ACEXTIC provides premier cyber security consulting services. We partner with your organization to meet your unique IT security needs and commit to a lasting relationship of excellent service. Acextic strives to understand our partners' specific security needs and mobilize the right people, skills, and technologies to implement world-class security solutions

"THE UNTHINKABLE"

Disaster strikes when least expected it, causing heavy losses, confusion and in some cases brings entire organizations to their knees. The information threat landscape that your organization operates in continues to change at a breath-taking speed, more than ever it is imperative that you continually adapt, innovate and respond to the mounting security threats assailing your corporation's assets.

Acextic plans for the best while preparing for the worst by implementing security programs designed to ensure your peace of mind.

WHY ACEXTIC?

- We deliver results you can measure.
- Our performance-based processes are designed to work, and they do.
- Our certified security experts make their experience count for your organization.
- Our strategic mix of technology and business expertise is designed to give you more than what you expect.

WHAT CAN WE CREATE AND MANAGE FOR YOU?

Cyber Security Roadmap framework designs, development

- Security Compliance
- Security Design Architecture

Information Security Risk, Governance and Compliance

Business impact analysis

Disaster Recovery and Business Continuity Solutions

Access Management Solutions

Identity Management Solutions

Security Audits

OUR EXPERTISE INCLUDES:

Vulnerability & risk assessment

- Estimating potential losses

Penetration testing

- Simulated attacks to systems to identify weaknesses

Digital forensics

- The process of uncovering and interpreting electronic data for use in a court of law

Security Audits & Assessment

- A qualitative risk analysis of your organization's IT security posture

Security Training and awareness

- Training and raising of awareness of all organization personnel on IT security

Intrusion Detection systems (IDS)

- An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system

Identity and Access Management

-
- Identity and access management refers to the processes, technologies and policies for managing digital

Network and Data Security

- The protection of the organization's networks and data

Security Monitoring

- Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as the review of: user account logs, application logs, data backup and recovery logs, automated intrusion detection system logs, etc.

Contingency Management Solutions

- Emergency solutions to keep your organizations running when your main systems have been disabled

Authentication Services

- Authentication Service facilitates username/password validation

Security Hardening

- Make organizations system more difficult to penetrate

OUR MISSION

Total security through innovation and proactive processes

SERVICES AND SOLUTIONS

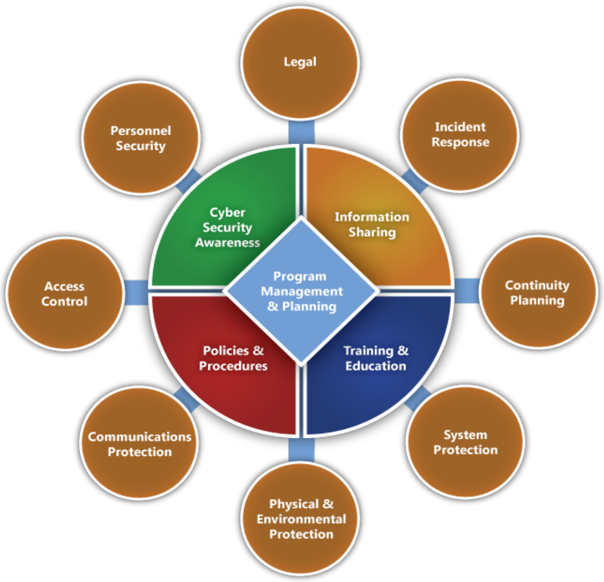
Acextic offers expertise in the following security spectrum:

- Cyber Security Roadmap Framework
- Information Security Risk, Governance and Compliance
- Identity Management
- Intrusion Detection Systems (IDS)
- E-Discover and Digital Forensics
- Network and Data Security
- Business Continuity and Disaster Recovery
- Security Hardening
- Penetration Testing
- Vulnerability and Threat Management
- IT Security Audit and Control Assurance
- Cloud and Bring Your Own Device (BYOD)
- Training and Awareness

CYBER SECURITY ROADMAP FRAMEWORK

Acextic Cyber Security understands the importance of a cyber-security roadmap framework. Outpacing the rapidly evolving cyber threat spectrum demands constant innovation and well-developed framework; online threat levels race higher each day. Around the globe, information and networks are under attack from forces that are more sophisticated, more organized, more dangerous, and better supported than ever before. While we use our security experience and expertise to develop security programs, we understand each client situation and environment is unique and we tailor programs to each client's specific needs. Our security framework includes the following aspects:

- Roadmap assessment and analysis
- Development of security policies, processes and procedures
- Security Design and Architecture
- Roadmap development and implementation
- Security Compliance



Security roadmaps rely on factors that will vary according to the needs of your organization. An effective security roadmap helps identify low hanging fruit, establish quick wins, and quantify the organization's tolerance for improvement over time.

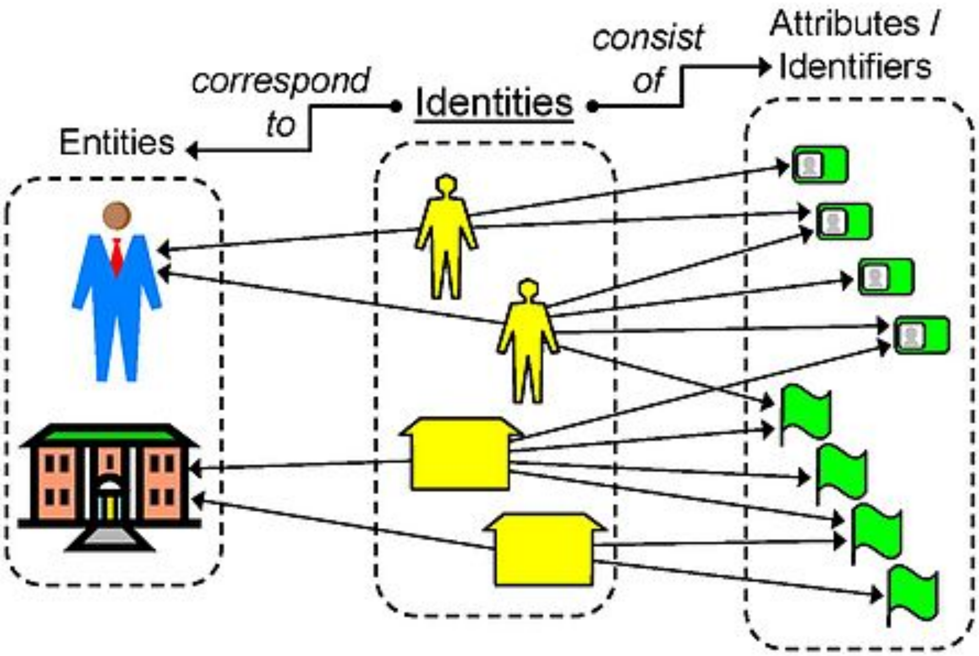
INFORMATION SECURITY RISK, GOVERNANCE AND COMPLIANCE

The quick succession of changes in the information threat landscape overwhelm many companies with the demand to keep up-to-date their governance, risk management and compliance initiatives.
Acextic takes that burden off your shoulders and provides you with the assurance and confidence that your initiatives meet compliance management requirements.

Compliance is not just about developing security policies and satisfying internal audits. It is about establishing and assessing the right risk-based controls that support a comprehensive risk management program. Essentially collecting and communicating this information to facilitate corporate governance, risk, and compliance programs.
Our Security Governance, Risk and Compliance Services ensure your security practices satisfy your business requirements and objectives by identifying compliance gaps, providing recommendations to close the gaps, and providing alternative action plans

IDENTITY MANAGEMENT

Acextic specializes in delivering comprehensive identity-based solutions that provide the tools to manage user identities, their entitlements, and control access to information, all of which are essential for protecting (and sharing) organizational information while meeting regulatory and security requirements. We blend the latest technologies, systems, policies and business processes to deliver integrated identity management solutions that are secure, efficient and increase business value.



INTRUSION DETECTION SYSTEMS (IDS)

Cyber-attacks, by their very nature, constantly evolve. Old-school reliance on detecting known bad behavior doesn't work in this age of cyber warfare. Your security strategy must immediately detect incidents and respond to threats—even the ones that nobody knows about (yet)—to contain system damage and safeguard data.

A big part of doing that is seeing threats and anomalous patterns despite the vast amounts of data that alerting systems produce. Let Acextic deliver proactive defensive security competencies for your data/information assets.

E-DISCOVERY AND DIGITAL FORENSICS

Electronic evidence is fragile and can easily be modified. Cyber criminals and dishonest employees (sometimes even honest ones) can hide, wipe, disguise and destroy it. Acextic helps you stop these individuals in their tracks and prove compliance with regulatory compliance requirements.

NETWORK AND DATA SECURITY

Network defenses are constantly under attack from cyber criminals, organized hacktivists, and even disgruntled ex-employees. In the past five years alone, data breaches have cost companies and individuals nearly $150 billion. Even small vulnerabilities in networks or data center infrastructures can lead to major financial and reputation damage.

Traditional network security testing using penetration methods or canned attacks is outdated and impractical. Only through subjugating your devices, systems, and yourself to live cyber war conditions can you battle-test network defenses, transform IT personnel into cyber warriors, and institute predictive and proactive security processes.

BUSINESS CONTINUITY AND DISASTER RECOVERY

Organizations today need to find knowledgeable experts to help them develop a Business Continuity and Disaster Recovery solution that that delivers results and adheres to ever-changing domestic and international standards. Acextic provides those capabilities and develops for our clients a mature Business Continuity program that increases resiliency in the event of “the unthinkable”. Our solutions are executed by certified Business Continuity professionals with extensive experience in IT operations and management.

The following are part of Acextic’s Business Continuity/Disaster Recovery solution portfolio:

Business Continuity Program Assessment and Development: We evaluate our client’s Business Continuity management program, including review and gap analysis of policy, governance, management, strategy, documentation and testing. Then proceed to provide clients with an improved and possibly better path forward in the development of their Business Continuity program.

Business Impact Analysis: The cornerstone of Business Continuity planning is a Business Impact Analysis our experts do to identify mission critical business functions, recovery time objectives and recovery point objectives to meet all our client's mission critical needs.

Risk Analysis: We provide this critical first step for our clients to identify threats and vulnerabilities and determine the potential for service loss. Followed by a determination of mission impacting threats such as natural disasters (floods, hurricanes), access denial (geopolitical or labor unrest), and loss of environment component systems and communications. Our vulnerability analysis identifies potential exposures and seeks to determine best prevention methods.

Business Continuity Planning and Testing: We establish a variety of plans including work area recovery; supply chain alternate supplier plans; alternate workforce mitigation plans, and other non-IT business continuity plans. We develop the plan and educate and train all client stakeholders to prove the feasibility.

Crisis Management: We build a crisis management program and recommend a team for the development and execution of the plan including: tool selection, process development, and validation testing.

Business Disaster Recovery Services - Planning and Testing: We provide executable Disaster Recovery plans and the coordination and execution of repeatable disaster recovery tests to assure currency and viability of the plans. Disaster Recovery Plan development and maintenance is at the heart of the Business Continuity process and is an on-going activity that assures survival when disaster strikes.

SECURITY HARDENING

Consistent, continual IT security hardening is your organization's most valuable security control. It minimizes network vulnerabilities, reduces the attack surface, and helps your organization avoid becoming a victim of zero-day exploits. Yet most security solutions simply try to limit outside access to the system where your sensitive data resides. This perimeter-centric approach to security leaves your infrastructure vulnerable to attack and compromise.

Our security hardening process includes:

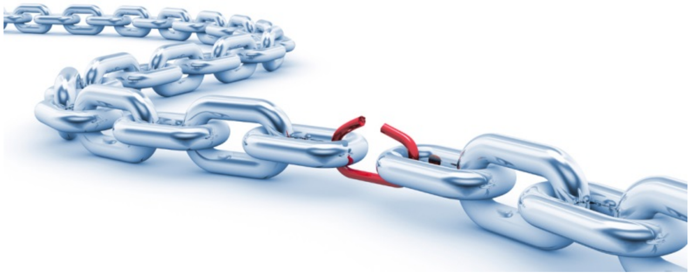
- Continuous system patching
- Configure and manage user privileges
- Remove used user accounts
- Remove unwanted services
- Enforce password complexity and policies
- Close unused open network ports

PENETRATION TESTING

Penetration testing is a critical component to an over-arching information security program. Acextic will battle test your security infrastructure to determine how well it can withstand persistent onslaught.

VULNERABILITY AND THREAT MANAGEMENT

As documented by SANS, "Vulnerabilities are the gateways by which threats are manifested" (1). In other words, a system compromise usually manifest through a weakness found in a system. A vulnerability assessment is a search for these weaknesses/exposures to apply a patch or fix to prevent a compromise. Acextic will pinpoint these vulnerabilities.



Our assessment ensures you manage risk and improve your overall security posture while maximizing business results. Through our vulnerability assessments we provide our customers with a solid understanding of their susceptibility to intrusion via the Internet, while internal assessments address the insider threat and provide valuable information on patch management, system configuration and hardening.

IT SECURITY AUDIT AND CONTROL ASSURANCE

Our security audits are designed to provide third-party objective testing of your organization's internal controls and compliance objectives thereby strengthens your Information Security Program. They will give you an accurate understanding of your security and risk posture, while ensuring compliance with information security best practices. We also offer annual or on-going security audits in the following areas:

- User accounts
- Permissions
- Passwords
- Firewall configuration
- System configuration
- Application stress tests

CLOUD AND BRING YOUR OWN DEVICE (BYOD)

Allowing employees to use their own smartphones through the corporate networks brings new challenges to IT security compliance. With Acextic we can help you develop a robust policy framework which will give you a peace of mind that these devices are not introducing security challenges but benefits to the corporate network.

TRAINING AND AWARENESS

One of the weakest links in your security chain is your organization's employees. While it is usually non-malicious, the uninformed employee can do harm to your network by visiting websites infected with malware, responding to phishing e-mails, storing their login information in an unsecured location, or even giving out sensitive information over the phone when exposed to social engineering. One of the best ways to make sure company employees will not make costly errors regarding information security is to institute company-wide security-awareness training initiatives that include, but are not limited to classroom style training sessions, security awareness website(s), helpful hints via e-mail, or even posters. These methods can help ensure employees have a solid understanding of company security policy, procedure and best practices.

Some of the more important items to cover in your security awareness training may include:

- Organization's security policy
- data classification and handling
- workspace
- Physical Security
- Desktop Security
- Wireless Networks and Security
- Password Security
- Phishing
- Hoaxes
- Malware
  - Viruses
  - Worms
  - Trojans
  - Spyware and Adware
- File Sharing and Copyright

Acextic is in a crucial position to strengthen this weak link in your security protection through training. We have certified experts who can help your employees get informed and certified.

Think cyber security, think Acextic!