weighing and managing the risks that face your organization Gives insights into universal principles that can be adapted to specific situations and threats Covers topics needed by homeland security professionals as well as IT and physical security managers
The Manager’s Guide to Simple, Strategic, Service-Oriented Business Continuity - Rachelle Loyear, MBCP, AFBCI, CISM, PMP 2017-05-10
You have the knowledge and skill to create a workable Business Continuity Management (BCM) program – but too often, your projects are stalled while you attempt to get the right information from the right person. Rachelle Loyear experienced these struggles for years before she successfully revamped and reinvented her company’s BCM program. In The Manager’s Guide to Simple, Strategic, Service-Oriented Business Continuity, she takes you through the practical steps to get your program back on track. Rachelle Loyear understands your situation well. Her challenge was to manage BCM in a large enterprise that required hundreds of BC plans to be created and updated. The frustrating reality she faced was that subject matter experts in various departments held the critical information she needed, but few were willing to write their parts of the plan. She tried and failed using all the usual methods to educate and motivate – and even threaten – departments to meet her deadlines. Finally, she decided there had to be a better way. The result was an incredibly successful BCM program that was adopted by BCM managers in other companies. She calls it “The Three S’s of BCM Success,” which can be summarized as: Simple – Strategic – Service-Oriented. Loyear’s approach is easy and intuitive, considering the BCM discipline from the point of view of the people in your organization who are tasked to work with you on building the plans and program. She found that most people prefer: Simple solutions when they are faced with something new and different. Strategic use of their time, making their efforts pay off. Service to be provided, lightening their part of the load while still meeting all the basic requirements. These tactics explain why the 3S program works. It helps you, it helps your program, and it helps your program partners. Loyear says, “If you follow the ‘Three S’ philosophy, the number of plans you need to document will be fewer, and the plans will be simpler and easier to produce. I’ve seen this method succeed repeatedly when the traditional method of handing a business leader a form to fill out or a piece of software to use has failed to produce quality plans in a timely manner.” In The Manager’s Guide to Simple, Strategic, Sevice-Oriented Business Continuity, Loyear shows you how to: Completely change your approach to the problems of “BCM buy-in.” Find new ways to engage and support your BCM program partners and subject matter experts. Develop easier-to-use policies, procedures, and plans. Improve your overall relationships with everyone involved in your BCM program. Craft a program that works around the roadblocks rather than running headlong into them.
Managing Risk in Information Systems - Darril Gibson 2014-07-17
This second edition provides a comprehensive overview of the SSCP Risk, Response, and Recovery Domain in addition to providing a thorough overview of risk management and its implications on IT infrastructures and compliance. Written by industry experts, and using a wealth of examples and exercises, this book incorporates hands-on activities to walk the reader through the fundamentals of risk management, strategies and approaches for mitigating risk, and the anatomy of how to create a plan that reduces risk. It provides a modern and comprehensive view of information security policies and frameworks; examines the technical knowledge and software skills required for policy implementation; explores the creation of an effective IT security policy framework; discusses the latest governance, regulatory mandates, business drives, legal considerations, and much more. --
The Official (ISC)2 SSCP CBK Reference - Mike Wills 2019-11-01
The only official body of knowledge for SSCP—(ISC)2’s popular credential for hands-on security professionals—fully revised and updated. Systems Security Certified Practitioner (SSCP) is an elite, hands-on cybersecurity certification that validates the technical skills to implement, monitor, and administer IT infrastructure using information security policies and procedures. SSCP certification—fully compliant with U.S. Department of Defense Directive 8140 and 8570 requirements—is valued throughout the IT security industry. The Official (ISC)2 SSCP CBK Reference is the only official Common Body of Knowledge (CBK) available for SSCP-level practitioners, exclusively from (ISC)2, the global leader in cybersecurity certification and training. This authoritative volume contains essential knowledge practitioners require on a regular basis. Accurate, up-to-date chapters provide in-depth coverage of the seven SSCP domains: Access Controls; Security Operations and Administration; Risk Identification, Monitoring and Analysis; Incident Response and Recovery; Cryptography; Network and Communications Security; and Systems and Application Security. Designed to serve as a reference for information security professionals throughout their careers, this indispensable (ISC)2guide: Provides comprehensive coverage of the latest domains and objectives of the SSCP Helps better secure critical assets in their organizations Serves as a complement to the SSCP Study Guide for certification candidates The Official (ISC)2 SSCP CBK Reference is an essential resource for SSCP-level professionals, SSCP candidates and other practitioners involved in cybersecurity.
Operational and Business Continuity Planning for Prolonged Airport Disruptions - Scott Corzine 2013
"TRB's Airport Cooperative Research Program (ACRP) Report 93: Operational and Business Continuity Planning for Prolonged Airport Disruptions provides a guidebook and software tool for airport operators to assist, plan, and prepare for disruptive and catastrophic events that have the potential for causing prolonged airport closure resulting in adverse impacts to the airport and to the local, regional, and national economy. The software tool is available in a CD-ROM format and is intended to help develop and document airport business continuity plans or revise current plans in light of this guidance. The CD is also available for download from TRB's website as an ISO image."--Publisher's description.
Mastering Windows Security and Hardening - Mark Dunkerley 2022-08-19
A comprehensive guide to administering and protecting the latest Windows 11 and Windows server operating system from ongoing cyber threats using zero-trust security principles Key Features Learn to protect your Windows environment using zero-trust and a multi-layered security approach Implement security controls using Intune, Configuration Manager, Defender for Endpoint, and more Understand how to onboard modern cyber-threat defense solutions for Windows clients Book Description Are you looking for the most current and effective ways to protect Windows-based systems from being compromised by intruders? This updated second edition is a detailed guide that helps you gain the expertise to implement efficient security measures and create robust defense solutions using modern technologies. The first part of

the book covers security fundamentals with details around building and implementing baseline controls. As you advance, you'll learn how to effectively secure and harden your Windows-based systems through hardware, virtualization, networking, and identity and access management (IAM). The second section will cover administering security controls for Windows clients and servers with remote policy management using Intune, Configuration Manager, Group Policy, Defender for Endpoint, and other Microsoft 365 and Azure cloud security technologies. In the last section, you'll discover how to protect, detect, and respond with security monitoring, reporting, operations, testing, and auditing. By the end of this book, you'll have developed an understanding of the processes and tools involved in enforcing security controls and implementing zero-trust security principles to protect Windows systems. What you will learn Build a multi-layered security approach using zero-trust concepts Explore best practices to implement security baselines successfully Get to grips with virtualization and networking to harden your devices Discover the importance of identity and access management Explore Windows device administration and remote management Become an expert in hardening your Windows infrastructure Audit, assess, and test to ensure controls are successfully applied and enforced Monitor and report activities to stay on top of vulnerabilities Who this book is for If you're a cybersecurity or technology professional, solutions architect, systems engineer, systems administrator, or anyone interested in learning how to secure the latest Windows-based systems, this book is for you. A basic understanding of Windows security concepts, Intune, Configuration Manager, Windows PowerShell, and Microsoft Azure will help you get the best out of this book.

CISA Certified Information Systems Auditor Exam Practice Questions & Dumps - James Bolton 2020-02-06

Certified Information Systems Auditor (CISA) is a certification issued by ISACA to people in charge of ensuring that an organization's IT and business systems are monitored, managed and protected; the certification is presented after completion of a comprehensive testing and application process. The CISA certification is a globally recognized standard for appraising an IT auditor's knowledge, expertise and skill in assessing vulnerabilities and instituting IT controls in an enterprise environment. It is designed for IT auditors, audit managers, consultants and security professionals. Preparing for the Certified Information Systems Auditor exam to become an CISA Certified by ISACA? Here we've brought 900+ Exam Questions for you so that you can prepare well for this CISA exam Unlike other online simulation practice tests, you get a Paperback version that is easy to read & remember these questions. You can simply rely on these questions for successfully certifying this exam.

The Disaster Recovery Handbook - Michael Wallace 2004

It takes careful planning to ensure that a disaster of any typewhether the result of fire, an electrical outage, a major computer virus, or even terrorismdoes not result in a prolonged service interruption that could affect your business for years to come. By creating a proactive disaster recovery program, you can keep your people, inventory, and resources safe and secure. The Disaster Recovery Handbook is a comprehensive reference to help your business survive any kind of major disruption, giving you the tools you need to protect your organization in the event of extraordinary circumstances. Filled with practical solutions and ready-to-use tools, the book provides detailed instructions for: * Assessing risk * Assembling a disaster recovery team * Building an interim plan for immediate protection * Setting up an emergency operations center * Clearly documenting recovery procedures * Testing and debugging the plan to make sure it works * Ensuring the health and physical safety of your people * Recovering vital records * Protecting your material resources

Business Continuity Planning - Brenda D. Phillips 2020-11-24

Terrorism, natural disasters, or hazardous materials threaten the viability for all types of businesses. With an eye toward business scale, scope, and diversity, Business Continuity Planning: Increasing Workplace Resilience to Disasters, addresses a range of potential businesses from home-based to large corporations in the face of these threats, including the worldwide COVID-19 pandemic. Information on business continuity planning is easy to find but can be difficult to work through. Terminology, required content, and planning barriers often prevent progress. This volume solves such problems by guiding readers, step-by-step, through such actions as identifying hazards and assessing risks, writing critical functions, forming teams, and encouraging stakeholder participation. In essence, this volume serves as a business continuity planning coach for people new to the process or seeking to strengthen and deepen their ongoing efforts. By engaging stakeholders in a business continuity planning process, businesses can protect employees, customers, and their financial stability. Coupled with examples from recent disasters, planners will be able to inspire and involve stakeholders in creating a more resilient workplace. Designed for both educators and practitioners, Business Continuity Planning: Increasing Workplace Resilience to Disasters walks users through how to understand and execute the essential steps of business continuity planning. Presents evidence-based best practices coupled with standard operating procedures for business continuity planning in a stepwise, user-oriented manner Includes numerous examples and case studies bringing the ideas and procedures to life Provides user-friendly materials and resources, such as templated worksheets, checklists, and procedures with clear instructions, making the volume engaging and immediately operational

Building an Enterprise-Wide Business Continuity Program - Kelley Okolita 2016-04-19

If you had to evacuate from your building right now and were told you couldn't get back in for two weeks, would you know what to do to ensure your business continues to operate? Would your staff? Would every person who works for your organization? Increasing threats to business operations, both natural and man-made, mean a disaster could occur at any time. It is essential that corporations and institutions develop plans to ensure the preservation of business operations and the technology that supports them should risks become reality. Building an Enterprise-Wide Business Continuity Program goes beyond theory to provide planners with actual tools needed to build a continuity program in any enterprise. Drawing on over two decades of experience creating continuity plans and exercising them in real recoveries, including 9/11 and Hurricane Katrina, Master Business Continuity Planner, Kelley Okolita, provides guidance on each step of the process. She details how to validate the plan and supplies time-tested tips for keeping the plan action-ready over the course of time. Disasters can happen anywhere, anytime, and for any number of reasons. However, by proactively planning for such events, smart leaders can prepare their organizations to minimize tragic consequences and readily restore order with confidence in the face of such adversity.

Practitioner's Guide to Business Impact Analysis - Priti Sikdar 2017-09-19

This book illustrates the importance of business impact analysis, which covers risk assessment, and moves towards better understanding of the business environment, industry specific compliance, legal and regulatory landscape and the need for business continuity. The book provides charts, checklists and flow diagrams that give the roadmap to collect, collate and analyze data, and give enterprise management the entire mapping for controls that comprehensively covers all compliance that the enterprise is subject to have. The book helps professionals build a control framework tailored for an enterprise that covers best practices and relevant standards applicable to the enterprise. Presents a practical approach to assessing security, performance and business continuity needs of the enterprise Helps readers understand common objectives for audit, compliance, internal/external audit and assurance. Demonstrates how to build a customized controls framework that fulfills common audit criteria, business resilience needs and internal monitoring for effectiveness of controls Presents an Integrated Audit approach to fulfill all compliance requirements

Blueprints for High Availability - Evan Marcus 2003-09-10

Expert techniques for designing your system to achieve maximum availability and predictable downtime With your company's reputation and profits at stake, downtime on your 24/7 web site is not an option, nor is poor application performance. Now in its second edition, this authoritative book provides you with the design blueprints to maximize your system availability. Striking a balance between costs and benefits, the authors show you all of the elements of your computer system that can fail-as well as ways to assess their reliability and attain resiliency and high availability for each one. A unique feature is "Tales from the Field," a collection of true-to-life experiences that will help you avoid mistakes and deploy your system with confidence. Learn how to design your system to limit the impact of such problems as computer viruses, natural disasters, or the corruption of critical files and discover how to: * Implement effective backup-and-restore and tape management strategies * Arrange disks and disk arrays to avoid downtime caused by inevitable failures * Utilize technologies such as Storage Area Networks (SANs), Network Attached Storage (NAS), Virtualization, and clustering * Achieve effective application recovery after any part of the system has failed * Replicate critical data to remote systems across a network

Information Security Illuminated - Michael G. Solomon 2005
A comprehensive textbook that introduces students to current information security practices and prepares them for various related certifications.
Business Continuity Exercises - Charlie Maclean-Bristol, MA (Hons), PgD, FBCI, FEPS, CBCI 2020-11-01
An Unexercised Continuity Plan Could Be More Dangerous Than No Plan At All! Is exercising your continuity program too time-consuming, costly, or difficult to justify in the face of conflicting organizational priorities or senior management buy-in? What if you could use quick, cost-effective, easy exercises to get valuable results with only a relatively modest commitment? Whether you're a seasoned practitioner or just getting started, Charlie Maclean-Bristol provides you with expert guidance, a practical framework, and lots of proven examples, tools, tips, techniques and scenarios to get your business continuity exercise program moving! You can carry out any of the 18 simple yet effective exercises detailed in this book in less than an hour, regardless of your level of experience. Plus, you will find all the support you will need to produce successful exercises. Build your teams' knowledge, experience, confidence and abilities while validating your business continuity program, plans and procedures with these proven resources! Business Continuity Exercises: Quick Exercises to Validate Your Plan Will Help You To: Understand the process of planning and conducting business exercises efficiently while achieving maximum results. Develop the most appropriate strategy framework for conducting and assessing your exercise. Overcome obstacles to your business continuity exercise program, whether due to budget restrictions, time constraints, or conflicting priorities. Choose the most appropriate and effective exercise scenario, purpose and objectives. Plan and conduct your exercise using a straightforward, proven methodology with extensive tools and resources. Conduct exercises suitable for responding to all types of business interruptions and emergencies, including cyber incidents and civil disasters. Conduct exercises for newcomers to business continuity as well as for experienced practitioners. Create a comprehensive post-exercise report to achieve valuable insights, keep management and participants in the loop, and to further your objectives.
The Manager's Guide to Business Continuity Exercises - Jim Burtles, KLJ, MMLJ, Hon FBCI 2016-10-06
You designed your Business Continuity Plan to keep your business in business regardless of the forces of man and nature. But how do you know that the plan really works? Few companies can afford the recommended full-scale exercises several times a year. In The Manager's Guide to Business Continuity Exercises, Jim Burtles, an internationally known expert, details the options for conducting a range of tests and exercises to keep your plan effective and up to date. Your challenge is to maintain a good and effective plan in the face of changing circumstances and limited budgets. If your situation is like that in most companies, you really cannot depend on the results of last year's test or exercise of the plan. People tend to forget, lose confidence, lose interest, or even be replaced by other people who were not involved in your original planning. Jim Burtles explains: "You cannot have any real confidence in your plans and procedures until they have been fully tested...Exercises are the only way we can be sure that the people will be able to interpret the plans and procedures correctly within the requisite timeframe under difficult circumstances." As you do your job in this constantly shifting context, Jim Burtles helps you to: • Differentiate between an "exercise" and a "test" – and see the value of each in your BC program. • Understand the different types of plans and identify the people who need to be involved in exercises and tests for each. • Use the "Five-Stage Growth Path" – from desktop to walkthrough to full-scale exercise -- to conduct gradual testing, educate personnel, foster capability, and build confidence. • Create a variety of unusual scenario plot-lines that will keep up everyone's interest. • Identify the eight main elements in developing and delivering a successful BC exercise. • Select and prepare a "delivery team" and a "response team" for your exercise. • Make sure everyone understands the "rules of engagement." • Use the lessons learned from exercises and tests to audit, update, and maintain the plan. You are well aware that a host of problems may crop up in any kind of company-wide project. These problems can range from basic logistics like time and place, to non-support from executives and managers, to absenteeism, to the weather, to participants forgetting their lines. Throughout the book, Burtles uses his decades of experience working with companies like yours to give you useful examples, case studies, and down-to-earth advice to help you handle the unexpected and work toward the results you are looking for.
Business Continuity and Risk Management - Kurt J. Engemann 2014-10-01
As an instructor, you have seen business continuity and risk management grow exponentially, offering an exciting array of career possibilities to your students. They need the tools needed to begin their careers -- and to be ready for industry changes and new career paths. You cannot afford to use limited and inflexible teaching materials that might close doors or limit their options. Written with your classroom in mind,Business Continuity and Risk Management: Essentials of Organizational Resilience is the flexible, modular textbook you have been seeking -- combining business continuity and risk management. Full educator-designed teaching materials available for download. From years of experience teaching and consulting in Business Continuity and Risk, Kurt J. Engemann and Douglas M. Henderson explain everything clearly without extra words or extraneous philosophy. Your students will grasp and apply the main ideas quickly. They will feel that the authors wrote this textbook with them specifically in mind -- as if their questions are answered even before they ask them. Covering both Business Continuity and Risk Management and how these two bodies of knowledge and practice interface, Business Continuity and Risk Management: Essentials of Organizational Resilience is a state-of-the-art textbook designed to be easy for the student to understand -- and for you, as instructor, to present. Flexible, modular design allows you to customize a study plan with chapters covering: Business Continuity and Risk principles and practices. Information Technology and Information Security. Emergency Response and Crisis Management. Risk Modeling – in-depth instructions for students needing the statistical underpinnings in Risk Management. Global Standards and Best Practices Two real-world case studies are integrated throughout the text to give future managers experience in applying chapter principles to a service company and a manufacturer. Chapter objectives, discussion topics, review questions, numerous charts and graphs. Glossary and Index. Full bibliography at the end of each chapter. Extensive, downloadable classroom-tested Instructor Resources are available for college courses and professional development training, including slides, syllabi, test bank, discussion questions, and case studies. Endorsed by The Business Continuity Institute (BCI) and The Institute of Risk Management (IRM). QUOTES "It's difficult to write a book that serves both academia and practitioners, but this text provides a firm foundation for novices and a valuable reference for experienced professionals."--Security Management Magazine "The authors...bring the subject to life with rich teaching and learning features, making it an essential read for students and practitioners alike." – Phil AUTHOR BIOS Kurt J. Engemann, PhD, CBCP, is the Director of the Center for Business Continuity and Risk Management and Professor of Information Systems in the Hagan School of Business at Iona College. He is the editor-in-chief of the International Journal of Business Continuity and Risk Management Douglas M. Henderson, FSA, CBCP, is President of Disaster Management, Inc., and has 20+ years of consulting experience in all areas of Business Continuity and Emergency Response Management. He is the author of Is Your Business Ready for the Next Disaster? and a number of templates.
A Supply Chain Management Guide to Business Continuity - Betty Kildow 2011-01-12
A well-monitored supply chain is any business's key to productivity and profit. But each link in that chain is its own entity, subject to its own ups, downs, and business realities. If one falters, every other link—and the entire chain—becomes vulnerable. Kildow's book identifies the different phases of business continuity program development and maintenance, including: • Recognizing and mitigating potential threats, risks, and hazards • Evaluating and selecting suppliers, contractors, and service providers • Developing, testing, documenting, and maintaining business continuity plans • Following globally accepted best practices • Analyzing the potential business impact of supply chain disruptions Filled with powerful assessment tools, detailed disaster-preparedness checklists and scenarios, and instructive case studies in supply chain reliability, A Supply Chain Management Guide to Business Continuity is a crucial resource in the long-term stability of any business.
How to Measure Anything in Cybersecurity Risk - Douglas W. Hubbard 2016-07-25
A ground shaking exposé on the failure of popular cyber risk management methods How to Measure Anything in Cybersecurity Risk exposes the shortcomings of current "risk management" practices, and offers a series of improvement techniques that help you fill the holes and ramp up security. In his bestselling book How to Measure Anything, author Douglas W. Hubbard opened the business world's eyes to the critical need for better measurement. This book expands upon that premise and draws from The Failure of Risk Management to sound the alarm in the cybersecurity realm. Some of the field's premier risk

management approaches actually create more risk than they mitigate, and questionable methods have been duplicated across industries and embedded in the products accepted as gospel. This book sheds light on these blatant risks, and provides alternate techniques that can help improve your current situation. You'll also learn which approaches are too risky to save, and are actually more damaging than a total lack of any security. Dangerous risk management methods abound; there is no industry more critically in need of solutions than cybersecurity. This book provides solutions where they exist, and advises when to change tracks entirely. Discover the shortcomings of cybersecurity's "best practices" Learn which risk management approaches actually create risk Improve your current practices with practical alterations Learn which methods are beyond saving, and worse than doing nothing Insightful and enlightening, this book will inspire a closer examination of your company's own risk management practices in the context of cybersecurity. The end goal is airtight data protection, so finding cracks in the vault is a positive thing—as long as you get there before the bad guys do. How to Measure Anything in Cybersecurity Risk is your guide to more robust protection through better quantitative processes, approaches, and techniques.

Instructor's Guide - Regina Phelps 2012-07-20

Exercises are a mainstay in the field of emergency management and business continuity planning. Although many organizations conduct exercises, and the organizers may be emergency management/business continuity subject matter experts, they do not excel in the discipline of designing and conducting the actual exercise - which means they simply don't get the best results out of their effort. This comprehensive and highly interactive course provides everything that an instructor needs to teach - and inspire - students to create great exercises. The course begins with a "silly little question": Why are we doing this? What seems like a simple query is actually one of the keys to get the most out of every exercise design. The course then peels back the mysteries of the design process with the goal of creating the best experience possible. Whether your students are developing simple tabletop exercises or working on a full-scale extravaganza that resembles a Hollywood movie, this course will provide you and them with gems of wisdom to make their exercises powerful and pack a punch. An internationally recognized expert in exercise design, Regina Phelps whispers her secrets into your ear week by week to ensure your course success.

Scrappy Business Contingency Planning - Michael Seese 2010

In simple terms, business contingency planning (BCP) is the art of preparing an enterprise for "bad things." "Scrappy Business Contingency Planning" provides a blueprint for the creation of a business contingency program from the ground up.

Wiley CIA Exam Review 2020, Part 3 - S. Rao Vallabhaneni 2019-11-19

Get effective and efficient instruction on all CIA business knowledge exam competencies in 2020 Updated for 2020, the Wiley CIA Exam Review 2020, Part 3 Business Knowledge for Internal Auditing offers readers a comprehensive overview of the internal auditing process as set out by the Institute of Internal Auditors. The Exam Review covers the four domains tested by the Certified Internal Auditor exam, including: ??? Business acumen ??? Information security ??? Information technology ??? Financial management The Wiley CIA Exam Review 2020, Part 3 Business Knowledge for Internal Auditing is a perfect resource for candidates preparing for the CIA exam. It provides an accessible and efficient learning experience for students regardless of their current level of proficiency.

IRS Management - Bernice Steinhardt 2010-01

The IRS collects the revenues that fund the fed. gov¿t. and issues billions of dollars in refunds. Consequently, IRS's ability to demonstrate agility and speed in restoring its functions after a disruption is vital to the gov¿t. and the economy. This report: (1) identified the definition and attributes of organizational resilience; (2) examined the extent to which these attributes are exhibited within IRS; and (3) reviewed the challenges and opportunities faced by the IRS in becoming more resilient. The auditor reviewed IRS human capital and emergency preparedness policies and strategic plans, observed campus operations and emergency working group meetings, and interviewed officials from headquarters and each of the four business units. Illus.

How to Measure Anything - Douglas W. Hubbard 2010-03-25

Now updated with new research and even more intuitive explanations, a demystifying explanation of how managers can inform themselves to make less risky, more profitable business decisions This insightful and eloquent book will show you how to measure those things in your own business that, until now, you may have considered "immeasurable," including customer satisfaction, organizational flexibility, technology risk, and technology ROI. Adds even more intuitive explanations of powerful measurement methods and shows how they can be applied to areas such as risk management and customer satisfaction Continues to boldly assert that any perception of "immeasurability" is based on certain popular misconceptions about measurement and measurement methods Shows the common reasoning for calling something immeasurable, and sets out to correct those ideas Offers practical methods for measuring a variety of "intangibles" Adds recent research, especially in regards to methods that seem like measurement, but are in fact a kind of "placebo effect" for management – and explains how to tell effective methods from management mythology Written by recognized expert Douglas Hubbard-creator of Applied Information Economics-How to Measure Anything, Second Edition illustrates how the author has used his approach across various industries and how any problem, no matter how difficult, ill defined, or uncertain can lend itself to measurement using proven methods.

Business Continuity from Preparedness to Recovery - Eugene Tucker 2014-12-22

Business Continuity from Preparedness to Recovery: A Standards-Based Approach details the process for building organizational resiliency and managing Emergency and Business Continuity programs. With over 30 years of experience developing plans that have been tested by fire, floods, and earthquakes, Tucker shows readers how to avoid common traps and ensure a successful program, utilizing, detailed Business Impact Analysis (BIA) questions, continuity strategies and planning considerations for specific business functions. One of the few publications to describe the entire process of business continuity planning from emergency plan to recovery, Business Continuity from Preparedness to Recovery addresses the impact of the new ASIS, NFPA, and ISO standards. Introducing the important elements of business functions and showing how their operations are maintained throughout a crisis situation, it thoroughly describes the process of developing a mitigation, prevention, response, and continuity Management System according to the standards. Business Continuity from Preparedness to Recovery fully integrates Information Technology with other aspects of recovery and explores risk identification and assessment, project management, system analysis, and the functional reliance of most businesses and organizations in a business continuity and emergency management context. Offers a holistic approach focusing on the development and management of Emergency and Business Continuity Management Systems according to the new standards Helps ensure success by describing pitfalls to avoid and preventive measures to take Addresses program development under the standards recently developed by ISO, ASIS and NFPA Provides both foundational principles and specific practices derived from the author’s long experience in this field Explains the requirements of the Business Continuity Standards

Business Continuity - Bob Hayes 2013-04-03

The Business Continuity playbook provides the background and tools to create, manage, and execute all facets of an organization’s business continuity program (BCP). Business continuity planning is an activity performed daily by organizations of all types and sizes to ensure that critical business functions are available before, during, and after a crisis. This playbook guides the security leader through the development, implementation, and maintenance of a successful BCP. The text begins with a detailed description of the concept and value of business continuity planning, transitioning into a step-by-step guide to building or enhancing a BCP. Its 14 appendices, which include sample forms, templates, and definitions, make it an invaluable resource for business continuity planning. The Business Continuity playbook is a part of Elsevier’s Security Executive Council Risk Management Portfolio, a collection of real world solutions and "how-to" guidelines that equip executives, practitioners, and educators with proven information for successful security and risk management programs. Answers the unavoidable question, "What is the business value of a business continuity program?" Breaks down a business continuity program into four major elements for better understanding and easier implementation Includes 14 appendices that provide sample forms, templates, and definitions for immediate adaptation in any business setting

Official (ISC)2 Guide to the CISSP CBK - Steven Hernandez CISSP 2009-12-22

With each new advance in connectivity and convenience comes a new wave of threats to privacy and security capable of destroying a company's reputation, violating a consumer's privacy, compromising

intellectual property, and in some cases endangering personal safety. This is why it is essential for information security professionals to stay up to da

Wiley CIA Exam Review Focus Notes, Internal Audit Knowledge Elements - S. Rao Vallabhaneni 2013-03-14

Reinforce, review, recap—anywhere you like. Study for the three parts of the CIA Exam no matter where you are with each of the three Focus Notes volumes. With updated content for 2013 exam changes, Wiley CIA Exam Review Focus Notes 2013 reviews important strategies, basic skills and concepts—so you can pass the CIA Exam your first time out. Its portable, spiral-bound, flashcard format helps you study on the go with hundreds of outlines, summarized concepts, and techniques designed to hone your CIA Exam knowledge.

Business Continuity Planning - Ralph L. Kliem 2015-08-21

If a major event such as a terrorist attack, 7.2 earthquake, tsunami, or hacker attack were to disrupt business operations, would your organization be prepared to respond to the financial, political, and social impacts? In order for your company to be resilient, it must be ready to respond and recover quickly from the impact of such events. Busines

Security Program and Policies - Sari Greene 2014-03-20

Everything you need to know about information security programs and policies, in one book Clearly explains all facets of InfoSec program and policy planning, development, deployment, and management Thoroughly updated for today’s challenges, laws, regulations, and best practices The perfect resource for anyone pursuing an information security management career ¿ In today’s dangerous world, failures in information security can be catastrophic. Organizations must protect themselves. Protection begins with comprehensive, realistic policies. This up-to-date guide will help you create, deploy, and manage them. Complete and easy to understand, it explains key concepts and techniques through real-life examples. You’ll master modern information security regulations and frameworks, and learn specific best-practice policies for key industry sectors, including finance, healthcare, online commerce, and small business. ¿ If you understand basic information security, you’re ready to succeed with this book. You’ll find projects, questions, exercises, examples, links to valuable easy-to-adapt information security policies...everything you need to implement a successful information security program. ¿ Learn how to ·¿¿¿¿¿¿¿ Establish program objectives, elements, domains, and governance ·¿¿¿¿¿¿¿ Understand policies, standards, procedures, guidelines, and plans—and the differences among them ·¿¿¿¿¿¿¿ Write policies in “plain language,” with the right level of detail ·¿¿¿¿¿¿¿ Apply the Confidentiality, Integrity & Availability (CIA) security model ·¿¿¿¿¿¿¿ Use NIST resources and ISO/IEC 27000-series standards ·¿¿¿¿¿¿¿ Align security with business strategy ·¿¿¿¿¿¿¿ Define, inventory, and classify your information and systems ·¿¿¿¿¿¿¿ Systematically identify, prioritize, and manage InfoSec risks ·¿¿¿¿¿¿¿ Reduce “people-related” risks with role-based Security Education, Awareness, and Training (SETA) ·¿¿¿¿¿¿¿ Implement effective physical, environmental, communications, and operational security ·¿¿¿¿¿¿¿ Effectively manage access control ·¿¿¿¿¿¿¿ Secure the entire system development lifecycle ·¿¿¿¿¿¿¿ Respond to incidents and ensure continuity of operations ·¿¿¿¿¿¿¿ Comply with laws and regulations, including GLBA, HIPAA/HITECH, FISMA, state data security and notification rules, and PCI DSS ¿

CompTIA Security+ SY0-401 Exam Cram - Diane Barrett 2015-02-07

CompTIA® Security+ Exam Cram, Fourth Edition, is the perfect study guide to help you pass CompTIA’s newly updated version of the Security+ exam. It provides coverage and practice questions for every exam topic. The book contains a set of 200 questions in two full practice exams. The CD-ROM contains the powerful Pearson IT Certification Practice Test engine that provides real-time practice and feedback with all the questions so you can simulate the exam. Covers the critical information you need to know to score higher on your Security+ exam! --Categorize types of attacks, threats, and risks to your systems --Secure devices, communications, and network infrastructure -- Troubleshoot issues related to networking components -- Effectively manage risks associated with a global business environment -- Differentiate between control methods used to secure the physical domain -- Identify solutions to secure hosts, data, and applications -- Compare techniques to mitigate risks in static environments -- Determine relevant access control, authorization, and authentication procedures -- Select appropriate mitigation techniques in response to attacks and vulnerabilities -- Apply principles of cryptography and effectively deploy related solutions --Implement security practices from both a technical and an organizational standpoint

Cyber Security Culture - Peter Trim 2016-05-13

Focusing on countermeasures against orchestrated cyber-attacks, Cyber Security Culture is research-based and reinforced with insights from experts who do not normally release information into the public arena. It will enable managers of organizations across different industrial sectors and government agencies to better understand how organizational learning and training can be utilized to develop a culture that ultimately protects an organization from attacks. Peter Trim and David Upton believe that the speed and complexity of cyber-attacks demand a different approach to security management, including scenario-based planning and training, to supplement security policies and technical protection systems. The authors provide in-depth understanding of how organizational learning can produce cultural change addressing the behaviour of individuals, as well as machines. They provide information to help managers form policy to prevent cyber intrusions, to put robust security systems and procedures in place and to arrange appropriate training interventions such as table top exercises. Guidance embracing current and future threats and addressing issues such as social engineering is included. Although the work is embedded in a theoretical framework, non-technical staff will find the book of practical use because it renders highly technical subjects accessible and links firmly with areas beyond ICT, such as human resource management - in relation to bridging the education/training divide and allowing organizational learning to be embraced. This book will interest Government officials, policy advisors, law enforcement officers and senior managers within companies, as well as academics and students in a range of disciplines including management and computer science.

Fundamentals of Communications and Networking - Michael G. Solomon 2014-08-08

Today's networks are required to support an increasing array of real-time communication methods. Video chat, real-time messaging, and always-connected resources put demands on networks that were previously unimagined. The Second Edition of Fundamentals of Communications and Networking helps readers better understand today's networks and the way they support the evolving requirements of different types of organizations. It discusses the critical issues of designing a network that will meet an organization's performance needs and discusses how businesses use networks to solve business problems. Using numerous examples and exercises, this text incorporates hands-on activities to prepare readers to fully understand and design modern networks and their requirements. Key Features of the Second Edition: - Introduces network basics by describing how networks work - Discusses how networks support the increasing demands of advanced communications - Illustrates how to map the right technology to an organization's needs and business goals - Outlines how businesses use networks to solve business problems, both technically and operationally.