

enterprise risk management

The Control Professionals

Keeping watch over your best business interests.





enterprise risk management

The Control Professionals

Businesses today face growing IT security compliance obligations and increasing risks to the integrity of their systems. Enterprise Risk Management brings clients the highest level of expertise to assess and address risks, comply with standards and regulations and mitigate risks, using integrated, proven and reasonably priced security services and solutions.



IT Security Services

Information systems provide the back bone for all organizations to conduct their day to day activities. Today, legislators, regulators, investors, and customers are demanding increased IT security. Proactive risk management is critical not only for safeguarding organizational assets and continuity, but also to avoid the legal consequences of failing to meet regulatory requirements or having security breached.

ERM evaluates and mitigates risk by ensuring that the right security infrastructure is in place with the necessary security controls, policies and procedures. ERM provides the following IT security services:

Information Security Design and Implementation

ERM assists organizations to design and implement their security infrastructure by providing the following specific services:

- Design and implementation of security architectures
- Performance of information security risk assessments
- Development of information security policies, standards, procedures and guidelines
- Design and implementation of network security, operating systems & subsystems security, application systems security, E-commerce/E-banking security, and wireless security

Vulnerability Assessment

ERM performs in-depth technical security reviews of hardware and software components supporting the technical infrastructure of an organization.

Penetration Testing

ERM performs live tests of IT security controls using techniques used by hackers. ERM provides the following types of tests:

- External network penetration tests
- Internal network penetration tests
- Wireless network penetration tests
- Application penetration tests
- Social engineering tests





Security Breach Investigation and Remediation

ERM assists organizations to investigate security breaches and resolve IT operational issues related to such incidents.

ERM's services include the following:

- Incident response support
- Assistance with the preservation of evidence
- Forensic investigation
- E-crime expert support

Business Continuity Planning

ERM assists organizations to develop, test and update business continuity plans.

Logwatch

ERM's Logwatch service assists organizations to detect information security problems as well as actual or potential security breaches by performing periodic evaluations of security logs. Specifically, ERM provides the following:

- Guidance to properly configure different types of security logs in order to capture system and user activities that may reveal security problems or breaches
- Remote monitoring and analysis of different security logs tailored to the client's needs and IT platforms
- Periodic generation of reports based on security log analysis

Specialized Security Training

ERM provides security training tailored for each of the following types of employees:

- Management
- IT Personnel
- IT Auditors
- Operational personnel

Thousands of organizations suffer financial losses related to IT security problems every year.

Regulatory Compliance Services

Today, statutes and regulations impose IT controls and security obligations on virtually all industries. Regulatory issues can be complex, technical and time consuming. ERM specializes in compliance services for the following areas:

Gramm Leach Bliley Act (GLBA)

The GLBA requires financial institutions to develop, implement and enforce sound technical, physical and administrative security controls to protect their customers' non-public information from being improperly accessed or misused. ERM provides the following services to assist organizations to comply with GLBA requirements:

- Development and updating of Information Security Programs
- Performance of security risk assessments, vulnerability assessments and network penetration tests
- Providing guidance to implement sound security measures
- Training organizational personnel

Fair and Accurate Credit Transactions Act (FACTA)

Federal regulations issued pursuant to FACTA require organizations to address identity theft risks. The identity theft regulations require organizations in different industries to develop, implement and enforce adequate programs, policies, procedures and controls to prevent, detect and respond to identity theft. ERM provides the following services to assist organizations to comply with the identity theft regulations:

- Development and updating of Identity Theft Prevention Programs
- Performance of periodic risk assessments
- Development of policies and procedures
- Providing guidance to implement sound controls
- Training organizational personnel

Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act established standards for corporate accountability and penalties for corporate wrongdoing. The Act established the Public Company Accounting Oversight Board (PCAOB) to oversee the audits of public companies and to protect the interests of investors. ERM assists organizations with evaluations of their internal controls.





Health Insurance Portability and Accountability Act (HIPAA)

HIPAA requires healthcare organizations to develop, implement and enforce sound technical, physical and administrative security controls to protect health information. ERM provides the following services to assist organizations to comply with HIPAA requirements:

- Development and updating of Information Security Programs
- Performance of security risk assessments, vulnerability assessments and network penetration tests
- Providing guidance to implement sound security measures
- Training organizational personnel

Family Education Rights and Privacy Act (FERPA)

Educational institutions are required by law to protect confidential student information. Student records are now stored digitally, and web based systems are being used to process applications for enrollment, loans and grants. Sensitive bursar information and social security numbers are also stored electronically. ERM's experts assist universities to assess the security of their information systems and to design and implement necessary security controls.

Bank Secrecy Act (BSA)

BSA aims to combat money laundering and terrorist financing. BSA requires financial institutions to implement adequate risk-based record-keeping and monitoring systems to identify, research and report suspicious activity. Failure to comply with BSA may lead to serious sanctions. ERM assists organizations with various aspects of BSA regulations.

Payment Card Industry (PCI)

The Payment Card Industry Data Security Standard (PCI DSS) is managed by the PCI Security Standard Council as a consolidated effort of major credit card brands. The PCI DSS is a worldwide security standard that applies to entities that store, process and transmit credit card transactions. To assist organizations in the implementation and oversight of this standard the PCI Security Standard Council certifies Approved Scanning Vendors (ASVs) and Qualified Security Assessors (QSAs). ERM is certified as an ASV and several ERM professionals are certified QSAs. ERM helps organizations in different industries to comply with the credit card industry security standard.

Prevent sanctions, fines and lawsuits.



IT Audit Services

Organizations have become dependent on integrated technologies and automated systems. Therefore, management is increasingly concerned about performing audits of their internal information systems. However, information systems audit is not the core competency of some organizations. ERM provides a variety of cost-effective IT audit services tailored to each organization's needs including the following:

Internal Information Systems Audit

- Complete or partial outsourcing of the information systems audit department functions
- Assisting internal audit functions to properly address federal regulations and industry standards
- Technical audit training for internal audit personnel
- Special assistance on a project by project basis

Application System Implementation Review

- Pre-implementation application reviews to evaluate management practices, code design, control structures design, security requirements, testing coverage, data conversion integrity, system interfaces and general controls
- Post-implementation application reviews to ensure that systems are operating as intended, meeting organizational objectives and that security and other general controls are adequate

Many organizations would not even know if someone broke into their system.





Forensic Services

Almost all information is now stored in electronic form. Legal cases now frequently involve the use of electronic documents. ERM assists organizations in all matters related to Electronically Stored Information (ESI) from storage to retrieval procedures and analysis in order to ensure that the information can be utilized in court. To assist in this area, ERM provides the following services:

Computer Forensics

ERM assists organizations to conduct comprehensive computer forensics investigations after a security breach, a fraud incident or as part of litigation support. ERM addresses the following aspects:

- Recovery of data from target computers and electronic devices with preservation of the integrity of the evidence
- Secure handling of the retrieved/recovered data
- Identification and analysis of data
- Preparation of forensic reports summarizing the results of the investigation
- Testifying in depositions and court proceedings

E-Discovery

ERM assists organizations and their counsel with the following aspects of e-discovery:

- Complying with e-discovery requirements
- Understanding the information systems infrastructure of the client and the opposing party
- Identifying and preserving relevant ESI of the client
- Identifying the scope, time period, sources and formats of the ESI provided by the client
- Providing information systems expertise needed to deal with the opponent's ESI requests
- Testing whether the opposing party has properly preserved ESI and determining accessibility of ESI
- Analyzing ESI obtained from the opposing party



Risk Management Services

Today's organizations face a wide spectrum of business risks. The use of computer systems and applications introduces risks that may result in the loss of data, or impact the confidentiality, integrity, or availability of data. Such a compromise of data may further result in a dip in performance and increased costs. Managing these risks is crucial.

ERM provides top quality risk management services tailored to meet the needs of individual organizations. ERM's professionals help identify, evaluate and mitigate risks using time-tested tools, techniques and methodologies. Specifically, ERM provides the following services:

Risk Assessments

ERM provides different types of risk assessments covering the following aspects:

- Identification of information assets to be protected
- Classification of information assets
- Identification of all threats, risks, concerns and issues related to information assets
- Evaluation of organizational controls and measures to protect information assets
- Determination of the level to which the information assets are vulnerable to security threats
- Recommendation of required controls and safeguards

Fraud Prevention and Detection

ERM assists organizations to prevent and detect fraud. ERM's services include:

- Performance of a Fraud Risk Assessment tailored to an organization's vulnerabilities
- Development of a comprehensive Anti-Fraud Program based on the results of a risk assessment





Attestation Services

With the increased reliance on information systems, shareholders, management, customers, government and regulatory entities need the assurance that the controls within an organization's automated systems are in place and working properly.

To assist in this area, ERM provides attestation services that assess whether certain management assertions, related to information systems functions and processes, are fairly stated. These types of reviews result in formal opinions, issued under the Statement on Standards for Attestation Engagements (SSAE) guidelines.

Specifically, ERM performs SAS 70 (Statements of Auditing Standards No. 70) reviews to provide a comprehensive description of controls related to specific areas of operation and assess the design and operating effectiveness of control structures.

Voted the Best Boutique Risk Management Firm
by the South Florida CEO magazine.



ERM was founded in Florida in 1998 to meet the high demand for top quality information systems risk management services at reasonable rates.

Our highly trained and experienced professionals are committed to ongoing training and continuous professional development, to ensure that our clients are always ahead of regulations, new technologies and opportunities to not just mitigate risks but eliminate redundancies and unnecessary costs.

ERM's practice of integrated and comprehensive security services provides organizations with the tools they need to address the compliance and risk management issues of today as well as the broader and ever-increasing security challenges of the future.

