International Journal of Multidisciplinary Innovative Research
ISSN: 2583-0228 Volume 5, Number 4 (Oct' 2025) pp. 23-30
© CIIR, Noida, INDIA (www.ciir.in)
https://www.ijmir.org
Article Received: 13 May' 2025; Accepted: 1 Jul' 2025.

Research Article

OPEN ACCESS

Designing an Efficient Audit Management System: A Compliance and Audit Tool

Aman Kamble, Anmol Mishra, Arnav Bhandarkar and Priyanshu Naiya

MIT School of Computing, MIT ADT University, Pune, India.

Email: aman.kamble@mituniversity.edu.in, anmol05me@gmail.com, arnavbhandarkar5@gmail.com, naiyapriyanshu@gmail.com

ABSTRACT: This research paper delves into the process of designing and developing an all-in-one platform that aims to improve the efficiency and security of audit processes. The proposed tool provides how digital management of a complex process such as auditing an organization can be simplified through a simple solution. Compliance and Audit Tool provides a centralized platform for conducting audits, creating and managing templates, and providing granular access control. This approach not only provides streamlined audit execution but also enhances transparency and accountability in compliance management. The scope of this research is to design and develop a system that increases the efficiency and security of the auditing process. Our focus areas were to increase user data isolation which can be implemented in hierarchical role management. The result demonstrates a scalable auditing system which provides simple management and monitoring, proper access control for users, creating templates, conducting assessment and accurate report generation. It is developed with Next.js MERN stack, MongoDB and JWT secure authentication system.

KEYWORDS: Access Control, Compliance, Audit, Assessment, Regulations, Authorization, Granular, Security, Regulations, Transparency, Scalability.

INTRODUCTION

Auditing is the process of examining and verifying the security postures and standards of an organization. Any organization needs to conduct an assessment of some form to make sure that it is secure and robust to some extent. Lack of such assessments can be fatal for an organization as these audits show what vulnerabilities these organizations have and what measures can be taken. The reports generated by these audits generate suggestions regarding improvement, enhancement and robust optimization for the organization structure and relevant systems. Organizations have to follow and abide by some compliances and regulations, related to their sector or domain. The compliance requires the organization to adhere to certain laws, regulations and guidances that are imposed by Auditors and Regulatory bodies like the government.

In this digital landscape of regulations and business operations, organizations must maintain rigorous compliance standards to improve their security posture. These measures are taken to ensure security, accountability, transparency, integrity of data, and proper access control. Consistent audits and assessments of organizations are critical in identifying risks and making sure that the security practices align with the compliance frameworks that are being followed. However, there are still many legacy organizations that still conduct audits and assessments with manual, semi-digital, laborious methods. They have serious disadvantages in the process that lacks structure, transparency, and most importantly, scalability.

Traditional auditing and assessment systems often fail to keep up with the complexity of modern organization. Complexities like number of users, distributed teams, different compliances for multiple sectors, hierarchy of roles and regulations, multi-level workflow approvals. Lack of a proper access control makes it more difficult to maintain accountability, ensure appropriate responsibility and clear audit trails.

To address and solve these gaps, this paper presents the system 'Compliance and Audit Tool', which is software that streamlines the creation and management of assessments and templates, promotes a structured assessment process, and introduces a granular user segmentation across distinct organization layers. To provide a distinct separation between many user roles, the divides them in two sides: the Platform side, which has the roles: Access Manager, Template Manager and Template Reviewer; and the Client side, which has the roles: Client Owner, Client Admin and Client User. During an audit assessment, the Client Admin assigns and divides the Client Users in an organization into three different roles based on their tasks: Assessee, Assessor, and Supervisor.

LITERATURE REVIEW

Compliance Auditing in Legacy Organization

In the traditional auditing process, auditors manually review all the printed documentation or digital documentation provided by the organization. The provided information was then validated by conducting physical interviews and On-premise walk-throughs of the environment. Auditors used printed or spreadsheet-based assessment checklists that aligns with the frameworks and templates. Then, scoring and results are calculated manually. Risk levels are defined based on simple heuristics and the report is compiled manually. The whole process takes weeks or even months, resulting in slower implementation of the patches and fixes.

Perception of Audit and Auditing Profession

This study titled,[1]'Auditor Perceptions of Audit Workloads, Audit Quality, and the Auditing Profession' conducted by Persellin et al. from Trinity University, described the perspective from over 700 auditors that auditing as a process can be very demanding with the workload, that the auditors find the process less rewarding and ineffective. Manual process for auditors leads to negative impact, and they believe that audit quality begins to suffer.

Access Control Models

Task-Role Based Dual Access Control Model' by ZHANG et al. [2] proposed a task-based dynamic management system that could be beneficial by providing advantages of both RBAC model (Role Based Access Control) and TBAC model(Task Based Access Control). In the TBAC model, roles are appointed to an individual, who then acquires the task that needs to be carried out by the roles, and owns its permission when the task gets executed.

A Systematic Literature Review on Compliance Requirements Management of Business Processes

Author: A. M. Mustapha, O. T. Arogundade, S. Misra, R. Damasevicius, and R. Maskeliunas [3]. Key Points: Research contributions revealed that the approaches more of formal techniques instead and formal checking and semantic methods. Hence, the compliances should be defined after a proper analysis of each criterion.

Audit Logs Management and Security—A Survey

Author: Ali, Ahmad, Mansoor Ahmed, and Abid Khan. Key Points: Presents how Logs are important [5] and crucial for finding abnormal activities and promoting accountability and transparency.

Securing Distributed Systems: A Survey on Access Control Techniques for Cloud, Blockchain, IoT and SDN

Author: Golightly, L., Modesti, P., Garcia, R., & Chang, V. Key Points: It was discussed that adoption strategies for Access Control prevents unauthorized users from accessing protected data [13] and how it could be integrated into network architecture strategy.

A Survey on Forensics and Compliance Auditing for Critical Infrastructure Protection

Author: Henriques, J., Caldeira, F., Cruz, T., & Simões, P. Key Points: The collected survey resulted in development of a reference Forensics [14] and Compliance Auditing (FCA) Architecture, which was introduced as a generic template for converged platforms. These would guide them on future research on forensics.

PROPOSED METHODOLOGY

Platform Side

One of the goals for this project was to provide a platform that can manage different types of users, based on their roles [2]. Hence, the users were categorized into two sides: Platform Side and Client Side. The platform side is mainly populated by developers, administrators, or any member of authority and trust for the given task. The Access Manager is at the top of the chain, as it provides access to users like the Template Manager and the Template Reviewer. These roles are generally consequential on a global level. Meaning, every change they conduct reflects on all users of the platform.

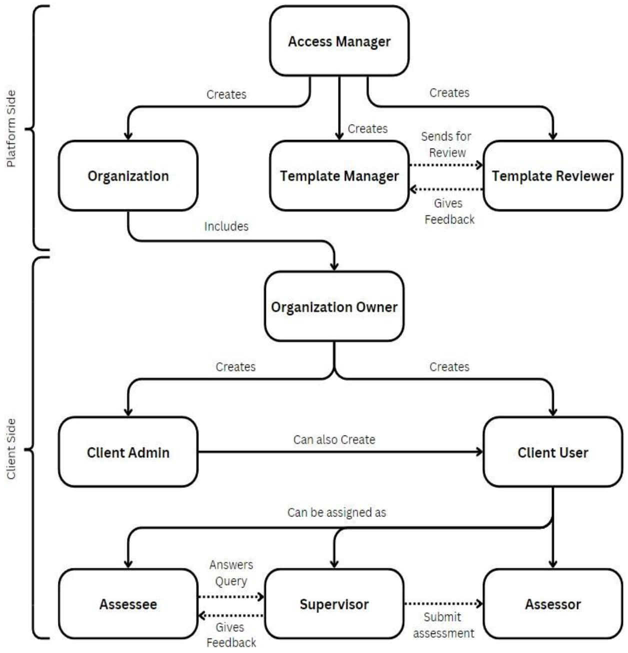


Figure 1: Represents the User Architecture

A template created by the Template Manager is first reviewed and evaluated by the Template Reviewer. Reviewers can approve or reject the template with proper feedback attached to them.

Once the template gets the seal of approval from the Template Reviewer, it is then published for the entire user base to refer to. These templates are then available in the 'General Template' section, along with other predefined frameworks and templates.

Access Manager can also do something very crucial, which opens up the Client Side. They can create an organization. These organizations are the actual users of the software. They ask for the services of the Access Manager for conducting internal audits. Access Manager creates the organization, selects the services, and assigns the Organization Owner. Now, the owner of the organization has the responsibility to add the client-side users to their organization.

Client Side

Client Admin can now add more Client Users to the organization if they want to. Client Admin can create an assessment based on a template. These templates can be general templates or custom templates, which are specific to an organization. Organization templates are created by Client Admin if it is necessary for a particular assessment. Such templates are only visible to the users of that particular organization. Organization templates are published without any external or internal review. Client Admin creates an assessment and assigns the Client User roles, which are Assessor, Supervisor, and Assessor. These roles are only specific to the assessment. Hence, they are task-based roles. An Assessee can be a Supervisor for another assessment, and vice versa. Hence, a Client User can have multiple roles at the same time. These roles can be assigned to different subsections in the assessment. So, different subsections can have different Assessee, Supervisor, and Assessor, but one Client cannot have multiple roles in the same subsection.

Assessments and Reports

An assessment will be created by the Client Admin, which then first goes to the Assessee. Assessee will complete their part of the assessment before the due date. That subsection will then be visible to the Supervisor for review, who will then give feedback on it. The supervisor can send it back to the Assessee for changes if they are unsatisfied with the Assessee's answers. If not, then they can approve the part, which can finally go to the Assessor. Once the Assessor gets the complete assessment from the Supervisor, they can then start scoring it based on the answers and evidence provided. Once everything is scored and given feedback, a report is generated of the complete assessment. This report will then have the scores, mentions, feedback, suggestions, and metadata.

TESTBED SETUP AND CONFIGURATION DETAILS

Environment Configuration

- Development Environment:
  1. Node.js version 18.x or higher
  2. MongoDB version 6.0 or higher
  3. Use npm for package management
  4. Import the dotenv library, and a file is created in the root directory to configure essential environment variables:

     ```
     NEXTAUTH_URL="Enter the Next URL"
     NEXTAUTH_SECRET= "your_secure_nextauth_secret"
     ```

```
DATABASE_URL= Enter Database URL"

ENCRYPTION_KEY="your-secure-32byte-key-for-file-
encryption"
```

Technical Stack

- Frontend:

1. React.js 18.x
2. Next.js 14.x (App Router)
3. TailwindCSS 3.x
4. Headless UI
5. Heroicons

- Backend:

1. Next.js API routes
2. MongoDB (using MongoDB Client and Amazon EC2)
3. NextAuth.js for authentication
4. bcrypt.js for password hashing

Database Setup

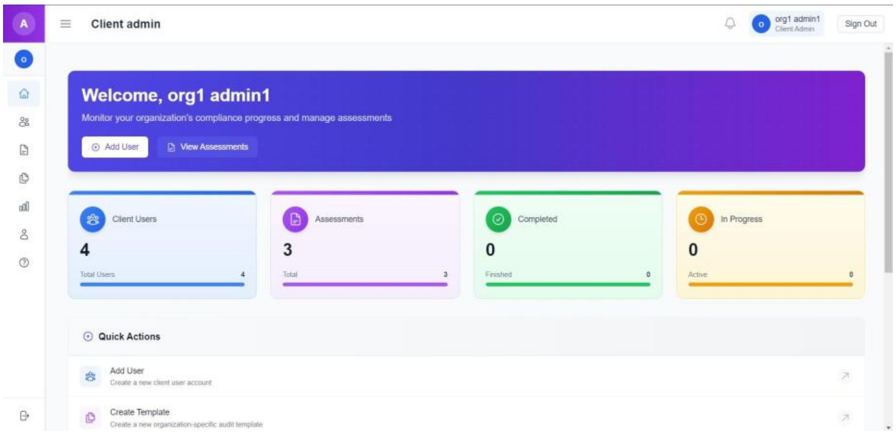
- The CAT system uses an architecture where each client organization has a separate MongoDB database, where the User information, organization-based custom templates, assessments, and reports are stored.
- The Access Manager dedicates specific databases for each organization, which ensures data isolation between clients and organizations.
- Simply connect to the Localhost for the MongoDB connection. Predefined databases will be visible.

RESULT AND DISCUSSION

(a) Security Coding Practices: During the development, industrial standard secure coding practices were maintained. Key implementations included here with bcrypt-based password hashing, input sanitization, and protected API routes with role-based access. No known vulnerabilities (SQL injection, XSS, etc.) were found both in manual testing and automatic security linting which shows high integrity in the codebase [23].

(b) Authentication using JWT Tokens: The application adopts JSON Web Tokens (JWT) for session-based authentication, securing and maintaining stateless access control among the different user roles. This mechanism has denied all attempts at unauthorized access in every testing scenario and has also permitted scalable session validation while avoiding server overload with session data.

(c) SMTP Integration for Alerts: SMTP services provided by Google (Nodemailer) were added to make automatic email alerts possible. These were checked for happenings like user creation, assessment assignment, and submission confirmation. Email dependability and delivery time were measured under test loads; delivery was steady in all trials, improving user engagement as well as audit tracking.



Welcome, org1 admin1

Monitor your organization's compliance progress and manage assessments

Client Users	Assessments	Completed	In Progress
4	3	0	0
Total Users 4	Total 3	Finished 0	Active 0

Add User
Create a new client user account

Create Template
Create a new organization-specific audit template

Figure 2: Client Admin Dashboard

(d) Efficient API Calling: The setup worked around RESTful APIs, which were meant to be quick. The time taken by the APIs to give a response was checked for the main parts, and it was less than 200ms when averaged. Just to add more strength against heavy usage, we applied rules on the rate of calls and errors, too.

(e) Performance Under Load: The application was tested with simulated user activity for multiple organizations. The microservice-oriented architecture and the strategy of having one database per organization helped us achieve our main objectives, which were to maintain system stability and ensure data isolation. MongoDB's performance was efficient, especially with the consolidated assessment schema, it remained optimal even at scale.

(f) Robust and Access Control: By including multiple roles with appropriately defined permissions and abilities, the access control becomes impeccable and robust. The chances of accessing protected data and functionalities by unauthorised users is slim. These implementations increase the security levels of the overall system[13].

(g) Transparency and Accountability: An assessment that is being conducted, has all the involved users in sync, through status alerts. Status shows which party is currently working on it [6]. It reflects to all users involved users if the Assessee that is currently working on or if the Supervisor is suggesting some changes. This results in better implementation of transparency and accountability throughout the process, for all users.

CONCLUSION

This research demonstrates the successful implementation of a secure, scalable, and modular Compliance Audit Tool (CAT) designed to streamline audit management across multiple organizations. By integrating a hierarchical access architecture, customizable workflows, secure authentication (via JWT), granular API-level access control, and robust secure coding practices, CAT ensures data integrity, confidentiality, and usability. The system's RESTful APIs, combined with MongoDB's multi-tenant document model, provide high performance and strong data isolation, supporting enterprise-grade scalability. Under rigorous test conditions, CAT exhibits excellent responsiveness and reliability, confirming its suitability for diverse organizational contexts. The scope of this research covers secure audit workflow management, real-time communication, and scalable data handling. The results validate that CAT not only addresses current compliance and auditing demands effectively but also establishes a strong foundation for future advancements like real-time analytics, compliance dashboards, and integration with external regulatory systems.

REFERENCES

[1] J. Persellin, J. J. Schmidt, and M. S. Wilkins, ”Auditor perceptions of audit workloads, audit quality, and the auditing profession,” *SSRN Electron. J.*, 2014. [Online]. Available: https://doi.org/10.2139/ ssrn. 2534492.

[2] C. Zhang, Y. Hu, and G. Zhang, ”Task-role based dual system access control model,” *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 6, no. 7B, pp. 211–215, 2006. [Online]. Available: http://paper. ijcsns.org/ 07.book/200607/200607C14.pdf.

[3] A. M. Mustapha, O. T. Arogundade, S. Misra, R. Damasevicius, and R. Maskeliunas, ”A systematic literature review on compliance requirements management of business processes,” *Int. J. Syst. Assur. Eng. Manag.*, vol. 11, no. 3, pp. 561–576, 2020. [Online]. Available: https://doi.org/10.1007/s13198-020-00985-w.

[4] N. A. Chandra, K. Ramli, A. A. P. Ratna, and T. S. Gunawan, ”Information security risk assessment using situational awareness frameworks and application tools,” *Risks*, vol. 10, no. 8, p. 165, Aug. 2022. [Online]. Available: https://doi.org/10. 3390/risks10080165.

[5] A. Ali, M. Ahmed, and A. Khan, "Audit Logs Management and Security - A Survey," *Kuwait Journal of Science*, vol. 48, no. 3, 2021. [Online]. Available: https://doi.org/10.48129/kjs.v48i3.10624.

[6] M. Zelmati, Z. Oulqaid, and A. Elouadi, ”Real-time tracking of auditing process progress with a customizable application for cybersecurity standards compliance: A case study on ISO 27001 and TISAX,” in *Proc. 10th Int. Conf. Wireless Networks Mobile Commun. (WINCOM)*, 2023, pp. 1–6. [Online]. Available: https://doi.org/10.1109/WINCOM59760.2023.10322925.

[7] B. Ngalim, "Integrating NIST and ISO Cybersecurity Audit and Risk Assessment Frameworks into Cameroonian Law," *Journal of Cybersecurity Education Research and Practice*, vol. 2024, no. 1, 2023. [Online]. Available: https://doi.org/10.32727/8.2023.29.

[8] B. B. and M. N. Hiremath, "Cyber Security and Compliance Management through a Single Integrated Platform," *International Journal for Research in Applied Science and Engineering Technology*, vol. 12, no. 1, pp. 1243–1247, 2024. [Online]. Available: https://doi.org/10.22214/ijraset.2024.58153.

[9] T. O. Abrahams, S. K. Ewuga, S. K., P. U. U., A. O. Hassan, and S. O. Dawodu, "Mastering compliance: A comprehensive review of regulatory frameworks in accounting and cybersecurity," *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 120–140, 2024. [Online]. Available: https://doi.org/10.51594/ csitrj.v5i1.709.

[10] M. Howison, M. Angell, and J. S. Hastings, "Protecting sensitive data with secure data enclaves," *Digital Government: Research and Practice*, vol. 5, no. 2, 2024. [Online]. Available: https://doi.org/10. 1145/3643686.

[11] G. Almufadda and N. A. Almezeini, "Artificial Intelligence Applications in the Auditing Profession: A Literature Review," *Journal of Emerging Technologies in Accounting*, vol. 19, no. 2, pp. 29–42, 2022. [Online]. Available: https://doi.org/10.2308/JETA-2020-083.

[12] K. A. K. Saputra and S. Paranoan, "Do Cyber security, Digitalisation and Data Visualisation Affect the Quality of Internal Environmental Audits?," *Australasian Accounting, Business and Finance Journal*, vol. 18, no. 2, pp. 158–174, 2024. [Online]. Available: https://doi.org/10.14453/aabfj.v18i2.10.

[13] L. Golightly, P. Modesti, R. Garcia, and V. Chang, "Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN," *Cyber Security and Applications*, KeAi Communications Co., Dec. 1, 2023. [Online]. Available: https://doi.org/10.1016/j.csa.2023.100015.

[14] J. Henriques, F. Caldeira, T. Cruz, and P. Simões, "A Survey on Forensics and Compliance Auditing for Critical Infrastructure Protection," *IEEE Access*, vol. 12, pp. 2409–2444, 2024. [Online]. Available: https://doi.org/10.1109/ACCESS.2023.3348552.

[15] Y. S. Rajesh, V. G. K. Kumar, and A. Poojari, "A Unified Approach Toward Security Audit and Compliance in Cloud Computing," *J. Inst. Eng. (India): Ser. B*, Springer, Jun. 1, 2024. [Online]. Available: https://doi.org/10.1007/s40031-024-01034-x.

[16] J. P. Seara and C. Serrão, "Intelligent System for Automation of Security Audits (SIAAS)," *EAI Endorsed Trans. Scalable Inf. Syst.*, vol. 11, no. 1, 2024. [Online]. Available: https://doi.org/10.4108/ eetsis.3564.

[17] K. A. K. Saputra and S. Paranoan, "Do Cyber Security, Digitalisation and Data Visualisation Affect the Quality of Internal Environmental Audits?" *Australasian Accounting, Business and Finance Journal*, vol. 18, no. 2, pp. 158–174, 2024. [Online]. Available: https://doi.org/10.14453/aabfj.v18i2.10.

[18] C. Friedrich, W. R. Knechel, A. S. Sofla, and V. S. Zuiddam, "Client Employee Training and Audit Efficiency," *Auditing: A Journal of Practice & Theory*, vol. 43, no. 1, pp. 73–99, 2024. [Online]. Available: https://doi.org/10.2308/AJPT-2022-012.

[19] J. P. Seara and C. Serrão, "Automation of System Security Vulnerabilities Detection Using Open-Source Software," *Electronics (Switzerland)*, vol. 13, no. 5, 2024. [Online]. Available: https://doi.org/10.3390/ electronics13050873.

[20] A. Njowa, B. Schutte, and Z. Ally, "Insider Threats to Cyber Security in an Audit Environment," in *Springer Proceedings in Business and Economics*, pp. 379–397, Springer Nature, 2024. [Online]. Available: https://doi.org/10.1007/978-3-031-46177-4_21.

[21] S. S. Nair, "Securing Against Advanced Cyber Threats: A Comprehensive Guide to Phishing, XSS, and SQL Injection Defense," *Journal of Computer Science and Technology Studies*, vol. 6, no. 1, pp. 76–93, 2024. [Online]. Available: https://doi.org/10.32996/jcsts.2024.6.1.9.

[22] P. Rosati, F. Gogolin, and T. Lynn, "Cyber-Security Incidents and Audit Quality," *European Accounting Review*, vol. 31, no. 3, pp. 701–728, 2022. [Online]. Available: https://doi.org/10.1080/09638180.2020. 1856162.

[23] V. Casola, A. De Benedictis, C. Mazzocca, and V. Orbinato, "Secure software development and testing: A model-based methodology," *Computers and Security*, vol. 137, 2024. [Online]. Available: https://doi. org/10.1016/j.cose.2023.103639

[24] M. Assiri and M. Humayun, "A Blockchain-Enabled Framework for Improving the Software Audit Process," *Applied Sciences (Switzerland)*, vol. 13, no. 6, 2023. [Online]. Available: https://doi.org/10.3390/ app13063437.

[25] M. M. Thottoli and T. K. V, "Characteristics of information communication technology and audit practices: evidence from India," *VINE Journal of Information and Knowledge Management Systems*, vol. 52, no. 4, pp. 570–593, 2022. [Online]. Available: https://doi.org/10.1108/VJIKMS-04-2020-0068.

[26] M. H. A. Allbabidi, "Hype or hope: Digital technologies in auditing process," *Asian Journal of Business and Accounting*, vol. 14, no. 1, pp. 59–86, 2021. [Online]. Available: https://doi.org/10.22452/ajba. vol14no1.3.