Information Security Fundamentals **allows security professionals to gain a solid understandings of the foundations of the field and the entire range of issues that practitioners must address. This book enables you to understand the key elements that comprise the successful information security program and apply these concepts into your own effort. The book examines the element computer security, employee roles and responsibilities, and common threats. It examines the need for management controls, policies and procedures, and risk analysis, and also presents a comprehensive list of task and objectives that kame up a typical information protection program.**

The volume discusses organizational wide (Tier 1) policies and their documentation, and legal and business requirements. It explains policy format, focusing on global, topic-specific, and application-specific policies. Following a review of asset classification, the book explores access control, the components of physical security, and the foundation and processes of risk analysis and risk management. ***Information Security Fundamentals*** **concludes by describing business continuity planning, including preventive controls, recovery strategies, and ways to conduct a business impact analysis.**

Features :

- **Provides a solid understanding of the foundations of the field and the entire range of issues that practitioners must address**
- **Discusses the legal requirements that impact security policies, including Sarbanes-Oxley, HIPAA, and Gramm-Leach-Bliley Act (GLBA)**
- **Details physical sequrity requirement and controls, and offers a sample physical security policy**
- **Examines elements of the risk analysis process such as asset definition, threat identification occurrence probability, and more**
- **Describes components of business continuity planning, outlining how to conduct a business impact analysis, and how to test a plan**