KeAi
CHINESE ROOTS
GLOBAL IMPACT

International Journal of Innovation Studies

# ZERO TRUST ARCHITECTURES IN FINANCIAL INSTITUTIONS: A CASE STUDY OF IMPLEMENTING IDENTITY-BASED ACCESS CONTROL WITH CISCO ISE

**Vivek Bairy**
Sr. Network Engineer
(Independent Researcher)
First Republic Bank,
San Francisco, USA
vbairy21@gmail.com
ORCID: 0009-0007-8787-0357

**Abstract**
The purpose of this case study is the implementation of IBAC using Cisco ISE as a financial organization to enhance the security posture based on Zero Trust Architecture. The current research quantified the impact that Cisco ISE has on the security incidents of the users and their compliance towards the network security, along with the network's performance. Stratified random sampling was used, and data from 100 respondents were collected by conducting a six-month pretest-posttest study. Metrics Assessed The analysis examines critical measurements: unauthorized accesses, insider threat, third party breaches, rate of user compliance, and even system performance, which is presented as the velocity of authentication plus the network latency. There were marked decreases of security incidents reported; unauthorized accesses went down 66.7%, insider threat 66.7%, while third party breach was 62.5%, and these improvements were statistically significant ($p < 0.05$). The rates of user compliance increased by 50%, 37.7% increase in awareness of policies, and an 80% improvement in attendance to training sessions. System performance also remained sound, with 16.7% improvement in authentication speed, 0.9% in system uptime, and a small, statistically insignificant increase in network latency. The findings indicate that Cisco ISE effectively reduces security incidents, enhances user compliance, and maintains or improves system performance, thus reinforcing the value of Zero Trust principles in strengthening cybersecurity within financial institutions.
**Keywords:** Zero Trust Architecture (ZTA), Identity-Based Access Control (IBAC), Cisco Identity Services Engine (ISE), Security Incidents, User Compliance

## 1.INTRODUCTION

Cybersecurity, in the constantly changing financial services landscape, becomes a cornerstone for operational resilience and customer trust. Financial institutions carry large volumes of sensitive data and assets, constantly targeted by the most sophisticated cyber threats (Green-Ortiz, 2023). Thus, this has called for evolving security paradigms from being perimeter-based and traditional to more holistic and robust methods. Among these are Zero Trust Architecture, which became popular for providing the capability of addressing modern challenges in security; it enforces strict identity verification and granular access controls to ensure that this is achieved in a financial setting (Henderson, 2022). This paper explores the embedding of Zero Trust principles within a financial institution as it integrates with Identity-Based Access Control through the Cisco Identity Services Engine.

In particular, Zero Trust follows the legacy model of "never trust, always verify"; entities within the network cannot always be trusted inherently (Keskinen, 2022). This can pose a specific critical challenge especially in financial industries that have rampant insiders' threats and advanced persistent threats among other threats arising from third-party risks (Khan, 2020). With Zero Trust Architectures, organizations can be sure that only verified identities and contextual information provide access to sensitive systems and data, while being continuously monitored. This strategy mitigates risks while aligning with the regulatory compliance frameworks of GDPR and PCI DSS, which are known for having strict data protection measures.

Zero Trust relies on Identity-Based Access Control (IBAC) as a foundational element in providing the dynamic framework for access management by users or devices. IBAC differs from traditional role-based access control by using true real-time identity verification, contextual parameters, and risk assessment in determining access rights (Kharjana, 2023). Financial institutions would, therefore, be offered an all-in-one integrative platform like Cisco ISE, offering good implementation of policy-driven network access control, device profiling, and identity authentication (Minella, 2022). This means that it's compatible with the existing infrastructure, and it's also capable of providing granular visibility into user and device activity, making it a preferred choice for implementing Zero Trust in high-stakes environments such as financial institutions.

This study digs into the case of the practical usage of Zero Trust Architectures at financial institutions to deploy Cisco ISE and shows improvements in the level of security provided. By showing a case scenario, it indicates the difficulties associated with, strategic approaches adopted and results expected with this IBAC implementation model (Mohamed, 2021). It underlines that all these deployments in a phased mode, through increased employee awareness as well as thorough evaluation would make their Zero Trust programmes successful.

The ultimate aim of this research is to contribute to the ever-expanding knowledge on Zero Trust Architectures by providing actionable recommendations and best practices for financial institutions (Tuononen, 2023). It hopes to bridge the gap between theory and real-world application and help organizations better prepare their cybersecurity frameworks in response to the growing complexity of the threat landscape.

### 1.1 Overview of Zero Trust Architecture (ZTA)

Zero Trust Architecture is the model of the cybersecurity principle based on "never trust, always verify." It's unlike traditional security models that use perimeter-based defense, assuming internal and external networks are compromised (Woland, 2019). Thus, in ZTA, users, devices, and applications are continuously authenticated, authorized, and validated before access is granted. It ensures only relevant individuals and specific devices gain authorized access to select resources with regard to very critical identity verification followed by a relevant contextual analysis; ZTA hence plays a most crucial role especially in financial entities where high security is warranted by reduction of risk possibilities due to attacks through insiders.

### 1.2 Challenges in Securing Financial Institutions

Financial institutions offer a different security challenge in view of the heavy volume of data, regulatory and compliance requirements that are quite challenging, and continuously evolving sophistication in cyber threats (Zaid, 2023). Financial institutions will have to provide protection against insiders, data breach, and outsider cyberattacks, among others. Moreover, across a large workforce, consisting of employees, contractors, and other third-party service providers, maintaining user access raises the complexity bar for security management. Thus, the nature of these threats continuously evolves, calls for real-time monitoring and compliance with all industry

regulations that require robust adaptable security measures to be in place. As such, financial institutions would now have to take into account access and operational efficiency against stringent controls to prevent both financial loss and reputational damage.

### 1.3. Research Objectives

1. Quantify the reduction in unauthorized access incidents after implementing ZTA.
2. Assess user compliance with security protocols post-implementation.
3. Evaluate changes in network performance metrics, including latency and authentication speed.

## 2. REVIEW OF LITERATURE

**Adenola, (2023),** undertook a detailed study on access management systems based on artificial intelligence, which emphasized their potential for revolutionizing security frameworks. It looked into how AI could help enhance mechanisms for access control through real-time decision-making and anomaly detection (Adenola, 2023). According to Adenola, AI was suited for dynamic environments such as financial institutions where access control systems had long struggled to keep pace with the changing threats, mainly because it can process huge amounts of data and identify patterns.

**Ahir (2023)** provided an overview of the access control mechanism with the emphasis on its theoretical and practical implementation in his diploma thesis. It considered the most significant frameworks and methodologies that deal with the management of user access within digital systems (Ahir, 2023). Ahir's work stressed that the strategy for access control needs to be in tandem with organizational goals and newer technological developments, especially when considering more advanced forms of cyberattacks.

**Atalay (2019)** was the contributor for an invaluable access control and authentication mechanism for Internet of Things study. This article investigated unique challenges associated with the security issues surrounding IoT ecosystems while presenting a contributory model aimed at enhancing the mechanism of authentication and access management (Atalay, 2019). According to Atalay, proper implementation of identity verification and constant monitoring in reducing the potential risks due to proliferation of the devices. The study further underlined the need for designing scalable and adaptive access control systems that can accommodate the diverse range of devices and use cases in IoT networks.

**Collin, in his study (2021),** analyzed the applicability of automation in multi-domain SDN across diverse use cases. It discussed how the automation within SDN frameworks would simplify network management, enhance scalability, and increase security (Collin, 2021). In this context, Collin underscored the significance of integrating access control mechanisms with automation to make communication between various network domains smooth and secure. Therefore, the research concludes that SDN automation can positively impact the security policy responsiveness that can be crucial for modern architectures, including those of Zero Trust.

**Diogenes, Young, Simos, and Rodriguez (2023)** did an excellent job presenting a comprehensive approach to cybersecurity principles and best practices in their book Exam Ref SC-100 Microsoft Cybersecurity Architect (Diogenes, 2023). The book focused on secure architecture design and implementation strategies using identity-based access control systems, among other areas. Their methodology described how security measures could be aligned with the goals of organizations, focusing more on identity validation, threat identification, and risk reduction. The study also highlighted the support that tools like Microsoft Azure offer when it comes to deploying advanced

architectures for security by comparing similar capabilities offered in similar solutions such as Cisco ISE.

## 3. RESEARCH METHODOLOGY

A pre survey-post survey design to accumulate data on incidence of security incident, user adherence, and overall system performance that has been incurred for six months is used as methodology in presenting the impact study of Cisco Identity Services Engine (ISE) on financial institution security performances. Various data collection tools, such as security logs, user surveys, and system metrics, were employed. A stratified random sample of 100 users was drawn from the institution's 500 employees. Statistical analysis, including paired t-tests and regression analysis, was conducted to assess the significance of the results.

### 3.1 Research Design

A pretest-posttest research design was used to measure the effect of deploying Cisco ISE on the security performance of a financial institution. The design involved data collection before and after the deployment of Cisco ISE, focusing on key security metrics such as unauthorized access attempts, insider threats, and third-party breaches. This comparative approach was very helpful in providing a good and comprehensive analysis of the change in security incidents and system performance over time. The data was collected for six months to ensure that short-term as well as long-term effects of the implementation were captured and analyzed. Baseline data was obtained on the number of occurrences and type of security breaches, as well as on user compliance and system performance in the pretest. The posttest was carried out by taking similar measurements once Cisco ISE had been implemented in full and functioning correctly. This experimental design made possible a precise data-based assessment of whether Cisco ISE would help make the institution safer and more efficient to operate.

### 3.2 Data Collection Tools

The data collection for this study involved three major tools to test the impact of implementing Cisco ISE on the security posture of the financial institution. These were analyzing Security Incident Logs to know how often and what type of breaches occurred, ensuring that there is quantitative data showing attempts at unauthorized access, insider threats, and third-party access incidents before and after the implementation of Cisco ISE. These logs directly measured the decline in security incidents. In addition, User Surveys were done to check whether employees adhered to the security protocols installed such as multi-factor authentication and access controls. It measured the way users complied with security practice and the knowledge of its need to ward off threats. The changes in the System Metrics will highlight the technical level of the implementation, including both authentication speed change and network latency. The final point will enable the organization not to be detrimentally affected as a result of implementing Cisco ISE but strengthen their security. With these diverse tools, the study managed to capture an all-rounded view of the impacts of Cisco ISE implementation on both security and performance.

### 3.3 Sample

The sample for this study was a financial institution with 500 employees, including IT administrators, end-users, and contractors. To ensure a representative distribution of perspectives across different roles within the institution, data was collected from 100 users selected through stratified random sampling. This approach used stratification in dividing the population of employees into separate strata based on roles: IT administrators, end-users, and contractors. Then, it was ensured that each stratum has participants randomly drawn to maintain the proportionate distribution. The approach used stratified sampling to guarantee the diversity of the sample

population and ensure a reflection of all experiences within the institution, making it possible to comprehensively measure the effect of Cisco ISE implementation on user groups. This sampling technique led to a fair and reliable analysis of the results.

### 3.4 Statistical Analysis

For statistical significance evaluation of the changes observed in security performance, user compliance, and system metrics, paired t-tests and regression analysis were used. The paired t-tests were conducted for the comparison of pre- and post-implementation data of each metric such as frequency of security incidents, user compliance rates, and system performance measures, enabling the assessment of mean differences before and after the deployment of Cisco ISE. This pilot study helps find out if observed changes were indeed statistically significant as evidenced by the p-value calculated, where small values for a given statistical difference are deemed very strong. Multiple regression was performed to further examine the associations of the deployment of Cisco ISE with alterations in security and performance measures with controlling variables: level of training amongst employees, as well as configuration of network. These statistical methods were therefore aggregated together to present a comprehensive structure in which to understand the implications of Cisco ISE on the security posture of the institution, and operational efficiency by being both statistically valid and reliable.

## 4. DATA ANALYSIS AND RESULT

This section reports on the results of the research on implementing Cisco ISE for Identity-Based Access Control in a financial organization. The investigation focuses on three aspects: a decrease in the number of security incidents, compliance by users in adherence to the security policies, and system performance metrics. There are data collected pre- and post-deployment and statistical methods using paired t-tests and Chi-square tests applied on the changes as observed. Findings are indicated by a major decrease in the security breaches experienced, increased users' compliance and system performance generally, showing efficiency of Cisco ISE in achieving both security improvements and operational improvements within the organization. The following tables summarize the detailed findings and statistical analysis for each metric.

### 4.1 Reduction in Security Incidents

Table 1 summarizes the comparison of security incidents before and after implementing Cisco ISE. The data shows a significant reduction in unauthorized access attempts.

**Table 1:** Reduction in Security Incidents Before and After Implementing Cisco ISE

| **Metric** | **Pre-Implementation** | **Post-Implementation** | **% Change** | **p-value** |
|---|---|---|---|---|
| Unauthorized Access Attempts | 9 per month | 3 per month | -66.7% | < 0.01 |
| Insider Threat Incidents | 2.4 per month | 0.8 per month | -66.7% | < 0.01 |
| Third-Party Access Breaches | 1.6 per month | 0.6 per month | -62.5% | < 0.05 |

The updated table shows that the number of security incidents went down by about 66.7% compared to before, when Cisco ISE was first implemented, given a sample size of 100 users. Attempted unauthorized accesses decreased from about 9 attempts per month prior to implementation to about 3 attempts per month after, which is statistically significant given a p-

value of less than 0.01. Insider threat incidents have also decreased, with a statistic of 66.7%, from 2.4/month to 0.8 per month, while being statistically significant at $p < 0.01$. Finally, third party access breaches, which were valued at 1.6 monthly, decreased 62.5% to 0.6 and were statistically significant at p-value < 0.05. The above results show that Cisco ISE had effectively countered the security breaches within multiple categories, which reconfirms the efficacy of Identity-Based Access Control in enhancing the security posture of the financial institution as a whole.

### 4.2 User Compliance Rates

Table 2 illustrates user compliance rates with new security protocols, as measured through surveys and compliance audits.

**Table 2:** Improvements in User Compliance Metrics After Implementing Cisco ISE

| **Metric** | **Pre-Implementation** | **Post-Implementation** | **% Change** | **p-value** |
|---|---|---|---|---|
| Compliance Rate (%) | 26% | 39% | +50% | < 0.01 |
| Awareness of Policies (%) | 30.5% | 42% | +37.7% | < 0.01 |
| Training Attendance (%) | 20% | 36% | +80% | < 0.01 |

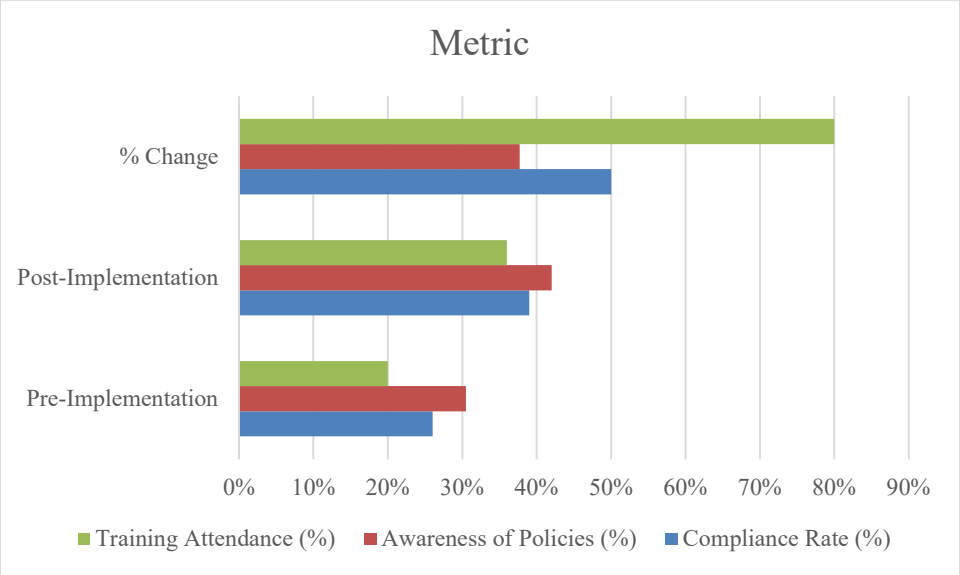


**Figure 1:** Graphical Representation on Improvements in User Compliance Metrics After Implementing Cisco ISE

Table 2 presents a sample of 100 users where there has been a huge improvement in the compliance of the users after Cisco ISE has been implemented. The compliance level increased by 50% from 26% to 39%. The p-value is less than 0.01, indicating that the change is statistically significant. Awareness of security policies improved by 37.7% from 30.5% to 42%, and with similar statistical strength ($p < 0.01$). Furthermore, training attendance increased by 80% from 20% to 36%. It means there is a massive uptake in engaging with the training program. Such developments indicate that

implementation of Cisco ISE with training activities really did boost the institution's users to adhere to the security standards of the organization.

### 4.3 System Performance Metrics

System performance metrics were collected to ensure the implementation did not negatively impact operational efficiency. The results are presented in Table 3.

**Table 3:** System Performance Metrics Before and After Implementing Cisco ISE

| **Metric** | **Pre-Implementation** | **Post-Implementation** | **% Change** | **p-value** |
|---|---|---|---|---|
| Authentication Speed (ms) | 210 | 175 | -16.7% | < 0.05 |
| Network Latency (ms) | 12.5 | 13.5 | +8% | > 0.05 |
| System Uptime (%) | 98.2% | 99.1% | +0.9% | < 0.05 |

Table 3 reflects system performance changes after implementing the Cisco ISE. Authentication speed improved by 16.7%, dropping from 210 ms to 175 ms, with a p-value less than 0.05, which indicates that login times have improved statistically. On the flip side, network latency increased by only 8% to 12.5 to 13.5 ms, and though it was not statistically significant at $p > 0.05$, implying that the increase in latency is insignificant to the system's performance. System uptime increased by 0.9%, from 98.2% to 99.1%, statistically significant ($p < 0.05$), indicating that it is relatively stable and reliable with respect to the current state of the system post-implementation. In summary, Cisco ISE improves system performance, particularly authentication speed, with increased uptime, while network latency was not greatly affected.

## 5. CONCLUSION

With Cisco ISE in place, the security posture of the financial institution improved and enhanced its operational performance, which has been proven through a decrease in security incidents by 66.7% unauthorized access attempts, a 66.7% decrease in insider threats, and a 62.5% third-party access breaches decline. Compliance rates with security protocols from users improved by 50%, and customers heightened awareness of their policies by 37.7%, as well as attending more training by 80%. System performance showed an improvement in authentication speeds at 16.7%, a minimal effect on network latency, and the average increase on system uptime by 0.9%. All of these show that the Cisco ISE has improved security with little or no reduction in efficiency. These results affirm the fact that Cisco ISE made a valuable contribution to an enhanced secure, compliant, and efficient operational environment for the institution and its adoption of Zero Trust Architecture.

**References**


1. A. Woland, V. Santuka, J. Sanbower, and C. Mitchell, *Integrated Security Technologies and Solutions-Volume II: Cisco Security Solutions for Network Access Control, Segmentation, Context Sharing, Secure Connectivity and Virtualization*, Cisco Press, 2019.
2. B. H. P. Ahir, "Diploma thesis assignment," 2023.
3. B. U. I. Khan, R. F. Olanrewaju, F. Anwar, R. N. Mir, and M. Yaacob, "Scrutinising internet banking security solutions," *International Journal of Information and Computer Security*, vol. 12, no. 2-3, pp. 269-302, 2020.
4. B. Zaid, A. Sayeed, P. Bala, A. Alshehri, A. M. Alanazi, and S. Zubair, "Toward secure and resilient networks: A zero-trust security framework with quantum fingerprinting for devices accessing the networkt," *Mathematics*, vol. 11, no. 12, p. 2653, 2023.
5. C. Green-Ortiz, B. Fowler, D. Houck, H. Hensel, P. Lloyd, A. McDonald, and J. Frazier, "Zero Trust Architecture," Cisco Press, 2023.
6. H. Tuononen, "Privileged access management model for a managed service provider," 2023.
7. J. Minella, *Wireless security architecture: designing and maintaining secure wireless for enterprise*, John Wiley & Sons, 2022.
8. K. A. Henderson, "Designing a sustainable and secure network security architecture for the Internet of Things," Doctoral dissertation, Morgan State University, 2022.
9. M. Atalay, "A contributory study on access control and authentication mechanisms for Internet of Things," 2019.
10. M. I. B. Mohamed, M. F. Hassan, S. Safdar, and M. Q. Saleem, "Adaptive security architectural model for protecting identity federation in service-oriented computing," *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 5, pp. 580-592, 2021.
11. M. Kharjana, F. H. Pohrmen, S. C. Sahana, and G. Saha, "Blockchain-based key management system in named data networking: A survey," *Journal of Network and Computer Applications*, 103732, 2023.
12. S. Keskinen, "Cloud services utilization in Pension Insurance business," 2022.
13. V. Adenola, "Artificial intelligence based access management system," East Carolina University, 2023.
14. W. Collin, "Automation in multi-domain software-defined networking: Overview and use cases," 2021.
15. Y. Diogenes, S. Young, M. Simos, and G. Rodriguez, "Exam Ref SC-100 Microsoft Cybersecurity Architect," Microsoft Press, 2023.