1st line of defense risk management

1st Line of Defense Risk Management: A Comprehensive Overview

Author: Dr. Anya Sharma, PhD, FRM, CISA, Certified Risk Management Assurance Professional (CRMAP)

Dr. Anya Sharma is a globally recognized expert in risk management with over 15 years of experience in financial institutions and consulting. Her PhD in Risk Management and her certifications (FRM, CISA, CRMAP) solidify her authority on the subject, particularly concerning the crucial role of the 1st line of defense.

Publisher: Institute of Risk Management (IRM) – A globally respected professional body for risk management professionals, offering qualifications, resources, and research in the field, including extensive materials on 1st line of defense risk management frameworks.

Editor: Mr. David Miller, CIPP/E, CIPM – A seasoned editor with a background in compliance and data privacy, ensuring accuracy and clarity in presenting complex concepts of 1st line of defense risk management.

Keywords: 1st line of defense risk management, risk management framework, operational risk management, compliance risk management, first line of defense responsibilities, risk identification, risk assessment, risk mitigation, risk control, effective risk management, integrated risk management

Introduction: Understanding the Foundation of 1st Line of Defense Risk Management

Effective risk management is the cornerstone of any successful organization. Within a robust three-lines-of-defense model, the 1st line of defense risk management plays a pivotal role. This first line isn't just about reacting to risks; it's about proactively identifying, assessing, and mitigating them at the source. This article provides a comprehensive overview of 1st line of defense risk management, exploring its principles, responsibilities, challenges, and best practices.

Defining 1st Line of Defense Risk Management: Ownership and

Accountability

The 1st line of defense in risk management encompasses the individuals and teams directly involved in the day-to-day operations of an organization. They are the "owners" of risk within their specific areas of responsibility. This means they are accountable for identifying, assessing, controlling, and monitoring risks inherent in their processes, products, and services. 1st line of defense risk management is not simply a compliance exercise; it's integral to achieving business objectives and ensuring sustainable success.

Core Responsibilities of the 1st Line of Defense in Risk Management

The effectiveness of 1st line of defense risk management hinges on several key responsibilities:

1. Proactive Risk Identification:

The 1st line actively seeks out potential risks through various methods, including:

Internal controls assessment: Regularly reviewing and testing existing controls to ensure their effectiveness.
Process mapping: Visualizing operations to pinpoint vulnerabilities and potential failure points.
Data analysis: Using data to identify trends and patterns that indicate emerging risks.
Stakeholder engagement: Gathering input from employees at all levels to gain a broad perspective on potential risks.

2. Risk Assessment and Prioritization:

Once risks are identified, the 1st line must assess their likelihood and potential impact. This often involves qualitative and quantitative assessments, leading to a prioritized risk register that focuses on the most critical issues.

3. Risk Mitigation and Control Implementation:

This is the crucial step where the 1st line implements controls to reduce or eliminate identified risks. This could involve:

Implementing new procedures: Creating or revising processes to address specific risk factors.
Investing in technology: Utilizing tools and systems to enhance control effectiveness.
Improving employee training: Equipping staff with the knowledge and skills to manage risks effectively.

4. Risk Monitoring and Reporting:

Continuous monitoring is vital. The 1st line tracks key risk indicators (KRIs) to ensure that controls remain effective and that new risks are promptly identified. Regular reporting to senior management and the second line of defense provides transparency and accountability.

Challenges in Effective 1st Line of Defense Risk Management

Implementing effective 1st line of defense risk management presents various challenges:

Resource constraints: Limited budgets and staffing can hinder the implementation of comprehensive risk management programs.
Lack of awareness and training: Employees may lack sufficient understanding of risk management principles and their individual responsibilities.
Resistance to change: Introducing new processes or controls can face resistance from staff accustomed to existing methods.
Data silos: Information dispersed across different departments can make it difficult to obtain a holistic view of risk.
Overburdened staff: Adding risk management responsibilities to already full plates can lead to burnout and ineffective implementation.

Best Practices for Strengthening 1st Line of Defense Risk Management

Organizations can strengthen their 1st line of defense through:

Clear roles and responsibilities: Defining who is accountable for specific risk areas.
Robust risk assessment methodologies: Implementing standardized processes for identifying and assessing risks.
Effective risk reporting and communication: Establishing clear channels for reporting and escalating risks.
Regular training and development: Equipping staff with the necessary skills and knowledge to manage risks effectively.
Technology integration: Utilizing risk management software to streamline processes and improve data analysis.
Strong risk culture: Fostering a culture where risk identification and management are valued and prioritized.

Integrating 1st Line of Defense Risk Management with Other Lines of

Defense

Effective 1st line of defense risk management is not an isolated function. It needs to be integrated with the other lines of defense:

2nd Line of Defense (Independent Assurance): Provides oversight and challenge to the 1st line, ensuring the effectiveness of risk management processes.
3rd Line of Defense (Internal Audit): Independently assesses the effectiveness of the entire risk management framework, including the performance of the 1st and 2nd lines.

This integrated approach fosters a holistic risk management system that effectively identifies, assesses, and mitigates risk across the organization.

Conclusion

1st line of defense risk management is not merely a compliance obligation; it's a strategic imperative for organizational success. By proactively identifying, assessing, and mitigating risks at the source, organizations can enhance operational efficiency, protect their reputation, and achieve sustainable growth. A strong 1st line, supported by effective 2nd and 3rd lines of defense, forms the bedrock of a robust and resilient risk management framework.

FAQs

1. What is the difference between 1st, 2nd, and 3rd lines of defense in risk management? The 1st line owns and manages risk within their operations; the 2nd line provides independent oversight and assurance; the 3rd line (internal audit) provides independent assessment of the entire risk management framework.

1. How can I ensure my staff are adequately trained in 1st line of defense risk management? Develop tailored training programs covering risk identification, assessment, mitigation, and reporting. Use case studies, simulations, and ongoing reinforcement.

1. What are key risk indicators (KRIs) in 1st line of defense risk management? KRIs are metrics that

signal potential risks. Examples include customer churn rate, operational downtime, and incident reports.

1. How can I improve risk communication within my 1st line of defense? Establish clear communication channels, use regular reporting mechanisms, and foster a culture of open communication about risk.

1. What role does technology play in 1st line of defense risk management? Technology can automate risk assessments, monitor KRIs, and provide early warning systems for emerging risks.

1. How can I measure the effectiveness of my 1st line of defense risk management program? Track key metrics such as the number of identified risks, the effectiveness of mitigation strategies, and the frequency of risk-related incidents.

1. How can I address resistance to change when implementing a 1st line of defense risk management program? Engage staff early in the process, clearly communicate the benefits, and provide ongoing support and training.

1. What are the legal and regulatory implications of failing to implement effective 1st line of defense risk management? Failure can lead to fines, penalties, reputational damage, and even legal action.

1. How can I integrate 1st line of defense risk management with my organization's overall strategy? Align risk management objectives with business goals, integrate risk considerations into decision-making processes, and regularly review the effectiveness of the program.

Related Articles:

1. "Building a Strong 1st Line of Defense: A Practical Guide": This article offers step-by-step instructions on establishing and implementing a robust 1st line of defense risk management program.

1. "The Role of Technology in Enhancing 1st Line of Defense Risk Management": Explores the use of technology to streamline risk management processes and improve data analysis.

1. "Overcoming Challenges in 1st Line of Defense Risk Management": Addresses common obstacles and provides practical solutions for overcoming them.

1. "Integrating 1st Line of Defense with the Three Lines of Defense Model": Details how the 1st line interacts with the 2nd and 3rd lines for a holistic approach.

1. "Measuring the Effectiveness of 1st Line of Defense Risk Management": Presents key metrics and methods for evaluating program success.

1. "Case Studies in Effective 1st Line of Defense Risk Management": Provides real-world examples of successful risk management initiatives.

1. "The Importance of Risk Culture in 1st Line of Defense Risk Management": Explores how a strong risk culture enhances program effectiveness.

1. "Developing a Risk Appetite Statement for 1st Line of Defense": Focuses on defining acceptable levels

of risk for specific areas of operation.

1. "Regulatory Compliance and 1st Line of Defense Risk Management": Examines how 1st line activities contribute to meeting regulatory obligations.

1st line of defense risk management: *Interest Rate Risk in the Banking Book* PAUL. NEWSON, 2017

1st line of defense risk management: Proactive Risk Management Guy M. Merritt, 2020-10-28 Listed as one of the 30 Best Business Books of 2002 by Executive Book Summaries. Proactive Risk Management's unique approach provides a model of risk that is scalable to any size project or program and easily deployable into any product development or project management life cycle. It offers methods for identifying drivers (causes) of risks so you can manage root causes rather than the symptoms of risks. Providing you with an appropriate quantification of the key factors of a risk allows you to prioritize those risks without introducing errors that render the numbers meaningless. This book stands apart from much of the literature on project risk management in its practical, easy-to-use, fact-based approach to managing all of the risks associated with a project. The depth of actual how-to information and techniques provided here is not available anywhere else.

1st line of defense risk management: World-Class Risk Management Norman Marks, 2015-06-13 Considers why many top executives do not link risk management to organisational effectiveness. Examines how risk relates to strategy-setting and identifies each risk management activity. Advises that risk is an integral part of day-to-day management rather than a periodic exercise.

1st line of defense risk management: HBR Guide to Making Better Decisions Harvard Business Review, 2020-02-11 Learn how to make better; faster decisions. You make decisions every day--from prioritizing your to-do list to choosing which long-term innovation projects to pursue. But most decisions don't have a clear-cut answer, and assessing the alternatives and the risks involved can be overwhelming. You need a smarter approach to making the best choice possible. The HBR Guide to Making Better Decisions provides practical tips and advice to help you generate more-creative ideas, evaluate your alternatives fairly, and make the final call with confidence. You'll learn how to: Overcome the cognitive biases that can skew your thinking Look at problems in new ways Manage the trade-offs between options Balance data with your own judgment React appropriately when you've made a bad choice Communicate your decision--and overcome any resistance Arm yourself with the advice you need to succeed on the job, from a source you trust. Packed with how-to essentials from leading experts, the HBR Guides provide smart answers to your most pressing work challenges.

1st line of defense risk management: Risk, Uncertainty and Profit Frank H. Knight, 2006-11-01 A timeless classic of economic theory that remains fascinating and pertinent today, this is Frank Knight's famous explanation of why perfect competition cannot eliminate profits, the important differences between risk and uncertainty, and the vital role of the entrepreneur in profitmaking. Based on Knight's PhD dissertation, this 1921 work, balancing theory with fact to come to stunning insights, is a distinct pleasure to read. FRANK H. KNIGHT (1885-1972) is considered by some the greatest American scholar of economics of the 20th century. An economics

professor at the University of Chicago from 1927 until 1955, he was one of the founders of the Chicago school of economics, which influenced Milton Friedman and George Stigler.

1st line of defense risk management: *Why Don't We Defend Better?* Robert Sloan, Richard Warner, 2019-07-05 The wave of data breaches raises two pressing questions: Why don’t we defend our networks better? And, what practical incentives can we create to improve our defenses? Why Don't We Defend Better?: Data Breaches, Risk Management, and Public Policy answers those questions. It distinguishes three technical sources of data breaches corresponding to three types of vulnerabilities: software, human, and network. It discusses two risk management goals: business and consumer. The authors propose mandatory anonymous reporting of information as an essential step toward better defense, as well as a general reporting requirement. They also provide a systematic overview of data breach defense, combining technological and public policy considerations. Features Explains why data breach defense is currently often ineffective Shows how to respond to the increasing frequency of data breaches Combines the issues of technology, business and risk management, and legal liability Discusses the different issues faced by large versus small and medium-sized businesses (SMBs) Provides a practical framework in which public policy issues about data breaches can be effectively addressed

1st line of defense risk management: The Legal Risk Management Handbook Matthew Whalley, Chris Guzelian, 2016-12-03 Legal risk covers all areas of business where regulation and the law impact on operations and decisions. From risks arising from contract drafting and management, through to regulators' new focus on conduct, as well as compliance, regulatory and dispute risks, the effective management of legal risk is key for organizations that want to maximise value while minimizing cost and exposure to legal losses. The Legal Risk Management Handbook is a practical guide to making sure your business is legal, protected and making the most of its opportunities. Written by experts in law and risk management, this highly practical guide sets out a clear definition for legal risk and a framework for its management. Covering the full spectrum of legal risks that international businesses can face, it translates legal concepts into clear mitigatory actions. Whether you are an in-house lawyer needing a clear approach to managing risk in your areas of influence, or a member of the risk management function needing a jargon-free guide to your company's legal responsibilities, you will find authoritative insight and guidance. Containing case studies from international businesses and real-life insights from those at the coal-face of legal risk management, The Legal Risk Management Handbook is essential reading for everyone who needs a better understanding of this important business topic. Now includes online resources: author-recorded lectures that align with the book and the Legal Risk Management course at Texas A&M School of Law, U.S.

1st line of defense risk management: Understanding and Managing Model Risk Massimo Morini, 2011-10-20 A guide to the validation and risk management of quantitative models used for pricing and hedging Whereas the majority of quantitative finance books focus on mathematics and risk management books focus on regulatory aspects, this book addresses the elements missed by this literature--the risks of the models themselves. This book starts from regulatory issues, but translates them into practical suggestions to reduce the likelihood of model losses, basing model risk and validation on market experience and on a wide range of real-world examples, with a high level of detail and precise operative indications.

1st line of defense risk management: *Metrics and Methods for Security Risk Management* Carl Young, 2010-08-21 Security problems have evolved in the corporate world because of technological changes, such as using the Internet as a means of communication. With this, the creation, transmission, and storage of information may represent security problem. Metrics and Methods for Security Risk Management is of interest, especially since the 9/11 terror attacks, because it addresses the ways to manage risk security in the corporate world. The book aims to provide information about the fundamentals of security risks and the corresponding components, an analytical approach to risk assessments and mitigation, and quantitative methods to assess the risk components. In addition, it also discusses the physical models, principles, and quantitative methods

needed to assess the risk components. The by-products of the methodology used include security standards, audits, risk metrics, and program frameworks. Security professionals, as well as scientists and engineers who are working on technical issues related to security problems will find this book relevant and useful. - Offers an integrated approach to assessing security risk - Addresses homeland security as well as IT and physical security issues - Describes vital safeguards for ensuring true business continuity

1st line of defense risk management: Risk Management and Assessment Jorge Rocha, Sandra Oliveira, César Capinha, 2020-10-14 Risk analysis, risk evaluation and risk management are the three core areas in the process known as 'Risk Assessment'. Risk assessment corresponds to the joint effort of identifying and analysing potential future events, and evaluating the acceptability of risk based on the risk analysis, while considering influencing factors. In short, risk assessment analyses what can go wrong, how likely it is to happen and, if it happens, what are the potential consequences. Since risk is a multi-disciplinary domain, this book gathers contributions covering a wide spectrum of topics with regard to their theoretical background and field of application. The work is organized in the three core areas of risk assessment.

1st line of defense risk management: Application of Enterprise Risk Management at Airports , 2012 TRB's Airport Cooperative Research Program (ACRP) Report 74: Application of Enterprise Risk Management at Airports summarizes the principles and benefits of enterprise risk management (ERM) and its application to airports. The report discusses implementation of the iterative ERM process, including roles and responsibilities from airport governing boards to all staff members. The project that developed ACRP Report 74 also developed an electronic tool that can be used to support the ERM process by creating a risk score and a risk map that can be used to identify mitigation strategies. The tool is included in CD-ROM format with the print version of the report.

1st line of defense risk management: Enterprise Risk Management John R. S. Fraser, Betty Simkins, 2010-01-07 Essential insights on the various aspects of enterprise risk management If you want to understand enterprise risk management from some of the leading academics and practitioners of this exciting new methodology, Enterprise Risk Management is the book for you. Through in-depth insights into what practitioners of this evolving business practice are actually doing as well as anticipating what needs to be taught on the topic, John Fraser and Betty Simkins have sought out the leading experts in this field to clearly explain what enterprise risk management is and how you can teach, learn, and implement these leading practices within the context of your business activities. In this book, the authors take a broad view of ERM, or what is called a holistic approach to ERM. Enterprise Risk Management introduces you to the wide range of concepts and techniques for managing risk in a holistic way that correctly identifies risks and prioritizes the appropriate responses. This invaluable guide offers a broad overview of the different types of techniques: the role of the board, risk tolerances, risk profiles, risk workshops, and allocation of resources, while focusing on the principles that determine business success. This comprehensive resource also provides a thorough introduction to enterprise risk management as it relates to credit, market, and operational risk, as well as the evolving requirements of the rating agencies and their importance to the overall risk management in a corporate setting. Filled with helpful tables and charts, Enterprise Risk Management offers a wealth of knowledge on the drivers, the techniques, the benefits, as well as the pitfalls to avoid, in successfully implementing enterprise risk management. Discusses the history of risk management and more recently developed enterprise risk management practices and how you can prudently implement these techniques within the context of your underlying business activities Provides coverage of topics such as the role of the chief risk officer, the use of anonymous voting technology, and risk indicators and their role in risk management Explores the culture and practices of enterprise risk management without getting bogged down by the mathematics surrounding the more conventional approaches to financial risk management This informative guide will help you unlock the incredible potential of enterprise risk management, which has been described as a proxy for good management.

1st line of defense risk management: Stepping Through Cybersecurity Risk

Management Jennifer L. Bayuk, 2024-03-26 Stepping Through Cybersecurity Risk Management Authoritative resource delivering the professional practice of cybersecurity from the perspective of enterprise governance and risk management. Stepping Through Cybersecurity Risk Management covers the professional practice of cybersecurity from the perspective of enterprise governance and risk management. It describes the state of the art in cybersecurity risk identification, classification, measurement, remediation, monitoring and reporting. It includes industry standard techniques for examining cybersecurity threat actors, cybersecurity attacks in the context of cybersecurity-related events, technology controls, cybersecurity measures and metrics, cybersecurity issue tracking and analysis, and risk and control assessments. The text provides precise definitions for information relevant to cybersecurity management decisions and recommendations for collecting and consolidating that information in the service of enterprise risk management. The objective is to enable the reader to recognize, understand, and apply risk-relevant information to the analysis, evaluation, and mitigation of cybersecurity risk. A well-rounded resource, the text describes both reports and studies that improve cybersecurity decision support. Composed of 10 chapters, the author provides learning objectives, exercises and quiz questions per chapter in an appendix, with quiz answers and exercise grading criteria available to professors. Written by a highly qualified professional with significant experience in the field, Stepping Through Cybersecurity Risk Management includes information on: Threat actors and networks, attack vectors, event sources, security operations, and CISO risk evaluation criteria with respect to this activity Control process, policy, standard, procedures, automation, and guidelines, along with risk and control self assessment and compliance with regulatory standards Cybersecurity measures and metrics, and corresponding key risk indicators The role of humans in security, including the “three lines of defense” approach, auditing, and overall human risk management Risk appetite, tolerance, and categories, and analysis of alternative security approaches via reports and studies Providing comprehensive coverage on the topic of cybersecurity through the unique lens of perspective of enterprise governance and risk management, Stepping Through Cybersecurity Risk Management is an essential resource for professionals engaged in compliance with diverse business risk appetites, as well as regulatory requirements such as FFIEC, HIIPAA, and GDPR, as well as a comprehensive primer for those new to the field. A complimentary forward by Professor Gene Spafford explains why “This book will be helpful to the newcomer as well as to the hierophants in the C-suite. The newcomer can read this to understand general principles and terms. The C-suite occupants can use the material as a guide to check that their understanding encompasses all it should.”

1st line of defense risk management: *Implementing Enterprise Risk Management* James Lam, 2017-03-13 A practical, real-world guide for implementing enterprise risk management (ERM) programs into your organization Enterprise risk management (ERM) is a complex yet critical issue that all companies must deal with in the twenty-first century. Failure to properly manage risk continues to plague corporations around the world. ERM empowers risk professionals to balance risks with rewards and balance people with processes. But to master the numerous aspects of enterprise risk management, you must integrate it into the culture and operations of the business. No one knows this better than risk management expert James Lam, and now, with Implementing Enterprise Risk Management: From Methods to Applications, he distills more than thirty years' worth of experience in the field to give risk professionals a clear understanding of how to implement an enterprise risk management program for every business. Offers valuable insights on solving real-world business problems using ERM Effectively addresses how to develop specific ERM tools Contains a significant number of case studies to help with practical implementation of an ERM program While Enterprise Risk Management: From Incentives to Controls, Second Edition focuses on the what of ERM, Implementing Enterprise Risk Management: From Methods to Applications will help you focus on the how. Together, these two resources can help you meet the enterprise-wide risk management challenge head on—and succeed.

1st line of defense risk management: HBR's 10 Must Reads on Making Smart Decisions (with featured article "Before You Make That Big Decision..." by Daniel Kahneman, Dan Lovallo, and

Olivier Sibony) Harvard Business Review, Daniel Kahneman, Ram Charan, 2013-03-05 Learn why bad decisions happen to good managers—and how to make better ones. If you read nothing else on decision making, read these 10 articles. We've combed through hundreds of articles in the Harvard Business Review archive and selected the most important ones to help you and your organization make better choices and avoid common traps. Leading experts such as Ram Charan, Michael Mankins, and Thomas Davenport provide the insights and advice you need to: Make bold decisions that challenge the status quo Support your decisions with diverse data Evaluate risks and benefits with equal rigor Check for faulty cause-and-effect reasoning Test your decisions with experiments Foster and address constructive criticism Defeat indecisiveness with clear accountability

1st line of defense risk management: Security Policies and Implementation Issues Robert Johnson, 2014-07-28 This book offers a comprehensive, end-to-end view of information security policies and frameworks from the raw organizational mechanics of building to the psychology of implementation. Written by an industry expert, it presents an effective balance between technical knowledge and soft skills, and introduces many different concepts of information security in clear simple terms such as governance, regulator mandates, business drivers, legal considerations, and much more. With step-by-step examples and real-world exercises, this book is a must-have resource for students, security officers, auditors, and risk leaders looking to fully understand the process of implementing successful sets of security policies and frameworks.--

1st line of defense risk management: *Fraud Risk Assessment* Tommie W. Singleton, Aaron J. Singleton, 2011-04-12 Praise for the Fourth Edition of Fraud Auditing and Forensic Accounting Tommie and Aaron Singleton have made important updates to a book I personally rely very heavily upon: Fraud Auditing and Forensic Accounting (FAFA). In the newest edition, they take difficult topics and explain them in straightforward actionable language. All my students benefitted from reading the third edition of the FAFA to better understand the issues and area of fraud and forensic accounting. With their singular focus on understandability and practicality, this Fourth Edition of the book makes a very important contribution for academics, researchers, practitioners, and students. Bravo!—Dr. Timothy A. Pearson, Director, Division of Accounting, West Virginia University, Executive Director, Institute for Fraud Prevention Finally someone has written a book that combines fraud examination and forensic accounting. The authors have clearly explained both in their earlier edition and now they have enhanced the first with additional materials. The order in which the material is presented is easy to grasp and logically follows the 'typical' fraud examination from the awareness that something is wrong to the court case. The explanatory materials presented aid this effort by being both well placed within the book and relevant to the narrative. —Dr. Douglas E. Ziegenfuss, Chair and Professor, Department of Accounting, Old Dominion University Fraud Auditing and Forensic Accounting is a masterful compilation of the concepts found in this field. The organization of the text with the incorporation of actual cases, facts, and figures provides a logical and comprehensive basis for learning the intricacies of fraud examination and forensic accounting. The authors successfully blend the necessary basics with advanced principles in a manner that makes the book an outstanding resource for students and professionals alike.—Ralph Q. Summerford, President of Forensic/Strategic Solutions, PC

1st line of defense risk management: *Governance, Ethics, Risk Management, Internal Control* Campuswise, 2020-06-19 The primary objective of this book is to help students understand the course subject.

1st line of defense risk management: Rational Cybersecurity for Business Dan Blum, 2020-06-27 Use the guidance in this comprehensive field guide to gain the support of your top executives for aligning a rational cybersecurity plan with your business. You will learn how to improve working relationships with stakeholders in complex digital businesses, IT, and development environments. You will know how to prioritize your security program, and motivate and retain your team. Misalignment between security and your business can start at the top at the C-suite or happen at the line of business, IT, development, or user level. It has a corrosive effect on any security project it touches. But it does not have to be like this. Author Dan Blum presents valuable lessons

learned from interviews with over 70 security and business leaders. You will discover how to successfully solve issues related to: risk management, operational security, privacy protection, hybrid cloud management, security culture and user awareness, and communication challenges. This book presents six priority areas to focus on to maximize the effectiveness of your cybersecurity program: risk management, control baseline, security culture, IT rationalization, access control, and cyber-resilience. Common challenges and good practices are provided for businesses of different types and sizes. And more than 50 specific keys to alignment are included. What You Will Learn Improve your security culture: clarify security-related roles, communicate effectively to businesspeople, and hire, motivate, or retain outstanding security staff by creating a sense of efficacy Develop a consistent accountability model, information risk taxonomy, and risk management framework Adopt a security and risk governance model consistent with your business structure or culture, manage policy, and optimize security budgeting within the larger business unit and CIO organization IT spend Tailor a control baseline to your organization’s maturity level, regulatory requirements, scale, circumstances, and critical assets Help CIOs, Chief Digital Officers, and other executives to develop an IT strategy for curating cloud solutions and reducing shadow IT, building up DevSecOps and Disciplined Agile, and more Balance access control and accountability approaches, leverage modern digital identity standards to improve digital relationships, and provide data governance and privacy-enhancing capabilities Plan for cyber-resilience: work with the SOC, IT, business groups, and external sources to coordinate incident response and to recover from outages and come back stronger Integrate your learnings from this book into a quick-hitting rational cybersecurity success plan Who This Book Is For Chief Information Security Officers (CISOs) and other heads of security, security directors and managers, security architects and project leads, and other team members providing security leadership to your business

1st line of defense risk management: Security Risk Assessment and Management Betty E. Biringer, Rudolph V. Matalucci, Sharon L. O'Connor, 2007-03-12 Proven set of best practices for security risk assessment and management, explained in plain English This guidebook sets forth a systematic, proven set of best practices for security risk assessment and management of buildings and their supporting infrastructures. These practices are all designed to optimize the security of workplace environments for occupants and to protect the interests of owners and other stakeholders. The methods set forth by the authors stem from their research at Sandia National Laboratories and their practical experience working with both government and private facilities. Following the authors' step-by-step methodology for performing a complete risk assessment, you learn to: Identify regional and site-specific threats that are likely and credible Evaluate the consequences of these threats, including loss of life and property, economic impact, as well as damage to symbolic value and public confidence Assess the effectiveness of physical and cyber security systems and determine site-specific vulnerabilities in the security system The authors further provide you with the analytical tools needed to determine whether to accept a calculated estimate of risk or to reduce the estimated risk to a level that meets your particular security needs. You then learn to implement a risk-reduction program through proven methods to upgrade security to protect against a malicious act and/or mitigate the consequences of the act. This comprehensive risk assessment and management approach has been used by various organizations, including the U.S. Bureau of Reclamation, the U.S. Army Corps of Engineers, the Bonneville Power Administration, and numerous private corporations, to assess and manage security risk at their national infrastructure facilities. With its plain-English presentation coupled with step-by-step procedures, flowcharts, worksheets, and checklists, you can easily implement the same proven approach and methods for your organization or clients. Additional forms and resources are available online at www.wiley.com/go/securityrisk.

1st line of defense risk management: Model Risk Management with SAS SAS, 2020-06-29 Cut through the complexity of model risk management with a guide to solutions from SAS! There is an increasing demand for more model governance and model risk awareness. At the same time, high-performing models are expected to be deployed faster than ever. SAS Model Risk Management

is a user-friendly, web-based application that facilitates the capture and life cycle management of statistical model-related information. It enables all stakeholders in the model life cycle — developers, validators, internal audit, and management – to get overview reports as well as detailed information in one central place. Model Risk Management with SAS introduces you to the features and capabilities of this software, including the entry, collection, transfer, storage, tracking, and reporting of models that are drawn from multiple lines of business across an organization. This book teaches key concepts, terminology, and base functionality that are integral to SAS Model Risk Management through hands-on examples and demonstrations. With this guide to SAS Model Risk Management, your organization can be confident it is making fact-based decisions and mitigating model risk.

1st line of defense risk management: Corporate Defense and the Value Preservation Imperative Sean Lyons, 2016-09-19 This is the first book to finally address the umbrella term corporate defense, and to explain how an integrated corporate defense program can help an organization address both value creation and preservation. The book explores the value preservation imperative, which represents an organization's obligation to implement a comprehensive corporate defense program in order to deliver long-term sustainable value to its stakeholders. For the first time the reader is provided with a complete picture of how corporate defense operates all the way from the boardroom to the front-lines, and vice versa. It provides comprehensive guidance on how to implement a robust corporate defense program by addressing this challenge from strategic, tactical, and operational perspectives. This arrangement provides readers with a holistic view of corporate defense and incorporates the management of the eight critical corporate defense components. It includes how an organization needs to integrate its governance, risk, compliance, intelligence, security, resilience, controls and assurance activities within its corporate defense program. The book addresses the corporate defense requirement from various perspectives and helps readers to understand the critical interconnections and inter-dependencies which exist at strategic, tactical, and operational levels. It facilitates the reader in comprehending the importance of appropriately prioritizing corporate defense at a strategic level, while also educating the reader in the importance of managing corporate defense at a tactical level, and executing corporate defense activities at an operational level. Finally the book looks at the business case for implementing a robust corporate defense program and the value proposition of introducing a truly world class approach to addressing the value preservation imperative. Cut and paste this link (https://m.youtube.com/watch?v=u5R_eOPNHbI) to learn more about a corporate defense program and how the book will help you implement one in your organization.

1st line of defense risk management: Machine Learning for Auditors Maris Sekar, 2022-02-27 Use artificial intelligence (AI) techniques to build tools for auditing your organization. This is a practical book with implementation recipes that demystify AI, ML, and data science and their roles as applied to auditing. You will learn about data analysis techniques that will help you gain insights into your data and become a better data storyteller. The guidance in this book around applying artificial intelligence in support of audit investigations helps you gain credibility and trust with your internal and external clients. A systematic process to verify your findings is also discussed to ensure the accuracy of your findings. Machine Learning for Auditors provides an emphasis on domain knowledge over complex data science know how that enables you to think like a data scientist. The book helps you achieve the objectives of safeguarding the confidentiality, integrity, and availability of your organizational assets. Data science does not need to be an intimidating concept for audit managers and directors. With the knowledge in this book, you can leverage simple concepts that are beyond mere buzz words to practice innovation in your team. You can build your credibility and trust with your internal and external clients by understanding the data that drives your organization. What You Will Learn Understand the role of auditors as trusted advisors Perform exploratory data analysis to gain a deeper understanding of your organization Build machine learning predictive models that detect fraudulent vendor payments and expenses Integrate data analytics with existing and new technologies Leverage storytelling to communicate and validate your

findings effectively Apply practical implementation use cases within your organization Who This Book Is For AI Auditing is for internal auditors who are looking to use data analytics and data science to better understand their organizational data. It is for auditors interested in implementing predictive and prescriptive analytics in support of better decision making and risk-based testing of your organizational processes.

1st line of defense risk management: Security Risk Management Body of Knowledge Julian Talbot, Miles Jakeman, 2011-09-20 A framework for formalizing risk management thinking in today¿s complex business environment Security Risk Management Body of Knowledge details the security risk management process in a format that can easily be applied by executive managers and security risk management practitioners. Integrating knowledge, competencies, methodologies, and applications, it demonstrates how to document and incorporate best-practice concepts from a range of complementary disciplines. Developed to align with International Standards for Risk Management such as ISO 31000 it enables professionals to apply security risk management (SRM) principles to specific areas of practice. Guidelines are provided for: Access Management; Business Continuity and Resilience; Command, Control, and Communications; Consequence Management and Business Continuity Management; Counter-Terrorism; Crime Prevention through Environmental Design; Crisis Management; Environmental Security; Events and Mass Gatherings; Executive Protection; Explosives and Bomb Threats; Home-Based Work; Human Rights and Security; Implementing Security Risk Management; Intellectual Property Protection; Intelligence Approach to SRM; Investigations and Root Cause Analysis; Maritime Security and Piracy; Mass Transport Security; Organizational Structure; Pandemics; Personal Protective Practices; Psych-ology of Security; Red Teaming and Scenario Modeling; Resilience and Critical Infrastructure Protection; Asset-, Function-, Project-, and Enterprise-Based Security Risk Assessment; Security Specifications and Postures; Security Training; Supply Chain Security; Transnational Security; and Travel Security.

1st line of defense risk management: Data Risk Management: Essentials to implement an Enterprise Control Environment Tejasvi Addagada , 2022-07-08 About the book (in English for listing the book on online portals in 100-150 words): You must hear this often if you manage any kind of risk - risk and value go together. And that's true, of course for data! Both data and its infrastructure must be managed for their benefits and risks. The purpose of the book is to elaborate on this need to formalize data risk management. Today, regulations drive enterprises to assess data related risks. Prioritizing and managing data associated with financial or operational risk has been the corner-stone of most regulations like BCBS, CCAR, GDPR to name a few. Nevertheless, data risks can extend beyond regulations to improve existing control environments in companies. By doing so, we will maximize the potential of data capabilities to reach 100%. Through structural alignment within the board and formalizing a data-risk function, the book focuses on managing data risks. Furthermore, the book explains quantitative and qualitative approaches to data risk assessments along with popular tools and techniques. Also, Tejasvi discusses a proven approach to managing data risks called capability-based assessment. As a technique, this can also be applied to data risk planning and formulating a data risk strategy. Twenty data risks and privacy risks are provided in this book by way of examples. These are accompanied by details such as a risk statements, scenarios, causes, and categories of impact if the data risks are to manifest

1st line of defense risk management: Banking conduct and culture : a call for sustained and comprehensive reform , 2015

1st line of defense risk management: *Solving for Project Risk Management: Understanding the Critical Role of Uncertainty in Project Management* Christian B. Smart, 2020-11-23 Risk is real—but you can manage it with this hard-hitting guide to reducing risk on any project, in any industry All projects, large and small, are subject to various risks. But the failure to manage inherent risk with diligence and know-how can lead to devastating consequences for an organization. In this comprehensive hands-on guide, a renowned expert in the field provides everything organizations need to conduct project risk management the right way. Why do so many projects come in over schedule and over budget? How do projected expenditures and schedules line up with reality? How

can you accurately assess risk to mitigate financial disaster? Through a methodical, statistics-based approach, Christian B. Smart reveals: The enduring problem of cost and schedule growth How rigorous project risk management can reduce the impact of uncertainty The systematic tendency to underestimate risk—and how to avoid it Ways to accurately assess confidence levels in project risk management The need for proper risk management at the portfolio level The author lays out common problems and explains how to effectively solve them. And while he employs a wealth of illustrative charts, graphs, and statistics, he presents the material in an accessible style, and peppers the text with powerful personal anecdotes. Ideal for project managers, business analysts, and senior decision makers in both the public and private sectors, Solving for Project Risk Management offers everything you need to ensure your projects run smoothly, on budget, and deliver the expected outcomes.

1st line of defense risk management: Capital Failure Nicholas Morris, David Vines, 2014 Argues that the trust-intensive nature of the financial services industry makes it essential to rebuild trustworthiness in the provision of financial services. It considers the lack of trust that emerged following deregulation of the financial sector and examines what is needed to rebuild trustworthiness.

1st line of defense risk management: Enterprise Risk Management James Lam, 2014-01-06 A fully revised second edition focused on the best practices of enterprise risk management Since the first edition of Enterprise Risk Management: From Incentives to Controls was published a decade ago, much has changed in the worlds of business and finance. That's why James Lam has returned with a new edition of this essential guide. Written to reflect today's dynamic market conditions, the Second Edition of Enterprise Risk Management: From Incentives to Controls clearly puts this discipline in perspective. Engaging and informative, it skillfully examines both the art as well as the science of effective enterprise risk management practices. Along the way, it addresses the key concepts, processes, and tools underlying risk management, and lays out clear strategies to manage what is often a highly complex issue. Offers in-depth insights, practical advice, and real-world case studies that explore the various aspects of ERM Based on risk management expert James Lam's thirty years of experience in this field Discusses how a company should strive for balance between risk and return Failure to properly manage risk continues to plague corporations around the world. Don't let it hurt your organization. Pick up the Second Edition of Enterprise Risk Management: From Incentives to Controls and learn how to meet the enterprise-wide risk management challenge head on, and succeed.

1st line of defense risk management: *The Fourth Industrial Revolution* Klaus Schwab, 2017-01-03 World-renowned economist Klaus Schwab, Founder and Executive Chairman of the World Economic Forum, explains that we have an opportunity to shape the fourth industrial revolution, which will fundamentally alter how we live and work. Schwab argues that this revolution is different in scale, scope and complexity from any that have come before. Characterized by a range of new technologies that are fusing the physical, digital and biological worlds, the developments are affecting all disciplines, economies, industries and governments, and even challenging ideas about what it means to be human. Artificial intelligence is already all around us, from supercomputers, drones and virtual assistants to 3D printing, DNA sequencing, smart thermostats, wearable sensors and microchips smaller than a grain of sand. But this is just the beginning: nanomaterials 200 times stronger than steel and a million times thinner than a strand of hair and the first transplant of a 3D printed liver are already in development. Imagine “smart factories” in which global systems of manufacturing are coordinated virtually, or implantable mobile phones made of biosynthetic materials. The fourth industrial revolution, says Schwab, is more significant, and its ramifications more profound, than in any prior period of human history. He outlines the key technologies driving this revolution and discusses the major impacts expected on government, business, civil society and individuals. Schwab also offers bold ideas on how to harness these changes and shape a better future—one in which technology empowers people rather than replaces them; progress serves society rather than disrupts it; and in which innovators respect moral and ethical boundaries rather

than cross them. We all have the opportunity to contribute to developing new frameworks that advance progress.

1st line of defense risk management: Risk Management Handbook Federal Aviation Administration, 2012-07-03 Every day in the United States, over two million men, women, and children step onto an aircraft and place their lives in the hands of strangers. As anyone who has ever flown knows, modern flight offers unparalleled advantages in travel and freedom, but it also comes with grave responsibility and risk. For the first time in its history, the Federal Aviation Administration has put together a set of easy-to-understand guidelines and principles that will help pilots of any skill level minimize risk and maximize safety while in the air. The Risk Management Handbook offers full-color diagrams and illustrations to help students and pilots visualize the science of flight, while providing straightforward information on decision-making and the risk-management process.

1st line of defense risk management: Department of Defense Dictionary of Military and Associated Terms United States. Joint Chiefs of Staff, 1979

1st line of defense risk management: QFINANCE: The Ultimate Resource, 4th edition Bloomsbury Publishing, 2013-09-26 QFINANCE: The Ultimate Resource (4th edition) offers both practical and thought-provoking articles for the finance practitioner, written by leading experts from the markets and academia. The coverage is expansive and in-depth, with key themes which include balance sheets and cash flow, regulation, investment, governance, reputation management, and Islamic finance encompassed in over 250 best practice and thought leadership articles. This edition will also comprise key perspectives on environmental, social, and governance (ESG) factors -- essential for understanding the long-term sustainability of a company, whether you are an investor or a corporate strategist. Also included: Checklists: more than 250 practical guides and solutions to daily financial challenges; Finance Information Sources: 200+ pages spanning 65 finance areas; International Financial Information: up-to-date country and industry data; Management Library: over 130 summaries of the most popular finance titles; Finance Thinkers: 50 biographies covering their work and life; Quotations and Dictionary.

1st line of defense risk management: Financial Risk Management For Dummies Aaron Brown, 2015-12-14 Take the risk out of financial risk management Written by bestselling author and past winner of the GARP Award's Risk Manager of the Year, Aaron Brown, Financial Risk Management For Dummies offers thorough and accessible guidance on successfully managing and controlling financial risk within your company. Through easy-to-follow instruction, you'll find out how to manage risk, firstly by understanding it, and then by taking control of it. Plus, you'll discover how to measure and value financial risk, set limits, stop losses, control drawdowns and hedge bets. Financial risk management uses financial instruments to manage exposure to risk within firms, large and small—particularly credit risk and market risk. From managing and measuring risk to working in financial institutions and knowing how to communicate risk to your company and clients, Financial Risk Management For Dummies makes it easy to make sense of the management of risk when working in various different financial institutions and concludes by covering the topic of how to communicate risk — how to report it properly and how to deal with and comply with all of the regulations. Covers managing risk and working as a financial risk manager Provides everything you need to know about measuring financial risk Walks you through working in financial institutions Demonstrates how to communicate risk If you work in the financial sector and want to make financial risk management your mission, you've come to the right place!

1st line of defense risk management: *Mastering Operational Risk* Tony Blunden, John Thirlwell, 2012-09-26 Operational risk is a constant concern for all businesses. It goes far beyond operations and process to encompass all aspects of business risk, including strategic and reputational risks. Within financial services, it became codified by the Basel Committee on Banking Supervision in the 1990s. It is something that needs to be taken seriously by all those involved in running, managing and leading companies. Mastering Operational Risk is a comprehensive guide which takes you from the basic elements of operational risk, through to its advanced applications.

Focusing on practical aspects, the book gives you everything you need to help you understand what operational risk is, how it affects you and your business and provides a framework for managing it. Mastering Operational Risk: Shows you how to make the business case for operational risk, and how to develop effective company-wide policies Covers the essential basic concepts through to advanced managements practices Uses examples and case studies which cover the pitfalls and explains how to avoid them Provides scenario analysis and modelling techniques for you to apply to your business Operational risk arises in all businesses. It is a broad term and can relate to internal processes, people, and systems, as well as external events. All listed companies, charities and the public sector must make risk judgements and assessments and company managers have an increasing responsibility to ensure that these assessments are robust and that risk management is at the heart of their organisations. In this practical guide, Tony Blunden and John Thirlwell, recognised experts in risk management, show you how to manage operational risk and show why operational risk management really will add benefits to your business. Mastering Operational Risk includes: The business case for operational risk Risk and control assessment How to use operational risk indicators Reporting operational risk Modelling and stress-testing operational risk Business continuity and insurance Managing people risk Containing reputational damage

1st line of defense risk management: Auditor Essentials Hernan Murdock, 2018-09-21 Internal auditors must know many concepts, techniques, control frameworks, and remain knowledgeable despite the many changes occurring in the marketplace and their profession. This easy to use reference makes this process easier and ensures auditors can obtain needed information quickly and accurately. This book consists of 100 topics, concepts, tips, tools and techniques that relate to how internal auditors interact with internal constitutencies and addresses a variety of technical and non-technical subjects. Non-auditors have an easy-to-use guide that increases their understanding of what internal auditors do and how, making it easier for them to partner with them more effectively.

1st line of defense risk management: Performance Management for the Oil, Gas, and Process Industries Robert Bruce Hey, 2017-04-06 Performance Management for the Oil, Gas, and Process Industries: A Systems Approach is a practical guide on the business cycle and techniques to undertake step, episodic, and breakthrough improvement in performance to optimize operating costs. Like many industries, the oil, gas, and process industries are coming under increasing pressure to cut costs due to ongoing construction of larger, more integrated units, as well as the application of increasingly stringent environmental policies. Focusing on the 'value adder' or 'revenue generator' core system and the company direction statement, this book describes a systems approach which assures significant sustainable improvements in the business and operational performance specific to the oil, gas, and process industries. The book will enable the reader to: utilize best practice principles of good governance for long term performance enhancement; identify the most significant performance indicators for overall business improvement; apply strategies to ensure that targets are met in agreed upon time frames. - Describes a systems approach which assures significant sustainable improvements in the business and operational performance specific to the oil, gas, and process industries - Helps readers set appropriate and realistic short-term/ long-term targets with a pre-built facility health checker - Elucidates the relationship between PSM, OHS, and Asset Integrity with an increased emphasis on behavior-based safety - Discusses specific oil and gas industry issues and examples such as refinery and gas plant performance initiatives and hydrocarbon accounting

1st line of defense risk management: *Bank Asset Liability Management Best Practice* Polina Bardaeva, 2021-04-19 As bankers incorporate more and more complicated and precise calculations and models, a solely mathematical approach will fail to confirm the viability of their business. This book explains how to combine ALM concepts with the emotional intelligence of managers in order to maintain the financial health of a bank, and quickly react to external environment challenges and banks’ microclimate changes. ALM embraces not only balance sheet targets setting, instruments and methodologies to achieve the targets, but also the correct and holistic understanding of processes

that should be set up in a bank to prove its prudency and compliance with internal and external constraints, requirements and limitations and the ongoing continuity of its operations. Bank Asset Liability Management Best Practice delves into the philosophy of ALM, discusses the interrelation of processes inside the bank, and argues that every little change in one aspect of the bank processes has an impact on its other parts. The author discusses the changing role of ALM and its historical and current concepts, its strengths and weaknesses, and future threats and opportunities.

1st line of defense risk management: Risk Culture E. Banks, 2012-09-11 Risk Culture is a practical volume devoted to the qualitative aspects of risk management, including those that should be firmly embedded in the corporate culture. Through descriptions, examples and case studies, the book analyzes weak and strong cultures and proposes a series of structural and behavioral actions to strengthen a company's culture.

1st line of defense risk management: *End-to-end Network Security* Omar Santos, 2008 This title teaches readers how to counter the new generation of complex threats. Adopting this robust security strategy defends against highly sophisticated attacks that can occur at multiple locations in an organization's network.

Additional Resources

abbreviations - When is it proper to abbreviate first to 1st?

Barring cases of extreme abbreviations (where one might use such abbreviations as "t ppl complaind abt t difficulty n reading &c", such as some live internet chat room, or mediaeval ...

"the 1st" or "1st" - English Language & Usage Stack Exchange

a) The United States ranked 1st in Bloomberg's Global Innovation Index. b) The United States ranked the 1st in Bloomberg's Global Innovation Index. I've seen a) in the news, however, it is ...

What do we call the “rd” in “3rd” and the “th” in “9th”?

Aug 23, 2014 · @WS2 In speech, very nearly always. In writing, much less so. I think what may be going on is that one just assumes that “June 1” is pronounced “June First”, or “4 July” as ...

First floor vs ground floor, usage origin - English Language

Apr 10, 2015 · The American convention is that the floor inside a building which is on the ground, is called the first floor and the floor above that is called the second floor and so forth.

meaning - English Language & Usage Stack Exchange

The "first week of April" is the first week that contains any date in April. For example, in the image below the "first week of April" is the week containing the 1st, 2nd, 3rd, and 4th of April. It could ...

abbreviations - When were st, nd, rd, and th, first used - English ...

In English, Wikipedia says these started out as superscripts: 1 st, 2 nd, 3 rd, 4 th, but during the 20 th century they migrated to the baseline: 1st, 2nd, 3rd, 4th. So the practice started during ...

1st hour, 2nd hour, 3rd hour... But how to say "zero"-th hour?

E.g. in School we have 5-7 or 8 hours every day (Math, History, Biology, Chemistry, English etc.). The first hour starts at 8:00 A.M.

Meaning of "by" when used with dates - inclusive or exclusive

Aug 28, 2014 · If, in a contract fr example, the text reads: "X has to finish the work by MM-DD-YYYY", does the "by" include the date or exclude it? In other words, will the work delivered on ...

Understanding "as of", "as at", and "as from"

Stack Exchange Network. Stack Exchange network consists of 183 Q&A communities including Stack Overflow, the largest, most trusted online community for developers to learn, share their ...

“20th century” vs. “20th century” - English Language & Usage ...

To some extent, it depends on the font you are using and how accessible its special features are. If you can do full typesetting, then you probably want to make the th part look different from the ...

abbreviations - When is it proper to abbreviate first to 1st? - English ...

Barring cases of extreme abbreviations (where one might use such abbreviations as "t ppl complaind abt t difficulty n reading &c", such as some live internet chat room, or mediaeval ...

"the 1st" or "1st" - English Language & Usage Stack Exchange

a) The United States ranked 1st in Bloomberg's Global Innovation Index. b) The United States ranked the 1st in Bloomberg's Global Innovation Index. I've seen a) in the news, however, it is like ...

What do we call the “rd” in “3rd” and the “th” in “9th”?

Aug 23, 2014 · @WS2 In speech, very nearly always. In writing, much less so. I think what may be going on is that one just assumes that “June 1” is pronounced “June First”, or “4 July” as “the ...

First floor vs ground floor, usage origin - English Language & Usage ...

Apr 10, 2015 · The American convention is that the floor inside a building which is on the ground, is called the first floor and the floor above that is called the second floor and so forth.

meaning - English Language & Usage Stack Exchange

The "first week of April" is the first week that contains any date in April. For example, in the image below the "first week of April" is the week containing the 1st, 2nd, 3rd, and 4th of April. It could ...

abbreviations - When were st, nd, rd, and th, first used - English ...

In English, Wikipedia says these started out as superscripts: 1 st, 2 nd, 3 rd, 4 th, but during the 20 th century they migrated to the baseline: 1st, 2nd, 3rd, 4th. So the practice started during the ...

1st hour, 2nd hour, 3rd hour... But how to say "zero"-th hour?

E.g. in School we have 5-7 or 8 hours every day (Math, History, Biology, Chemistry, English etc.). The first hour starts at 8:00 A.M.

Meaning of "by" when used with dates - inclusive or exclusive

Aug 28, 2014 · If, in a contract fr example, the text reads: "X has to finish the work by MM-DD-YYYY", does the "by" include the date or exclude it? In other words, will the work delivered on ...

Understanding "as of", "as at", and "as from"
Stack Exchange Network. Stack Exchange network consists of 183 Q&A communities including Stack Overflow, the largest, most trusted online community for developers to learn, share their ...

“20th century” vs. “20th century” - English Language & Usage ...
To some extent, it depends on the font you are using and how accessible its special features are. If you can do full typesetting, then you probably want to make the th part look different from the 20 ...

1st Line Of Defense Risk Management

1st Line Of Defense Risk Management

Related Articles

- 2 topic assessment form b
- 2 year electronics degree
- 2 step equations word problems worksheet

Back to Home