Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 12| 2025

Review Article **Received:** 07-11-2025| **Accepted:** 02-12-2025 | **Published:** 17-12-2025

A Critical Review of IT Audit Practices for Compliance in Port Operations in the U.S

Daniel Akoto-Bamfo [1]***, and Alice Ama Donkor*** [2]

[1] *Temple University, PA, USA*

[2] *Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana*

Abstract: Port operations in the United States have grown into highly digitalized environments, where sophisticated information systems are leveraged to support logistics, security, and regulatory compliance. As these digital infrastructures become increasingly critical to operational and national security, the integrity and value of IT audit procedures have similarly increased in significance. In this vein, this study examines U.S. port operations, evaluating their adequacy, uncovering prevailing challenges, and assessing their alignment with compliance mandates issued by governing bodies, such as the Maritime Transportation Security Act (MTSA) and the Customs-Trade Partnership Against Terrorism (C-TPAT). The study also discovers the major gaps, and areas of IT audit in different port facilities through an extensive review of IT audit frameworks and case studies. The study finds that although most ports have implemented basic cybersecurity measures and compliance checks, a lack of in-depth skills in auditing for risk assessment, testing third-party systems, and incident response preparedness has left ports vulnerable. A significant reliance on self-reported compliance without objective third-party verification was also noted. These deficiencies reflect weaknesses that could be exploited, posing national security risks and disrupting operations. The findings provide insights about the urgent need for a standardized, risk-based IT audit model tailored specifically for port environments, integrating continuous monitoring, independent validation, and enhanced incident response auditing. Addressing these issues is essential to continue to protect U.S. ports as critical infrastructure within the global supply chain.

Keywords: IT Audit, Port Operations, Regulatory Compliance, Cybersecurity Governance.

INTRODUCTION

Modern operations of U.S. maritime ports are no longer limited solely to transporting physical goods but also rely heavily on a web of information technology (IT) systems to facilitate logistics, security, inventory, customs clearance, and regulatory compliance. With digital technologies becoming an increasingly integral part of port management, their reliance on complex IT systems has simultaneously introduced significant vulnerabilities, which, if exploited, will significantly disrupt the flow of trade, national security, and economic stability (U.S. Government Accountability Office [GAO], 2017). Acknowledging the significance of ports to maintain both domestic and international trade, ensuring the security and compliance of their IT systems becomes a matter of national priority (Coast Guard Cyber Command, 2022).

Although IT systems play a central role in port operations, recent findings disclose a troubling inconsistency in the manner U.S. ports approach IT auditing. According to a GAO (2017) report, cybersecurity assessments across ports remain fragmented, with significant inconsistencies in frequency, rigor, and coverage of audits conducted. Most ports continue to depend on voluntary participation in cybersecurity programs, and many have been observed in several cases to conduct self-assessments without any third-party verification, resulting in potential gaps in compliance and risk management (Gunes, 2021). This inconsistency is concerning, given the growing cyber threats targeted at critical infrastructure, including ports, of which any minor breach can trigger cascading negative impacts on supply chain and national defense capabilities.

This study, therefore, critically examines existing research and practices surrounding IT audit frameworks within U.S. port operations, specifically focusing on their effectiveness in ensuring compliance and cybersecurity risk mitigation. This study aims to synthesize existing empirical evidence, evaluate the strengths and weaknesses of current practices, and identify emerging trends that inform the future direction of IT auditing in the maritime sector. In thoroughly examining the convergence of IT auditing protocols and regulatory compliance in U.S. port operations, this research aims to highlight systemic vulnerabilities and provide practical insights for policymakers, port authorities, and cybersecurity professionals concerned with securing America's maritime gateways.

The Regulatory and Operational Landscape

The U.S. port operations' cybersecurity and compliance posture is shaped by regulation,

***Corresponding Author:** Daniel Akoto-Bamfo

DOI- https://doi.org/10.5281/zenodo.17962956

standards, institutional expectations, and international standards. The center of this regulatory architecture is the Maritime Transportation Security Act (MTSA) of 2002, a federal statute passed in the wake of the September 11 attacks (United States Congress, 2002). Under the MTSA, port facilities are mandated to conduct vulnerability assessments and facility security plans, which must be approved and audited by the U.S. Coast Guard. While MTSA focuses on physical security, it implicitly incorporates cybersecurity through analyses of risk and control measures that involve IT systems. (U.S. Coast Guard, 2025)

Adding to this is the Customs-Trade Partnership Against Terrorism (C-TPAT), a voluntary supply chain security program led by U.S. Customs and Border Protection (CBP). It supports trade stakeholders, including ports and terminal operators, to adopt best practices for securing their operations, including cybersecurity practices for data sharing and access control (CBP, 2022). C-TPAT certification often necessitates internal audit, but there exists significant variation in how thoroughly ports assess their IT environments under this program.

Aside from these US-centric frameworks, worldwide standards such as ISO/IEC 27001 offer internationally acknowledged requirements for establishing, implementing, maintaining, and continually improving information security management system (ISMS) (Kitsios *et al.,* 2023). While not mandatory, some U.S. ports and logistics entities have begun implementing ISO/IEC 27001, showing a commitment towards standardizing cybersecurity practices. For example, the Freight Transport Association (FTA) is ISO 27001 certified, which demonstrates adherence to internationally accepted information security management standards (Logistics UK, 2025). Moreover, logistics providers are increasingly leveraging ISO 27001 to strengthen their information security frameworks in order to better safeguard sensitive information and improve operational resilience. Cargobase, a global logistics tech platform for enterprise shippers announced in June 2022 work on obtaining ISO 27001 certification, which proves a commitment to maintaining and protecting information security (Wagenaar, 2022).

Likewise, the National Institute of Standards and Technology (NIST) has issued multiple publications, most notably the Cybersecurity Framework (CSF) and Special Publication 800-series for risk assessments, control implementation, and audit planning (NIST, 2018). The CSF provides guidance to government agencies, industry, and other organizations, including ports, to manage their cybersecurity risks. It presents a taxonomy of high-level cybersecurity outcomes that can be applied across all sectors and industry despite their size, sector, or maturity, to better understand, assess, prioritize, and communicate their cybersecurity efforts (NIST, 2023). The Special Publication 800 series, on the other hand, is a collection of best practices and guidelines established by NIST to help organizations manage cybersecurity risk and protect their information systems (Clomera, 2023).

Despite the emergence of such frameworks, the port environment raises unique operating complexities that challenge conventional IT auditing. Modern ports are vast decentralized ecosystems of terminal operators, carriers, customs officers, forwarders, and third-party logistics providers. These role players are involved with various interconnected systems such as terminal operating systems (TOS), port community systems (PCS), and industrial control systems (ICS), many of which are based on legacy architectures, not initially designed with cybersecurity in mind (Kessler *et al.,* 2018).

Furthermore, the dynamic nature of port operations, where cargo volumes fluctuate daily, and global cooperation is essential, adds temporal and procedural volatility in IT environments. These are hard realities that hinder the creation of universal audit checklists or fixed compliance schedules. Audits often do not adapt to rapid IT changes, and their findings might be devoid of contextual nuances, focusing on general controls while overlooking port-specific vulnerabilities (Parra *et al.,* 2018).

There is also a considerable gap between what is expected by regulations and the current execution by IT audits in many ports in the United States. For example, MTSA mandates periodic security assessments, but it does not specifically stipulate how often or to what depth cybersecurity-specific audits should be done. Likewise, although NIST guidelines recommend continuous monitoring and adaptive risk management, many port IT audits are periodic and checklist driven (NIST, 2018).

The audit function, while present, is often not sufficiently keeping up with the emerging threat

Publisher: SARC Publisher

landscapes. With no standardized criteria for IT audit execution with respect to port complexities, the ports are exposed to operational disruptions and non-compliance with regulations.

REVIEW OF EXISTING IT AUDIT PRACTICES IN PORT OPERATIONS

Existing Research on IT Audits for Critical Infrastructure

Cybersecurity of critical infrastructure, including ports, has been getting more attention in the past few years. The U.S. Government Accountability Office (GAO) has highlighted the fragmented nature of cybersecurity evaluations among U.S. seaports, emphasizing the need for greater consistency and rigorous audit methods (GAO, 2017).

The U.S. Maritime Transportation System (MTS) is a vital asset of the United States to transport goods around the Globe. However, a recent GAO report identified substantial cybersecurity vulnerabilities in their system, highlighting the increased dangers from state actors such as China, Iran, North Korea, and Russia, as well as transnational criminal networks (United States Government Accountability Office (GAO) (2025). While the U.S. Coast Guard is responsible for oversight, it is faced with constraints from limited access to inspection data as a result of deficiencies in its Marine Information for Safety and Law Enforcement system. The Coast Guard's cyber strategy currently lacks a full risk assessment of the MTS, thus undermining strategic resource allocation. Moreover, the report found that there were defined competency standards and gap assessments within the cyber workforce, calling into question its readiness to address complex maritime cyber threats. (Norris, 2025).

The Jones Walker 2022 Ports and Terminals Cybersecurity Survey provides significant insights regarding the cyber preparedness of U.S. ports and terminals. It outlines four key findings related to risk awareness, preparedness, governance, and cybersecurity investment. This survey is a key measure to looking into existing practices and has identified those areas in which ports can improve their audit routines to mitigate cyber-threats efficiently. Its focus on quantifiable readiness promotes better strategic and more informed cybersecurity planning within port operations (Jones Walker LLP, 2022).

The Maritime Bulk Liquids Transfer Cybersecurity Framework Profile (MBLT CFP), developed by the US Coast Guard, provides a targeted approach to auditing and evaluating cybersecurity risk for bulk liquids transfer operations. It guides operators with a framework to identify vulnerabilities specific to MBLT systems, which are critical for safety as well as supply chain continuity (USCG, 2017). By aligning with national risk management standards, the framework supports greater situation awareness and assists in integrating cybersecurity controls into daily organizational operation protocols.

The Cybersecurity Guidelines for Ports and Port Facilities Version 1.0 issued by International Association of Ports and Harbors, offers ports a globally informed framework for enhancing cybersecurity in port environments (Kuhn *et al.*, 2021). Acknowledging that the sector has its unique vulnerabilities, the guidelines combine technical recommendations with strategic governance measures. They emphasize the importance of comprehensive risk assessments and standardized audit practices while also promoting a stronger collaboration across departments and amongst international partners. In encouraging ports to integrate cybersecurity into core management systems, the IAPH guidelines promote the systemic resilience of not only local ports but also extend across the wider global maritime networks (IAPH, 2021). World Port Sustainability Program.

Typical Audit Methodologies Employed

Port operations rely on a range of audit methodologies to evaluate the effectiveness and security of their IT systems. Control-based audits are very common audits to evaluate whether specific controls exist and are operating effectively. Frequently associated with control systems such as COBIT, these audits are designed to examine compliance with internal policies and regulatory requirements (De Haes *et al.*, 2013).

In addition to control-based approaches, many ports use risk-based audits by focusing resources on auditing the higher risk areas. This technique also allows auditors to focus on potential weaknesses that could have a serious operational or financial impact, which is a very proactive strategy for managing cybersecurity threats (Vicente, 2023).

Self-assessment is also very common, especially if ports are struggling with resource constraints. Those are usually conducted internally using standardized checklists or templates. While such

Publisher: SARC Publisher

tools serve as a low-cost approach to oversee the health of these systems, they do not possess the autonomy and depth that is required to reveal concealed problems (SentinelOne, 2025)

To address this gap, Third-party assessments are often employed. These external audits offer an independent analysis of the IT environment. Leveraging on specialized expertise, they enable port authorities to benchmark their systems against industry best practices and identify areas of improvement (NIST, 2018).

Identified Strengths and Limitations

Enhanced compliance is one of the main advantages delivered by existing IT audit practices among ports. Routine audits have ensured port systems conform to domestic and international cybersecurity standards, which has allowed organizations to keep regulatory integrity (GAO, 2017). Additionally, these audits have raised awareness of emerging cyber threats and the need for more structured risk management and incident response strategies (Coast Guard Cyber Command, 2022). Audits have also had a positive impact on operational effectiveness. Through the discovery of redundancies, configuration issues, and obsolete technologies, many ports have optimized their IT infrastructures to enable more efficient logistics and expedite decision making (Vicente, 2023).

However, various issues affect the efficiency of an audit, even with various pros of conducting an audit. A major concern is the overreliance on checklist-based evaluation. These may become mechanical and not reflect context-related risks, particularly in the case of dynamic port environments (Ward, 2025). Another notable vulnerability is limited assessment in the area of incident response functionality. Many of the audits do not verify how effectively ports can detect, respond to, and recover from cyber incidents, which means that at the time of an actual attack, the port will be left vulnerable (NIST, 2023).

In addition, the cybersecurity posture of third-party vendors is often overlooked during audits. Since ports rely heavily on external partners—from shipping lines to customs brokers—weak supply chain oversight may introduce severe risks (IAPH, 2021). Also, smaller ports in particular are resource-constrained, which limits how in-depth or frequent audits are conducted. Budget and staffing constraints limit their ability to maintain strong cybersecurity defenses, widening the gap between intention and implementation (GAO, 2017).

Real-World Case Studies Highlighting Audit Gaps

In August 2021, Port of Houston discovered and successfully stopped a cyber intrusion linked to a foreign nation-state actor, which exploited a known vulnerability within Zoho Corporation's ManageEngine ADSelfService Plus, which is an enterprise password management tool (The Associated Press, 2021). According to the Cybersecurity and Infrastructure Security Agency (CISA), it disclosed that the vulnerability CVE-2021-40539 opened the avenue for threat actors to bypass authentication and execute arbitrary code on affected systems, allowing them to remotely access and control vulnerable networks (CISA, 2021). Although there was no report on loss of operational control, the incident illustrated how well-protected critical infrastructure could be left vulnerable to publicly disclosed software vulnerabilities when audit and patches were not sufficiently robust or timely. The incident highlighted the limitations of traditional audit approaches that may establish the presence of tools but fail to verify that systems are kept up-to-date and properly configured to defend against known threats.

In June 2017, the Port of Los Angeles suffered severe operational disruptions due to a global ransomware attack targeted against A.P. Moller-Maersk, one of the port's primary shipping partners. This attack, identified as the NotPetya malware attack, infiltrated Maersk's IT systems around the world and shut down operations at the APM Terminals at Pier 400, the port's largest cargo terminal. This incident stopped the flow of cargo and trucking operations, demonstrating that port operations could be vulnerable to cyber threats that impact their interconnectedness (Hayes, 2017). The breach highlighted the necessity for ports to protect their own internal systems and also to ensure that their partners maintain robust cybersecurity practices. In response to the growing threat posed by cyber criminals, the Port of Los Angeles previously established a Cyber Security Operations Center (CSOC) in 2014, the first of its kind among U.S. ports. Building on this foundation, the port launched the Cyber Resilience Center (CRC) in partnership with IBM in 2022. The CRC serves as a centralized hub for sharing real-time cyber threat information among port stakeholders and collectively enhancing their defense systems against cyber threats (WPSP, 2022). These proactive actions demonstrate the port's

Publisher: SARC Publisher

commitment to hardening its cybersecurity posture in light of evolving threats.

DISCUSSION

A recurring thread in the literature is the presence of regulatory gaps and inconsistencies in cybersecurity protocols across ports. The absence of a uniform cybersecurity framework leads to varying levels of resilience and preparedness (Industrial Cyber, 2024). Also, over-reliance on internal audits, often with low objectivity and technical expertise, undermines the efficiency of cybersecurity assessments (Lois *et al.*, 2021). The integration of third-party assessments and adherence to international standards are needed to improve audit efficiency and cybersecurity resilience.

While some scholars argue for the integration of advanced technologies, including real-time monitoring in auditing, others warn of the danger of overdependence on automated systems and highlight the importance of human oversight and contextual understanding (De Haes *et al.*, 2013). This divergence highlights the complex nature of balancing technological advancement with human expertise in audit practices. Furthermore, there are inconsistencies in the prioritization of cybersecurity investments, as some ports are concerned with immediate operational needs over long-term investment in cybersecurity strategies (Industrial Cyber, 2024). Current audit practices in ports are often insufficient to meet regulatory requirements and best practices. The dynamic nature of cyber threats necessitates a shift from reactive to proactive audit approaches, incorporating continuous monitoring, threat intelligence, and adaptive risk assessments. However, configuring routine auditing procedures with the international frameworks in cybersecurity and establishing partnerships among various stakeholders are essential in improving the cybersecurity posture in ports (De Haes *et al.*, 2013).

CONCLUSION

This study explored the evolving role of IT audits in strengthening cybersecurity within port operations, highlighting the need for a more adaptive and intelligence-led approach to audit practices. Although existing frameworks set a foundation for compliance, the dynamic threat landscape characterized by ransomware, supply chain attacks, and nation-state intrusions demonstrates their limitations. Case studies, such as the Port of Houston attack, illustrate how advanced threat actors are capitalizing on audit loopholes, underscoring the necessity of blending threat intelligence and proactive risk assessment. Furthermore, the difficulties in adapting audit methodologies to match emerging risks highlight the need for continuous capability building, improved regulatory guidance, and greater inter-agency cooperation. There is an urgent need to bridge the gap between expected best practices and on-ground audit implementation, especially in high-value critical infrastructure such as ports. Future audits must go beyond static checklists and instead evolve into dynamic tools that support policy, operational resilience, and enable timely detection and response. With global supply chains becoming more interconnected, ensuring port IT audits are flexible, robust, and forward-looking becomes not only a cybersecurity requirement but a strategic imperative.

REFERENCES

1. Coast Guard Cyber Command. “2021 Cyber Trends and Insights in the Marine Environment.” *United States Coast Guard* (2022).
2. Gunes, B., Kayişoğlu, G., and Yilmaz Bolat, P. “Cyber security risk assessment for seaports: A case study of a container port.” *Computers & Security* 103 (2021): 102196.
3. United States Congress. “Public Law 107–295—Maritime Transportation Security Act of 2002.” *U.S. Federal Law* (2002).
4. National Institute of Standards and Technology (NIST). “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.” *U.S. Department of Commerce* (2018).
5. U.S. Government Accountability Office (GAO). “Cybersecurity: Actions Needed to Better Secure Maritime Ports.” *GAO Reports* (2017): GAO-22-105705.
6. Kitsios, F., Chatzidimitriou, E., and Kamariotou, M. “The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector.” *Sustainability* 15.7 (2023): 5828.
7. Wagenaar, A. “Cargobase Achieves ISO 27001 Certification.” *Cargobase Blog* (2022).
8. Logistics UK. “ISO 27001 Information Security.” *Logistics UK* (2025).
9. National Institute of Standards and Technology (NIST). “Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN).” *U.S. Department of Commerce* (2023).

Publisher: SARC Publisher

10. Clomera, A. "What Are the NIST Special Publications (SPs) 800 Series?" *IPKeys* (2023).
11. Parra, N., Nagi, A., and Kersten, W. "Risk Assessment Methods in Seaports: A Literature Review." *ResearchGate Publication* (2018).
12. Customs and Border Protection (CBP). "Customs-Trade Partnership Against Terrorism (C-TPAT) Minimum Security Criteria." *U.S. Department of Homeland Security* (2022).
13. Kessler, G. C., Craiger, J. P., and Haass, J. "A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System." *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation* 12.3 (2018): 429–437.
14. National Institute of Standards and Technology (NIST). "Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)." *U.S. Department of Commerce* (2020).
15. United States Coast Guard. "Maritime Transportation Security Act." *U.S. Coast Guard* (2025).
16. United States Congress. "Maritime Transportation Security Act of 2002." *Public Law* 107–295 (2002): 116 Stat. 2064.
17. United States Government Accountability Office (GAO). "Coast Guard: Additional Efforts Needed to Address Cybersecurity Risks to the Maritime Transportation System." *GAO Reports* (2025): GAO-25-107244.
18. Jones Walker LLP. "2022 Ports and Terminals Cybersecurity Survey." *Jones Walker LLP Report* (2022).
19. United States Coast Guard (USCG). "Maritime Bulk Liquids Transfer Cybersecurity Framework Profile." *USCG Framework Publication* (2017).
20. Kuhn, K., Kipkech, J., and Shaikh, S. "Maritime Ports and Cybersecurity." *IET Power and Energy Series* (2021).
21. Vicente, V. "5 Risk-Based Internal Auditing Approaches." *AuditBoard* (2023).
22. Ward, A. "Strengths and Weaknesses of the Checklist Approach to Auditing." *Chartered Quality Institute (CQI)* (2025).
23. International Association of Ports and Harbors (IAPH). "Cybersecurity Guidelines for Ports and Port Facilities." *IAPH Guidelines* (2021).
24. De Haes, S., Van Grembergen, W., and Debreceny, R. "COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities." *Journal of Information Systems* 27.1 (2013): 307–324.
25. Kessler, G. C., and Craiger, J. P. "Maritime Cybersecurity: A Need for Regulatory Alignment." *Journal of Maritime Law and Commerce* 51.2 (2020): 123–140.
26. National Institute of Standards and Technology (NIST). "Computer Security Incident Handling Guide (SP 800-61 Rev. 2)." *U.S. Department of Commerce* (2024).
27. SentinelOne. "Information Security Audit Checklist: Step-by-Step Guide." *SentinelOne* (2025).
28. Norris, M. "GAO: Report Highlights Cybersecurity Risks to Maritime Transportation System." *Homeland Security Today* (2025).
29. The Associated Press. "Port of Houston Target of Suspected Nation-State Hack." *NBC News* (2021).
30. Cybersecurity and Infrastructure Security Agency (CISA). "APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus." *Cybersecurity Advisory AA21-259A* (2021).
31. World Ports Sustainability Program (WPSP). "Port of Los Angeles – Cyber Resilience Center." *World Ports Sustainability Program* (2022).
32. Industrial Cyber. "New DHS Report Highlights Gaps in Cybersecurity Efforts of Coast Guard for Marine Transportation Systems." *Industrial Cyber* (2024).
33. Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., and Vrontis, D. "Internal Auditing and Cyber Security: Audit Role and Procedural Contribution." *International Journal of Managerial and Financial Accounting* 13.1 (2021): 25–43.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Bamfo, D. A. and Donkor, A. A. " A Critical Review of IT Audit Practices for Compliance in Port Operations in the U.S." *Sarcouncil Journal of Engineering and Computer Sciences* 4.12 (2025): pp 77-82.

Publisher: SARC Publisher