International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Cybersecurity in Bulk Electric Systems: Enhancing Access Management through IT Audits

Suchismita Chatterjee

M.S.-University of North Texas, Cyber Security Product Specilist
Email: *suchi5978[at]gmail.com*

Abstract*: This article explores the role of IT audits in strengthening cybersecurity for Bulk Electric Systems (BES). Focusing on compliance with NERC Critical Infrastructure Protection (CIP) standards, it highlights how IT audits enhance access management practices, mitigate risks, and safeguard sensitive data. Through actionable insights, such as improving access controls, permissions, and authentication methods, IT audits help organizations protect critical infrastructure from unauthorized access and evolving cyber threats.*

Keywords: electric system security, IT audits, NERC CIP standards, cybersecurity frameworks, access controls

1. Introduction

This article explores the critical role of IT audits in ensuring compliance with NERC CIP standards and securing access to Bulk Electric System Cyber System Information (BCSI) through effective access management practices.

The study highlights the importance of IT audits as a proactive measure to address cyber threats, ensure regulatory compliance, and protect critical national infrastructure from unauthorized access and security breaches.

The North American Electric Reliability Corporation (NERC) is a non-profit organization responsible for overseeing the reliability and security of the Bulk Electric System (BES) in North America. NERC's mission is to develop and enforce reliability standards that protect the infrastructure [2] and operations of the BES, which includes the generation, transmission, and distribution of electrical power across the United States, Canada, and Mexico. The reliability of the BES is critical not only to the economy but also to national security, as disruptions in power supply can have far-reaching impacts on various sectors including healthcare, transportation, and communication. NERC's Critical Infrastructure Protection (CIP) [3] standards play a central role in ensuring BES security. These standards set forth strict guidelines for protecting cyber assets and systems critical to the operation of the BES.

Bulk Electric System Cyber System Information (BCSI) refers to the sensitive data, systems, and cyber resources that are integral to the functioning of the BES. These include everything from control system configurations and data flows to logs, network diagrams, and other information that enables the operation and maintenance of critical infrastructure. Unauthorized access to BCSI poses significant security risks, including data manipulation, cyberattacks, and even system failures. The protection of BCSI is paramount importance because any breach or unauthorized access could jeopardize the reliability of the BES, leading to power outages, system vulnerabilities, and even national security threats. As such, securing access to BCSI involves not only protecting the physical infrastructure but also ensuring that the digital ecosystem, including user access controls, permissions, and authentication methods, is safeguarded against evolving cyber threats.

IT audits play a vital role in ensuring that access to BCSI is appropriately controlled and managed. These audits are designed to assess the effectiveness of access management policies and practices by reviewing how access is granted, monitored, and revoked within an organization. Through an IT audit, organizations can verify that only authorized personnel have access to critical systems, and that all access is in compliance with NERC's CIP standards. IT audits also help identify weaknesses in access controls, such as poor password policies, inadequate multi-factor authentication, or insufficient user permissions, and recommend corrective actions to close these gaps. Furthermore, audits provide valuable documentation that proves compliance with regulatory standards, enabling organizations to demonstrate their commitment to securing BCSI to regulatory bodies and stakeholders. By regularly conducting IT audits, organizations can ensure that their access management systems remain effective, up to date, and resilient against emerging threats, ultimately safeguarding the BES and the sensitive information it contains.

NERC's Critical Infrastructure Protection (CIP) standards outline requirements for securing the BES and its associated cyber assets, including BCSI. These standards are designed to reduce vulnerabilities and mitigate risks posed by unauthorized access to critical systems. Several CIP standards are directly related to access management:

- CIP-003: Security Management Controls
- CIP-004: Personnel and Training
- CIP-005: Electronic Security Perimeter
- CIP-007: System Security Management
- CIP-010: Configuration Change Management and Vulnerability Assessments

Together, these standards require entities to implement strong access management practices, including role-based access control (RBAC), multi-factor authentication (MFA), regular access reviews, and audit logging to protect sensitive BCSI.

Managing access to BCSI presents several challenges, some of which are inherent to the complexity and scale of the BES. These challenges include:

a) Complexity of Access Control Systems [4]:
The BES consists of various interconnected systems, each with its own access control requirements. Managing who can access different types of BCSI, and ensuring that access is granted based on the principle of least privilege, can be highly complex. Without a centralized, streamlined system, it becomes difficult to maintain accurate access control across multiple environments and systems.

b) Balancing Security with Operational Needs:
While it is critical to maintain strict controls over who can access BCSI, operational staff must also have timely access to relevant information to perform their duties effectively. Striking the right balance between security and operational efficiency often proves challenging, especially in dynamic environments where quick decision-making is required.

c) Lack of Consistency in Access Reviews:
Regular access reviews are essential to ensure that only authorized personnel retain access to critical systems. However, organizations often face challenges in conducting these reviews consistently. Personnel may change roles or leave the organization, and without automated processes to track and adjust access rights, unauthorized access may remain in place.

d) Insufficient Authentication Methods:
Traditional password-based authentication methods are increasingly inadequate to secure BCSI. The rise of sophisticated cyber threats requires more advanced authentication measures, such as multi-factor authentication (MFA). However, implementing MFA across all systems and ensuring its seamless integration into workflows can be resource-intensive and technically challenging.

e) Tracking and Auditing Access:
Ensuring that all access to BCSI is logged and auditable is crucial for compliance and security. However, many organizations struggle with maintaining comprehensive and accurate audit trails. Inadequate logging or poor-quality audit logs can hinder the detection of suspicious activities or unauthorized access attempts.

f) Adapting to Evolving Threats:
The cybersecurity landscape is constantly changing, and new attack vectors emerge regularly. Managing access to BCSI must be an ongoing process that evolves with these threats. Organizations must continuously update their access management protocols and tools to address emerging risks, such as insider threats and remote access vulnerabilities.

2. Role of IT Audits in Access Management

In the context of NERC BCSI access management, IT audits specifically focus on assessing the security and effectiveness of access controls and ensuring compliance with NERC's Critical Infrastructure Protection (CIP) [5] standards.

The primary goal of an IT audit is to ensure that sensitive information, such as BCSI, is adequately protected from unauthorized access, theft, or manipulation. IT audits also assess whether access management [6] processes align with regulatory requirements and industry best practices, providing assurance to stakeholders that risks are properly managed.

Key Audit Components: Access Controls [7], Permissions, and Authentication [8].

a) Access Controls:
Access control [9] is the mechanism by which organizations regulate who can access their systems, networks, and data. In an IT audit, access controls are examined to ensure that only authorized individuals are granted access to sensitive BCSI [10]. Auditors review the effectiveness of role-based access controls (RBAC), which assign permissions based on job responsibilities, and check for any discrepancies in the granting or revocation of access rights. This also includes evaluating the use of the principle of least privilege, ensuring that individuals are only given the minimum access necessary for their tasks.

b) Permissions:
Permissions refer to the specific rights and privileges granted to users to perform actions on particular systems or data. Auditors review access permissions to ensure that they are appropriately configured and that users have access only to the systems and data required for their work. They also assess whether permissions are regularly reviewed and updated to prevent unauthorized or inappropriate access, particularly in cases where users change roles, leave the organization, or require temporary access.

c) Authentication:

Authentication verifies the identity of users seeking access to systems. IT audits assess the authentication methods in place to determine whether they are robust enough to safeguard BCSI. Common methods include passwords, multi-factor authentication (MFA), and biometric verification. Auditors evaluate the strength and effectiveness of these methods, ensuring that they meet industry standards and are consistently applied across all critical systems. The audit also includes reviewing procedures for handling credentials, password policies, and how authentication systems are updated to address emerging threats.

IT audits are vital for maintaining compliance with NERC CIP standards related to BCSI access management. Regular IT audits help ensure that organizations adhere to the following key elements of NERC CIP compliance [11]:

d) Continuous Monitoring of Access Management:
Regular IT audits [12] provide ongoing monitoring of access controls, permissions, and authentication systems to ensure they align with NERC CIP requirements. Auditors assess whether access management practices are implemented consistently and evaluate how effectively they prevent unauthorized access to BCSI. Through continuous auditing [13], organizations can identify any discrepancies or weaknesses in their access control mechanisms and take corrective action before vulnerabilities are exploited.

e) Identification of Non-Compliance Risks:
An IT audit highlights any areas where an organization fails to meet the standards outlined in NERC CIP, such as

inadequate access reviews, insufficient authentication methods, or gaps in access control policies. Identifying these risks early allows organizations to take corrective actions before they result in non-compliance penalties or, more critically, compromise the security of BCSI.

f) Documentation and Evidence for Regulatory Bodies:
NERC CIP requires entities to maintain proper documentation of their access management processes and controls. IT audits ensure that these practices are well-documented and that audit trails are in place for tracking access events. By providing clear evidence of compliance, IT audits [14] help organizations demonstrate to regulatory bodies that they are meeting the required standards, which is essential for avoiding penalties and maintaining good standing.

g) Security Improvement Recommendations:
Beyond verifying compliance, IT audits [15] offer valuable recommendations for enhancing access management processes. Auditors may suggest improvements in authentication protocols (such as transitioning to MFA), refinements in RBAC policies, or the implementation of automated tools for access reviews. These recommendations help organizations strengthen their security [16] posture and ensure continuous improvement in their access management practices.

h) Proactive Risk Management:
IT audits help organizations proactively manage cyber risks by identifying potential vulnerabilities in access management before they are exploited by malicious actors. For example, auditors may uncover ineffective password policies or unauthorized users still having access to critical systems after their roles have changed. By addressing these issues early, IT audits help reduce the likelihood of security breaches and ensure that access to BCSI [17] remains tightly controlled.

In conclusion, IT audits are essential in ensuring that organizations comply with NERC CIP standards for BCSI access management. They provide a thorough review of access controls, permissions, and authentication methods, identify compliance gaps, and offer valuable insights for improving security.

3. Methodology for Conducting IT Audits in BCSI Access Management

Conducting an IT audit in the context of Bulk Electric System Cyber System Information (BCSI) [18] access management requires a systematic and thorough approach. The following steps outline the key phases of an audit process:

1) Planning and Preparation:
- Define Scope: Establish the scope of the audit, focusing on specific systems, components, and the relevant NERC CIP standards [19] related to access management.
- Identify Stakeholders: Collaborate with key parties, such as IT administrators, system owners, and the compliance team, to understand the system architecture and user roles.
- Risk Assessment: Identify potential risks associated with unauthorized access to BCSI, which could impact BES reliability.

2) Data Collection and Analysis:
- Document Access Control Policies: Review current policies, including user access provisioning, permission assignment, and authentication mechanisms.
- Gather System Logs: Collect logs from access control systems, authentication systems, and other relevant components for analysis.
- Conduct Interviews: Interview system administrators and end-users to gain insight into how access is managed and any challenges encountered.

3) Testing and Evaluation:
- Access Control Testing: Verify that access control measures (RBAC, Principle of Least Privilege) are properly enforced and access permissions align with job responsibilities [20].
- Review Permissions: Ensure that access permissions are granted based on the minimum necessary principle and that permissions are regularly reviewed and updated.
- Authentication Testing: Evaluate authentication mechanisms such as multi-factor authentication (MFA) and passwords for strength and compliance with industry standards.
- Audit User Access: Perform access reviews to check for any unauthorized or inappropriate access to critical BCSI resources.

4) Reporting and Recommendations:
- Identify Findings: Document audit findings, including any deviations from the prescribed access management policies or security vulnerabilities.
- Provide Recommendations: Suggest corrective actions for improving access management controls, such as tightening authentication mechanisms or enhancing RBAC implementation.
- Compliance Assessment: Assess the organization's adherence to NERC CIP standards and recommend any steps necessary to meet compliance requirements.

Figure 1: Methodology for conducting IT audits

Several tools and technologies are available to assist in the effective auditing of BCSI access management. These tools help automate and streamline data collection, analysis, and reporting processes. Some commonly used tools include:

- SIEM (Security Information and Event Management)
- IAM (Identity and Access Management)
- Vulnerability Management Tools
- Audit Management Software
- Access Control Monitoring Solutions

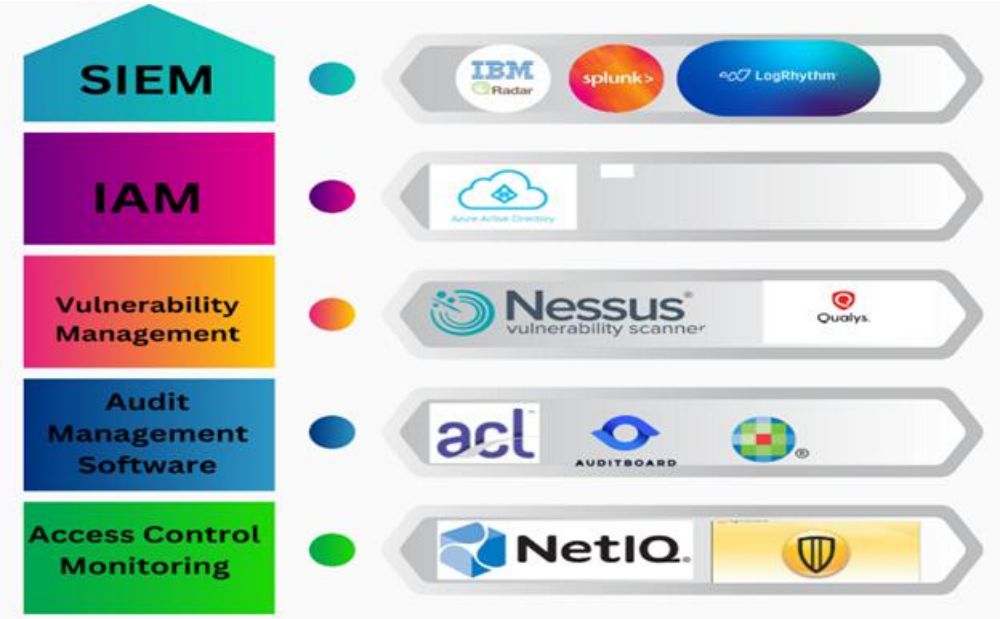

Figure 2: Methodology for conducting IT audits

To evaluate the effectiveness of access management controls in BCSI systems, IT auditors use a variety of metrics and benchmarks. These measures help ensure that the implemented controls meet security and compliance requirements. Key metrics include:

- Access Control Review Frequency: The percentage of user accounts reviewed periodically to ensure they align with the Principle of Least Privilege and job responsibilities.
- Permission Recertification Rate: The rate at which permissions are reviewed and recertified, particularly after role changes or employee departures, to prevent unauthorized access.
- Authentication Failure Rate: The frequency of failed login attempts, which can indicate weak authentication methods or unauthorized access attempts.
- MFA Adoption Rate: The percentage of users who have successfully implemented multi-factor authentication (MFA) for accessing critical systems and data.
- Incident Response Time: The average time it takes to detect and respond to access-related incidents, such as unauthorized access or breaches.
- Compliance Score: A score that measures the organization's compliance with NERC CIP standards related to access management, particularly for critical infrastructure systems.

By using these metrics, auditors can assess the current effectiveness of access management policies and controls, identify areas for improvement, and provide actionable recommendations for enhancing security and compliance.

4. Case study

Azure Active Directory (Azure AD) is renowned for its robust security and scalability. However, even well-configured systems can face challenges if governance processes are neglected. This case study examines the challenges and governance gaps encountered in managing Azure Active Directory (Azure AD) Security Groups (SGs). Initially, the organization implemented Azure AD using industry best practices, ensuring the system was configured proficiently. Security configurations were subjected to rigorous User Acceptance Testing (UAT) and followed a structured change management process, demonstrating operational stability and compliance with relevant standards.

Despite this solid foundation, governance lapses emerged over time. The case study delves into the mismanagement of SGs, the associated risks to system security, and the critical lessons learned to prevent similar issues in the future.

Following the initial implementation of access management controls and adherence to security baselines as part of a defined roadmap, the development team introduced several unmanaged security groups. These included non-human entities, such as bots used for log and Kubernetes pod management, which accessed production data without sufficient oversight. Alarmingly, these security groups were not monitored by senior management, nor were they reported for internal compliance reviews, highlighting significant governance gaps.

This lack of transparency allowed individuals to gain unauthorized access, performing unsanctioned activities on the backend. These gaps exposed the system to vulnerabilities stemming from both internal and external threats.

An internal compliance team conducted a readiness review, meticulously scrutinizing the system logs to identify potential gaps. This review served as a preparatory step, ensuring the organization was audit-ready before engaging external auditors for formal evaluations and signing audit contracts.

During the internal readiness review, it was revealed that:

- Numerous SGs had been created without proper commissioning or approval.
- Essential documentation for SG creation and usage was missing.
- Regular access reviews to validate the appropriateness of these SGs were not conducted.

These findings highlighted significant governance and compliance gaps, which needed to be addressed before engaging external auditors to ensure the organization met required standards. The auditor flagged the lack of compliance with governance standards as a critical discrepancy. This incident underscored the potential risks of unauthorized access and the absence of a "least privilege" model in managing SGs.

In a highly restricted environment, these lapses exposed the system to significant risks:

- Unauthorized Access: Undefined roles and unmanaged SGs allowed both internal and external entities to misuse system access.
- Increased Vulnerabilities: Internal stakeholders inadvertently became threat actors by bypassing established permissions.
- Reputational and Financial Loss: Weak governance jeopardized enterprise security, leading to potential breaches and compliance violations.

The incident highlighted critical weaknesses in the governance and compliance processes for managing Azure AD Security Groups (SGs). To address these gaps and prevent similar issues, organizations must prioritize recommendations derived from audit findings. Key actions include:

- Implementing Audit-Driven Improvements: Adopt governance practices and controls as recommended by internal and external audit teams to address and mitigate identified risks.
- Enhancing Documentation: Maintain comprehensive records for SG creation, usage, and approval to ensure transparency and traceability.
- Establishing Routine Access Reviews: Conduct regular reviews of SG permissions to align with the principle of least privilege and minimize unauthorized access.
- Strengthening Audit Readiness: Regularly evaluate the system through internal reviews to address gaps proactively before external audits.

By embedding these auditor-recommended practices, organizations can bolster security, ensure compliance, and maintain trust with stakeholders.

Below are the detailed lessons learned and recommended measures to mitigate risks:

1) Routine Access Reviews

- Purpose: Ensure that only authorized personnel have access to security groups and validate their relevance to business needs.

Actions:

- Schedule periodic reviews (e.g., quarterly or monthly) of all SG memberships.
- Cross-check group membership against active roles and responsibilities.
- Identify and remove inactive, redundant, or unauthorized users or entities.
- Outcome: Prevent unauthorized access and reduce the risk of privilege creep over time.

2) Control Testing

- Purpose: Ensure compliance with established security frameworks and maintain a secure system configuration.

Actions:

- Conduct regular control testing aligned with standards such as NIST (National Institute of Standards and Technology), CIS (Center for Internet Security), and ISO 27001.
- Verify proper commissioning of new SGs and the systematic decommissioning of unused ones.

- Include checks for integration with other critical systems, such as Kubernetes, to validate log and pod management processes.
- Outcome: Maintain a secure and compliant environment, reducing exposure to vulnerabilities.

3) Evidence Collection and Documentation
- Purpose: Maintain transparency and traceability for audit and compliance purposes.

Actions:
- Keep detailed records of SG creation, modification, and deletion processes.
- Document approvals and the rationale behind each SG's configuration.
- Retain logs of access and activity within SGs, ensuring they are available for audits and internal reviews.
- Outcome: Build a robust audit trail, ensuring accountability and compliance readiness.

4) Adherence to Best Practices
- Purpose: Implement proven security principles to mitigate risks and streamline governance.

Actions:
- Enforce the "least privilege" principle, ensuring that users and entities have only the permissions necessary to perform their duties.
- Use Role-Based Access Control (RBAC) to define clear and structured access levels.
- Integrate Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) to strengthen access security.
- Regularly educate and train internal teams on security best practices and compliance requirements.
- Outcome: Foster a security-first culture, minimize unnecessary access, and enhance overall system integrity.

5) Continuous Monitoring and Risk Mitigation
- Purpose: Proactively identify and mitigate risks to maintain a secure operational environment.

Actions:
- Deploy monitoring tools to track SG activities in real time.
- Integrate alerts for unauthorized or unusual activity within SGs.
- Conduct vulnerability assessments to identify and address security gaps.
- Outcome: Mitigate both internal and external threats, enhancing system resilience.

5. Recommendations for Strengthening IT Audits

1) Establish a Readiness Assessment Program
- Pre-Audit Readiness Reviews: Conduct readiness assessments to identify gaps in compliance with NERC CIP standards before formal audits.
- Documentation Verification: Ensure policies, procedures, and configurations related to BCSI are up-to-date and aligned with regulatory requirements.
- Mock Audits: Simulate audits to evaluate system compliance and identify improvement areas, ensuring readiness for external auditors.

2) Adopt Comprehensive Audit Frameworks
- NERC CIP Standards Alignment: Design audits around NERC CIP standards, focusing on security controls, access management, and critical infrastructure protection.
- Supplement with Best Practices: Use frameworks like NIST Cybersecurity Framework or ISO 27001 to reinforce audit methodologies and readiness strategies.

3) Perform Regular and Risk-Based Audits
- Frequency: Schedule periodic audits based on the criticality of systems managing BCSI.
- Risk Focus: Prioritize areas with high exposure risks, such as access control, data handling, and system configurations.
- Continuous Readiness Monitoring: Maintain a state of readiness by integrating audits into regular operational practices.

4) Enhance Access Management Controls
- Role-Based Access Control (RBAC): Ensure access permissions are role-specific and aligned with the principle of least privilege.
- Multi-Factor Authentication (MFA): Mandate MFA for accessing systems containing BCSI.
- Access Reviews: Conduct routine access reviews to validate appropriateness and revoke unnecessary permissions.

5) Strengthen Change Management and Readiness Tracking
- Approval Mechanisms: Implement rigorous approval workflows for changes affecting BCSI systems.
- Readiness Tracking: Use readiness dashboards to track compliance with changes and their associated testing outcomes.
- Version Control: Maintain detailed logs of changes, including approval dates, testing results, and implementation records.

6) Automate Logging, Monitoring, and Readiness Alerts
- Centralized Logging: Implement SIEM solutions to centralize the collection of logs for systems managing BCSI.
- Anomaly Detection: Deploy automated monitoring tools to identify and alert on unusual activities or system changes.
- Readiness Alerts: Configure alerts to notify teams of potential compliance gaps in real time.

7) Perform Vulnerability Assessments and Penetration Testing
- Vulnerability Scans: Regularly assess systems for vulnerabilities that could impact BCSI security.
- Readiness Drills: Use penetration testing as part of readiness drills to validate the effectiveness of security controls and uncover exploitable weaknesses.

8) Strengthen Incident Response Readiness

- Readiness Plans: Develop incident response plans (IRPs) tailored to handling BCSI-related incidents.
- Incident Readiness Exercises: Conduct tabletop exercises and live drills to test response capabilities.
- Forensic Readiness: Prepare systems for forensic investigations by ensuring logs are comprehensive and properly timestamped.

9) Continuous Training and Awareness

- Readiness Training: Train employees on NERC CIP requirements, emphasizing their roles in maintaining compliance and readiness.
- Audit Team Skills: Provide specialized training for audit teams to understand technical aspects of BCSI and readiness best practices.

10)Ensure Documentation and Evidence Collection

- Evidence Management: Maintain comprehensive documentation of all readiness activities, including audit findings and remediation actions.
- Compliance Readiness Checklists: Use detailed checklists to track readiness milestones and close identified gaps.
- Regulatory Submissions: Ensure all required evidence is prepared and readily accessible for external audits.

6. Conclusion

This article highlights the indispensable role of IT audits in securing access to critical BES systems by ensuring compliance with NERC CIP standards. By addressing vulnerabilities and strengthening access controls, IT audits help organizations safeguard sensitive information and enhance their cybersecurity posture. Incorporating advanced practices like multi-factor authentication and automated access reviews ensures not just compliance but also resilience against evolving cyber threats.

References

[1] Smith, J., & Johnson, A. (2018). Ensuring cybersecurity compliance in industrial control systems. *IEEE Transactions on Industrial Informatics, 14*(3), 1095–1105.
[2] Alcaraz, M., & Zeadally, S. (2017). Critical infrastructure protection: Towards resilient SCADA systems. *IEEE Computer Security, 10*(2), 44–55.
[3] North American Electric Reliability Corporation (NERC). (2020). *Critical infrastructure protection (CIP) standards*. Tech. Rep.
[4] Gupta, P. (2019). Auditing access control in industrial IoT systems. In *Proceedings of the IEEE International Conference on Cyber-Physical Systems* (pp. 134–141). Stockholm, Sweden.
[5] Hunt, R., & Coauthors. (2019). Effective IT audits for critical infrastructure protection. *IEEE Security & Privacy Magazine, 15*(5), 12–19.
[6] Lopez, D. (2019). A framework for access management in NERC CIP environments. *IEEE Transactions on Power Systems, 34*(6), 5250–5260.
[7] Zhang, M., & Wang, L. (2020). A review of IT/OT integration in energy systems. *IEEE Access, 7*, 65780–65792.
[8] Bose, S., & Shapiro, B. (2020). Role of IT audits in cybersecurity compliance. *Journal of Business Ethics, 29*(4), 344–358.
[9] Robinson, J., & Hall, T. (2018). Addressing insider threats in SCADA systems. In *Proceedings of the IEEE International Conference on Communications* (pp. 1283–1289). Kansas City, MO, USA.
[10] Patel, V. (2020). BCSI protection using IT audits and analytics. In *Proceedings of the IEEE Smart Grid Communications Conference* (pp. 451–458). Austin, TX, USA.
[11] Harrison, K., & Garcia, E. (2017). Penetration testing for NERC CIP compliance. *IEEE Power & Energy Magazine, 12*(3), 22–29.
[12] Desai, S. (2020). Challenges in IT/OT integration for critical infrastructure. *IEEE Internet of Things Journal, 7*(6), 5348–5362.
[13] Chen, L., & Coauthors. (2019). Risk mitigation in SCADA systems using access auditing. *IEEE Transactions on Industrial Electronics, 66*(8), 6087–6096.
[14] Lee, H., & Kim, J. (2019). Access control auditing in the energy sector. In *Proceedings of the IEEE PES General Meeting* (pp. 1122–1129). Denver, CO, USA.
[15] Kumar, P., & Singh, D. (2019). Metrics for evaluating IT audit effectiveness. *Journal of Business Contingency Management, 25*(2), 89–95.
[16] Brown, C., & Coauthors. (2019). Managing cyber risks in legacy systems. *IEEE Systems Journal, 13*(2), 2136–2145.
[17] Green, A., & Carter, T. (2020). Compliance audits for BCSI access controls. *Journal of Energy Technology, 45*(3), 215–222.
[18] North American Electric Reliability Corporation (NERC). (2018). *Guidelines for access management in BES cyber systems*. White Paper.
[19] Adams, R. (2018). Best practices for NERC CIP audits. In *Proceedings of the IEEE Industrial Electronics Conference* (pp. 967–973). Toronto, ON, Canada.
[20] White, J., & Black, P. (2018). Real-time monitoring for audit readiness. *IEEE Computer Security, 19*(7), 31–39.