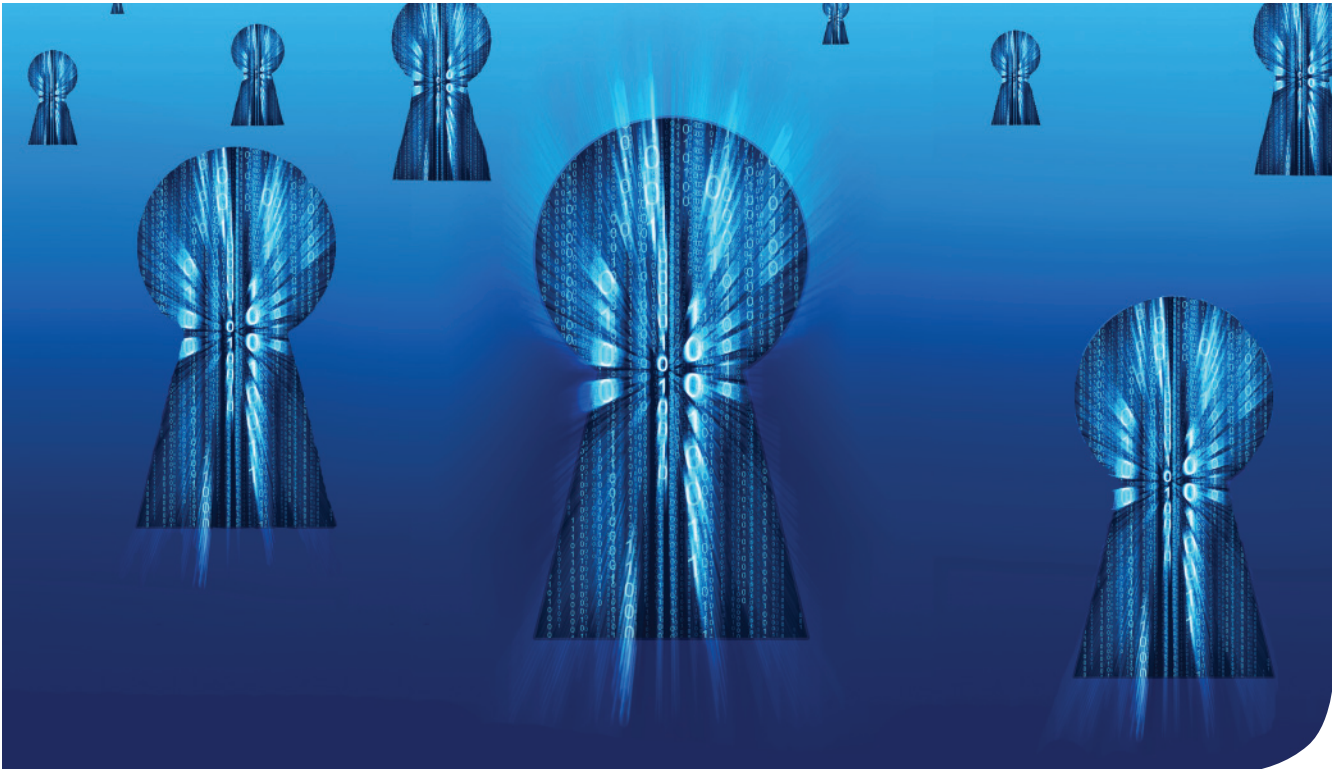




Managing and securing a critical network.



The need for cyber vigilance.



Electronic information and a secure digital network are essential for any modern organization. This is especially true for utilities and a rising concern as utilities upgrade their systems with intelligent devices that may expose them to greater risks. With growing dependency on computer based systems for real-time monitoring and control of their operations, cyber technology and security of these systems has emerged as a major concern.

Cyber standards

NERC CIP and NIST are continually working to set standards for cyber systems, including pending standards for Smart Grid. Increasing reliance on cyber systems to share data has also provided increased opportunities for malicious intrusion. Potential threats make it more critical than ever that organizations protect cyber systems to prevent catastrophic interference with their operations. In particular, real-time monitoring and control network systems are considered critical to the economy, security, and quality of life of the nation. Government agencies and industry organizations are involved in developing standards and best practices, to guide the protection of these critical cyber infrastructures.

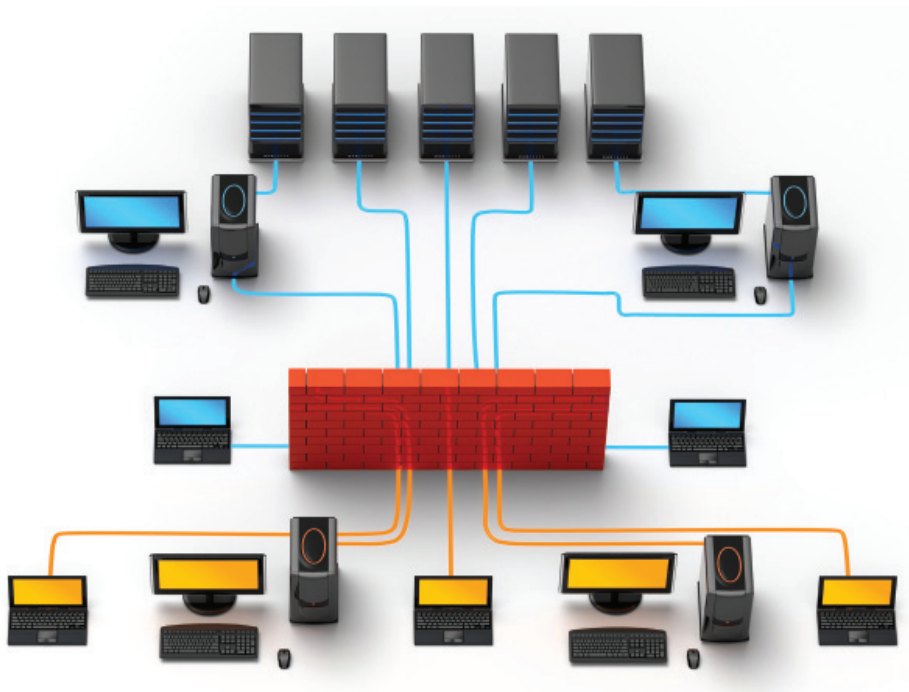
Vulnerabilities

More than 40,000 vulnerabilities have been identified by NIST, and new threats are discovered every day. These threats help to show the ease with which sophisticated hackers or disgruntled employees can disrupt system availability or obtain access to confidential data. Eliminating these risks requires a defense-in-depth strategy beyond standard protective measures such as firewalls and passwords. Protection of computer stored information from unauthorized access, use, or modification is essential to an organization's security. Information integrity, availability, and confidentiality must be considered when considering cyber protection of system or network architectural structures.

Cyber security framework

KEMA cyber security experts provide services that will formalize, enhance and validate your cyber security framework. KEMA services create assurance of IT controls and data security, minimizing potential business risk due to vulnerabilities, threats, and risks to your critical cyber assets and information. Our clients count on us for in-depth technical assessment and gap analysis, system and network architecture design and review, and system hardening measures.

Our methodology is based on a series of related, but separate, areas of concentration allowing us to focus on the specific area of client concern. Our practices are based on the most current relevant standards and best practices. We can assist your organization with adopting or adapting cyber security principles and practices.



Where to start, what to focus on.



KEMA concentrates cyber security services on these key areas of the operations network, including:

Information classification

The heart of a strong information protection program requires many measures in order to appropriately safeguard valuable data, from both internal and external threats, as well as from inadvertent disclosure.

An information classification strategy allows utilities to classify data based on its criticality and implement varying security controls based on the classification level. Classifying information also allows a utility to provide appropriate security on key operational data while avoiding the increased cost of doing so with less critical data.

Critical/Cyber Asset identification

Critical Cyber Assets may be defined as the infrastructure, devices, and applications to provide necessary information and manage operations. This asset identification activity includes identifying, developing or maintaining a critical asset inventory – a necessary foundation for risk analysis in conjunction with other control reviews for prioritization of protection efforts.

Security perimeter definition

Logical and physical boundaries must be properly determined and classified in order to ensure that necessary security controls are in place. This also entails identifying all access points in and out of any logical or physical security perimeters.

Perimeter protection design

The security perimeter must protect against unauthorized electronic or physical access or damage. Software or hardware such as temporary or test devices, applications that connect through firewalls, rogue wireless access points, direct internet access, and more are considered in KEMA's robust design process.

Security policies

Security policies specific to critical operations are necessary to establish sound cyber security practices. These policies are implemented through processes and procedures that secure the organization's critical physical and control assets and information as well as organizational and personnel security.

Monitoring & alerting

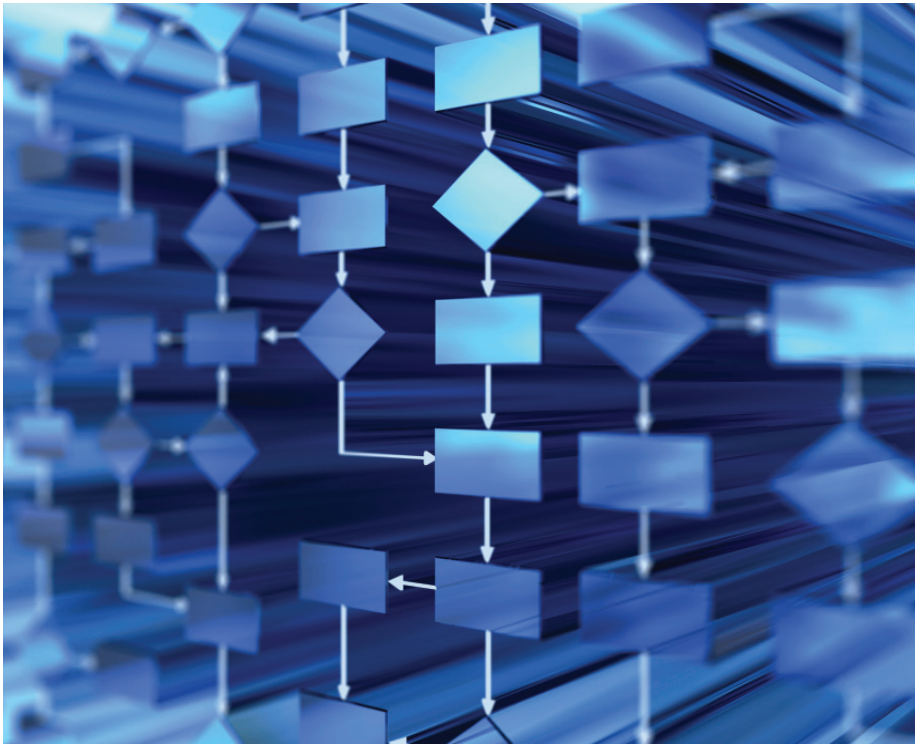
Monitoring is an essential step in establishing successful security. This activity goes beyond reading logs and installing an intrusion detection system (IDS) and/or intrusion prevention system (IPS). It requires the development of a methodology and processes that include the collection, analysis and escalation of indications and warnings to detect and respond to intrusions or security violations. Monitoring supports effective risk management before, during, and after security policies and technology are implemented.

Change management

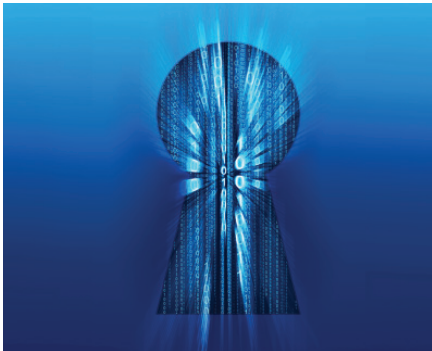
NERC CIP Reliability Standards mandate that electric utilities must have a process for managing changes to critical cyber assets, including hardware and software. These standards can form a basis for best practices for other industries. An organization must take many factors into consideration in the development of its change management model and processes, which can be complicated by legislative changes, shifting economic tides and currents, and organizational member resistance. This process can be especially difficult when dealing with legacy systems.

Information security validation services

The KEMA holistic approach encompasses various testing measures in addition to the traditional vulnerability scanning and penetration testing. While these may be incorporated, other measures can be taken to provide a strong level of confidence in your information security investment.



Comprehensive cyber services.



Assessments: Identify gaps in security best practices.

Cyber Security Audits: Develop mock audits of evidence to show compliance to NERC CIP Reliability Standards and may also include audits of industry best practices.

Gap Remediation: Resolve gaps identified through assessments or audits and the enhancement of flaws in best practices.

Network Security Design & Review: Review the design of existing network architectures or develop the design of a new network to ensure that layered security mechanisms and controls are built into the network

Policy and Procedure Development: Ensure security policy and procedures meet any mandated regulations and/or follow industry best practices.

Incident Response Planning: Ensure client security procedures support continuity of operations during and after a cyber attack.

Configuration Management: Ensure that security controls are maintained as changes are made to the systems, applications, and operational processes.

Forensics: Analyze systems following an event to ensure that all possible data is preserved and a correct interpretation of evidence related to the event is made.

Vulnerability Assessments: Perform controlled tests on critical primary or backup systems to determine if there are open ports and/or unnecessary services enabled. This can also be done as a table-top analysis.

Penetration Tests: Perform tests to validate vulnerabilities against network devices and systems.

Awareness training: Support “defense-in-depth” computer security objectives by enhancing employee awareness of the threats to and vulnerability of computer systems and by encouraging the use of improved computer security practices within the organization.

Knowledge transfer: Ensure staff has necessary skills and knowledge to use technology and perform effective self assessments to help continue the effectiveness of security and compliance solutions and investments.



KEMA's cyber security expertise

KEMA's cyber security team combines experts in IT, utility operations, as well as industry leaders with years of involvement in developing cyber security standards that address cyber risks in total. This makes us uniquely qualified to provide cyber security services to the utility industry. Our integrated approach allows us to provide cost effective and comprehensive consultation to fulfill our clients' cyber security goals. Our expertise and experience enables us to have a clear view of the issues affecting the security of critical cyber assets. KEMA Cyber Security Experts can help develop alternative compensating measures.

About KEMA

KEMA specializes in business and technical consulting, operational support, measurement and inspection, testing and certification. With over 85 years of experience in serving energy and utility clients, KEMA has developed a reputation for integrating deep technical and functional capabilities with management expertise to provide solutions that deliver profitable, reliable, sustainable results. More than 500 energy and utility clients in over 70 countries rely on KEMA's impartial, objective and expert consulting services to plan, build and maintain their strategies for growth.

For additional information, please contact:

KEMA Inc.
4377 County Line Road
Chalfont, PA 18914
Tel: +1 215 997 4500
info.consulting@kema.com
www.kema.com /cyber_security

www.kema.com

