Journal of
Cyber Security

Tech Science Press

Doi:10.32604/jcs.2025.067514

REVIEW

Implementing a Cybersecurity Continuous User Evaluation Program

Josh McNett[1] **and Jackie McNett**[2,*]

[1]The Beacom College of Computer and Cyber Sciences, Dakota State University, Madison, SD 57042, USA
[2]The Department of Criminal Justice, Auburn University at Montgomery, Montgomery, AL 36124, USA

*Corresponding Author: Jackie McNett. Email: jmcnett@aum.edu

Received: 06 May 2025; Accepted: 03 July 2025; Published: 25 July 2025

ABSTRACT: This review explores the implementation and effectiveness of continuous evaluation programs in managing and mitigating insider threats within organizations. Continuous evaluation programs involve the ongoing assessment of individuals' suitability for access to sensitive information and resources by monitoring their behavior, access patterns, and other indicators in real-time. The review was conducted using a comprehensive search across various academic and professional databases, including IEEE Xplore, SpringerLink, and Google Scholar and papers were selected from a time span of 2015–2023. The review outlines the importance of defining the scope and objectives of such programs, which should include all personnel, contractors, and third-party vendors with access to critical systems. The review also highlights the integration of automated monitoring and alerting tools, such as Security Information and Event Management (SIEM) systems, to enhance real-time threat detection and response. Additionally, the review emphasizes the need to clearly define roles and responsibilities across various organizational levels to ensure program success, while establishing robust policies and procedures for addressing identified risks. The review underscores the importance of compliance with relevant legal and regulatory frameworks, ensuring that the continuous evaluation program does not infringe on privacy or civil liberties. Training and awareness programs are also recommended to maintain user accountability and promote a proactive security culture. Regular updates and reviews of the evaluation program are crucial for adapting to evolving threats and ensuring long-term effectiveness. This review provides organizations with the necessary guidance to implement a comprehensive continuous evaluation system to safeguard against insider threats and maintain robust personnel security.

KEYWORDS: Insider threats; security; evaluation program; continuous monitoring; user behavior analytics; SIEM

1 Introduction

In today's rapidly evolving cybersecurity landscape, insider threats pose a significant risk to organizations, often resulting in data breaches, financial losses, and damage to reputation. Insider threats, incidents where trusted individuals misuse their access to sensitive information or systems, are particularly challenging to manage due to their complexity and the need for constant vigilance. Rauf et al. (2023) noted the number of organizations experiencing an insider incident increased 15% at a cost of $648,000 per incident over the previous four years [1]. To address this, many organizations are adopting continuous user evaluation programs. These programs aim to enhance security by monitoring user behavior in real time, allowing for immediate detection and response to potential risks.

Continuous user evaluation programs leverage automated tools, such as SIEM systems, behavioral analytics, and anomaly detection algorithms, to provide an ongoing assessment of user activities. By continuously tracking access patterns and detecting unusual behavior, these programs offer a proactive approach to mitigating insider threats before they escalate. However, the implementation of continuous monitoring raises concerns about privacy, organizational transparency, and compliance with legal standards, especially as organizations strive to balance robust security with individual rights.

The specific objectives of this report are as follows:

- To define the scope and goals of a continuous user evaluation program in the context of cybersecurity, emphasizing protection of sensitive data and user accountability.
- To identify and analyze the tools and technologies, such as SIEM systems, machine learning, and threat intelligence, used to support continuous monitoring.
- To delineate the roles and responsibilities of various stakeholders, including executives, security personnel, and end-users, in implementing and maintaining the program.
- To evaluate the legal and regulatory frameworks (e.g., General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA)) that govern data protection and surveillance practices within such programs.
- To assess training and awareness strategies that reinforce secure behavior and support ethical user monitoring.
- To propose mechanisms for compliance, enforcement, and policy improvement using audits, access control principles, and incident reporting.
- To establish a framework for maintaining and adapting the program over time, ensuring it remains effective amid changing threats and evolving regulatory landscapes.

This report examines the existing research on continuous user evaluation programs, focusing on their effectiveness, implementation strategies, and the challenges faced by organizations in deploying them. The review synthesizes findings from a range of studies to identify best practices and provides organizations with actionable insights into designing effective evaluation programs. It also highlights current gaps in the literature and suggests areas for future research. By exploring these programs, this review aims to offer a comprehensive overview of continuous evaluation as a critical strategy for insider threat management, contributing to the development of resilient cybersecurity frameworks that prioritize both security and user trust.

2 Discussion

2.1 Scope and Objectives

It is important to clearly define the scope and objectives of the continuous evaluation program, including the types of sensitive information and resources that will be protected, the levels of access that will be granted or restricted, and the specific risks that the program is intended to mitigate [2]. The scope should encompass all users who access sensitive or critical systems within the organization. This includes employees, contractors, and third-party vendors. The depth of evaluation (e.g., behavior monitoring, access patterns, or specific role-based risk) needs to be determined by the plan's creator to ensure it aligns with the organization's threat landscape and compliance requirements [2]. The plan's creator should also consider the potential impact of the evaluation on individual privacy and ensure that all evaluations are carried out in a fair, transparent, and ethical manner, in line with the organization's values and policies.

A continuous evaluation program will be part of the overall computer security program (CSP) which outlines the entire security plan for a system or systems. "The CSP contains details of how the goals set out in the computer security policy are achieved" [3]. The CSP establishes the organizational roles, responsibilities, processes and procedures for implementing the computer security policy. A CSP may be specific to a facility (including its associated buildings and equipment) or an organization (including all its sites and organizational units) [3]. Therefore, it's crucial to clearly define the scope of the computer security program at the outset, taking into account the specific threats and vulnerabilities associated with the targeted facility or organization, as well as any legal and regulatory requirements that must be met. Defining the objectives of a user evaluation system is another important piece of the puzzle. Objectives should be "systematic and repeatable" and should integrate well into the existing security policies [4]. Example objectives are as follows:

- Mitigate Insider Threats: The primary goal of a user evaluation program is to proactively identify potential insider threats by continuously monitoring user behavior and access patterns. This should involve ongoing assessments rather than periodic checks [2]. Furthermore, the user evaluation program should be designed in a way that balances the need for security with the need to maintain user trust and privacy, and should include clear communication channels for users to report any concerns or issues related to the evaluation.
- Ensure Compliance: The program should help maintain regulatory compliance, ensuring that user activities conform to the necessary legal and policy frameworks [2]. This will aid in reducing legal and financial risks, protecting the organization's reputation, and ensuring the confidentiality, integrity, and availability of sensitive information and systems.
- Risk Management: The program should incorporate risk assessment mechanisms, focusing on high-risk users, such as those with elevated privileges or access to sensitive data [2]. By prioritizing high-risk users, the program can more effectively allocate resources and attention to the areas of greatest need, ensuring that the organization's most valuable assets are protected while minimizing disruptions to normal operations.
- Enhance User Accountability: Through continuous evaluation, you create a culture of accountability, where users are aware that their actions are monitored in real time, leading to more responsible behavior [2]. This culture of accountability can also serve as a deterrent against potential insider threats, as users are more likely to think twice before engaging in risky or malicious activities when they know they are being monitored, thereby enhancing the overall security posture of the organization.
- Risk Mitigation: A primary objective is to reduce vulnerabilities and mitigate risks from cyber threats like malware, ransomware, and phishing. This includes establishing monitoring systems and incident response strategies [2]. The program should regularly review and update its strategies and tactics, staying abreast of the latest threats and trends in the cybersecurity landscape, and adapting to changing circumstances and needs within the organization.

2.2 Tools and Technologies

To ensure a robust cybersecurity posture, continuous evaluation programs must incorporate automated monitoring and alerting systems capable of identifying potential risks and triggering further investigation or action. These systems often utilize advanced software tools or services that can monitor and analyze data streams from multiple sources in real-time, issuing alerts when unusual activities or security threats are detected. Automated monitoring and alerting enable organizations to stay ahead of potential vulnerabilities by providing constant oversight and rapid incident detection.

A key component of such systems is SIEM platforms. SIEM systems aggregate data from various security sources such as firewalls, intrusion detection systems, and antivirus tools, offering centralized visibility into potential security events [5]. This integrated approach allows organizations to detect and responds to cybersecurity threats in real-time. By correlating events across systems, SIEM solutions generate actionable alerts that can reduce incident response times and streamline overall security operations [5]. The flowchart in Fig. 1 below illustrates how a typical SIEM system functions [5]. The correlation of disparate security data into a coherent picture helps security teams focus on true positives, minimizing noise from false alerts.

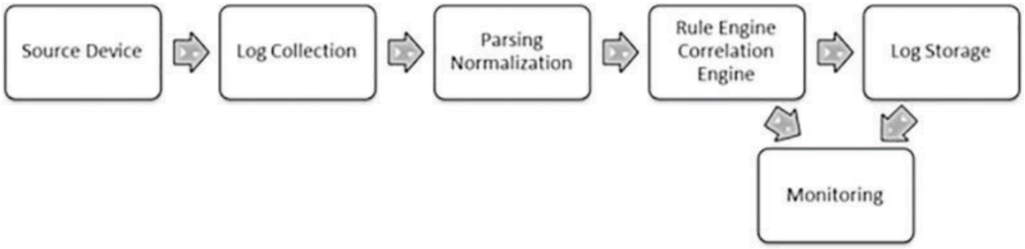


Figure 1: SIEM flowchart [5]

Recent research highlights the growing importance of integrating SIEM platforms with big data analytics to improve threat detection capabilities. The use of big data enhances the scalability and efficiency of SIEM systems, enabling them to handle large volumes of data while identifying patterns that might otherwise go unnoticed [6]. By incorporating machine learning algorithms, these systems can better detect evolving threats and anomalies, continuously learning from new data to improve their response accuracy [6]. This not only enhances the overall effectiveness of the security program, but also reduces the workload on human analysts, allowing them to focus on more complex and high-priority tasks, thereby increasing the organization's overall security posture.

Continuous monitoring is essential for maintaining an organization's security posture, providing up-to-the-minute insights into network and system behavior. Advanced monitoring tools perform real-time behavioral analysis and anomaly detection, leveraging automated alert systems to catch potential threats before they escalate into larger security incidents [6]. Artificial intelligence (AI) and machine learning (ML) technologies play a significant role in enhancing continuous monitoring. These technologies allow for predictive analytics, which can identify emerging patterns indicative of future threats [6]. The ability to anticipate threats not only improves response times but also reduces the rate of false positives, thereby optimizing operational efficiency. Additionally, using these technologies to aid in the tracking of Key Performance Indicators (KPIs) like the rate of false positives, enables organizations to gauge the effectiveness of their continuous user evaluation programs and focus on improving weak areas as necessary.

Tuning thresholds in SIEM systems is crucial to minimize false positives. To do this, first understand the SIEM system and its rules, analyze false positives to identify sources and causes, and adjust threshold values accordingly [7]. Consider increasing the threshold value, adjusting the time window, or implementing rate-based thresholds to reduce false positives. Additionally, use statistical models and machine learning, implement whitelisting and blacklisting, and leverage SIEM system features such as alert suppression, escalation, and event filtering [7]. By continuously monitoring and refining the thresholds, you can improve the effectiveness of your SIEM system. For example, adjusting a rule that triggers an alert for failed login attempts from 5 attempts within 1 min to 10 attempts within 5 min, and implementing a rate-based threshold to trigger an alert when the login attempt rate exceeds 20 attempts per minute, can help minimize false positives and reduce unnecessary resource utilization.

Cyber Threat Intelligence (CTI) further strengthens monitoring systems by providing real-time data on emerging threats, vulnerabilities, and adversary tactics. CTI platforms often integrate with SIEM systems and other security tools to offer a multi-layered approach to cybersecurity, leveraging signature based, behavior-based, and anomaly-based detection models [8]. With CTI, organizations can take proactive measures to defend against new types of attacks, as the system constantly updates with intelligence on the latest tactics used by cyber adversaries [8]. Cyber threat intelligence is a critical component of a modern security program, providing organizations with the knowledge and insights they need to defend against new types of attacks, collaborate with the wider security community, prioritize their security efforts, and anticipate and prepare for emerging threats.

Two more tools should be mentioned, data loss prevention (DLP), and user and behavior analytics (UEBA). DLP and UEBA are two distinct security solutions that serve different purposes. DLP is primarily focused on preventing unauthorized data transfer or exfiltration, typically through monitoring and controlling data movement at the network perimeter or on endpoints [9]. In contrast, UEBA is a more comprehensive solution that analyzes user and entity behavior to identify potential security threats, including insider threats, compromised accounts, and lateral movement [9]. While DLP can detect and prevent data exfiltration attempts, UEBA provides a more nuanced understanding of user behavior, allowing for the detection of anomalies and potential threats that may not be related to data exfiltration [9]. For example, UEBA can identify a user accessing sensitive data outside of normal working hours or from an unusual location, whereas DLP would only detect if the user attempted to transfer the data outside the organization. By combining DLP and UEBA, organizations can gain a more complete understanding of their security posture and improve their ability to detect and respond to potential threats.

It is important to note that there is no single solution for automated monitoring and alerting in cybersecurity [10]. Organizations must adopt a combination of technologies and strategies, including access controls, user behavior analytics, and insider threat detection systems, to address the complex landscape of potential security risks [4].

When deciding on technology solutions to implement, organizations must consider a multitude of factors. A key aspect of this decision-making process is evaluating the cost, scalability, and latency of various solutions, as illustrated in Table 1 for SIEM, UEBA, and DLP solutions. However, these factors are just the beginning, as organizations must also consider numerous other elements to determine which monitoring system will best suit their unique environment.

Table 1: SIEM, UEBA, DLP comparison

Tool	Cost	Scalability	Latency
SIEM	High ($50k–$500k)	High (supports thousands of devices)	Low (real-time, <1 min)
UEBA	Medium–high ($20k–$200k)	Medium-high (supports hundreds to thousands of users)	Medium (near real-time, 1–10 min)
DLP	Medium ($10k–$100k)	Medium (supports hundreds to thousands of devices)	Medium (near real-time, 1–10 min)

By combining monitoring systems with robust access controls and behavioral analytics, organizations can significantly enhance their ability to detect and prevent malicious activities, unauthorized access, and data exfiltration by insiders. For instance, user behavior analytics can identify deviations from normal user activity, flagging potential insider threats before they cause substantial damage. This proactive approach enables organizations to stay one step ahead of potential security breaches, ultimately protecting their sensitive data and maintaining the integrity of their systems.

In conclusion, automated monitoring and alerting systems, when coupled with SIEM platforms, continuous monitoring, and CTI form a comprehensive approach to safeguarding organizational assets.

However, organizations should remain flexible in their approach, using a variety of tools and strategies to ensure they can respond swiftly and effectively to an ever-evolving threat landscape.

2.3 Roles and Responsibilities

It is important to clearly define roles and responsibilities for managing and operating the continuous evaluation program, including who is responsible for monitoring data, investigating potential risks, and making decisions about access and security.

Defining roles and responsibilities within a cybersecurity user evaluation plan is crucial for the program's effectiveness and clarity. Key roles typically include senior management, security officers, system administrators, and users, each with specific duties that contribute to the overall security posture.

Senior Management: As outlined in various frameworks, including the NIST SP 800-12, senior management is responsible for setting the overall objectives of the cybersecurity program, ensuring that adequate resources are allocated, and establishing accountability within the organization. Their role involves defining the scope of the cybersecurity evaluation and making high-level decisions to support the program's success [11]. Senior management plays a critical role in the success of the cybersecurity program, providing resources and support, integrating security into all aspects of the organization's operations, serving as role models, and regularly reviewing and updating the program to ensure its continued effectiveness and relevance.

Security Officers (e.g., CISO): The Chief Information Security Officer (CISO) or equivalent security officer is responsible for the day-to-day management of cybersecurity, particularly the monitoring and evaluation of user activities. This role involves overseeing the security architecture, ensuring policy compliance, and directly managing risk mitigation strategies as highlighted in frameworks such as COBIT 5 and other organizational security policies [11]. The CISO's end goal is to ensure that the organization is able to maintain a strong and resilient security posture, protect its assets and reputation, and meet its legal and regulatory obligations.

System Administrators/Technical Staff: These personnel are tasked with implementing the technical aspects of the user evaluation plan. This includes setting up monitoring tools, managing access controls, and ensuring that systems are secure. Their role is to continuously assess and respond to potential vulnerabilities or suspicious activities within the network [12]. The system administrator should also be responsible for implementing and maintaining the organization's security policies and procedures, ensuring that all systems and networks are configured and operated in accordance with best practices and industry standards. This includes managing user accounts and access rights, configuring firewalls and intrusion detection systems, and implementing security controls and countermeasures to protect against threats and vulnerabilities [12]. By taking these steps, the system administrator can help to ensure that the organization's networks and systems are secure, reliable, and available, and that the organization is able to maintain a strong and resilient security posture.

Users: In a user evaluation plan, all individuals who access the system play a critical role. Their responsibilities include following the organization's security protocols, attending cybersecurity awareness training, and reporting any suspicious activities. Users must comply with access control policies and maintain good cybersecurity practices as part of their daily operations [13]. Users must also be vigilant and proactive in identifying and reporting any potential security incidents or suspicious activities and should promptly respond to any security-related communications or instructions from the security team. This includes following established procedures for reporting incidents and cooperating fully with the security team during incident response and recovery efforts [13]. By taking these steps, users can help to ensure that the organization is able to maintain a strong and resilient security posture, protect its assets and reputation, and meet its legal and regulatory obligations.

2.4 Policy Framework and Enforcement

Continuous evaluation programs should include policies and procedures for handling potential risks, including how to investigate and verify the accuracy of alerts, and how to take appropriate action to mitigate any identified risks. Establishing effective cybersecurity policies and procedures for user management involves several key components that align with recognized standards and frameworks. Peer-reviewed sources suggest a multi-layered approach that incorporates technical, procedural, and human factors.

Frameworks and Policy Models: A robust information security policy typically adheres to frameworks like the NIST Cybersecurity Framework or ISO 27001 [13]. These frameworks help define roles, responsibilities, and processes for managing user access, authentication, and overall security controls. These frameworks define roles and responsibilities for all stakeholders, including senior management, security officers, system administrators, and users, and establish clear processes for managing user access, authentication, and overall security controls [13]. This helps to ensure that everyone understands their role in maintaining the organization's security posture, and that security is integrated into all aspects of the organization's operations.

Compliance and Enforcement: Studies stress the importance of balancing deterrence strategies (e.g., disciplinary measures for non-compliance) with positive reinforcement, such as training programs that encourage secure behavior [14]. Security personnel should provide regular training and awareness programs, to help users understand the importance of security, and to provide them with the knowledge and skills they need to comply with security policies and procedures [14]. These training and awareness programs should be interactive, engaging, and relevant to the user's role and responsibilities, and should be tailored to the user's level of knowledge and experience [14]. Clear consequences for non-compliance with security policies and procedures should be established, and security personnel should consistently enforce these consequences [14]. This can help to discourage risky behavior and reinforce the importance of security. Consequences can take many forms, such as disciplinary action, loss of privileges, or education and training, and should be tailored to the user's actions and motivations.

Deterrence Strategies: Disciplinary measures serve as effective deterrents for non-compliance. The threat of consequences, such as warnings, reduced access, or even job termination, can motivate users to follow cybersecurity protocols [14]. Studies have shown that clear and consistent enforcement of these measures is key to their success. However, overreliance on punishment may lead to resentment or minimal compliance.

Positive Reinforcement: On the other hand, training programs that build cybersecurity awareness and skills are crucial for fostering a proactive security culture. Regular engaging training helps users understand their role in protecting organizational data and the consequences of security lapses [14]. Positive incentives, such as recognition programs or reward systems for users who demonstrate secure behavior, can further encourage adherence to policies.

Integrated Security Culture: For long-term success, organizations must strive to create an integrated security culture, where security becomes a shared responsibility [14]. This culture is cultivated by: Ongoing training tailored to different user levels, communicating the importance of cybersecurity in achieving organizational goals, and providing tools and resources that make compliance easier, like password managers or automated access controls.

Layered Policy: Best practices recommend a layered approach to information security policies. This includes a basic policy for public communication, specific security regulations for internal use, and detailed procedures for daily operations [15]. Each layer addresses different aspects of user management, such as role-based access and secure authentication methods.

Behavioral Factors: User behavior is a critical component in maintaining a strong cybersecurity posture, as employees frequently serve as both the first line of defense and the most targeted point of vulnerability. While technical controls are necessary, they must be supported by policies that address the psychological and behavioral dimensions of cybersecurity. Social engineering attacks, such as phishing, pretexting, and baiting, exploit human psychology and social norms, making it imperative that users are trained to recognize and respond to these deceptive tactics [16]. Traditional technical defenses often fall short in detecting such manipulations, which underscores the importance of equipping employees with the knowledge and confidence to act as proactive defenders.

However, the increasing use of continuous surveillance in the workplace, such as keystroke logging, behavioral analytics, and screen recording, introduces complex behavioral and ethical implications. While these tools can detect anomalies and deter insider threats, they may also erode employee morale, diminish trust in leadership, and foster a culture of fear and compliance rather than genuine engagement with security protocols [16]. Over-surveillance may lead to a chilling effect, where employees alter their behavior not to improve security but to avoid punitive scrutiny, ultimately suppressing creativity, collaboration, and initiative.

To mitigate these risks, organizations should adopt a privacy-aware approach to surveillance. This begins with transparency: clearly communicating what is being monitored, why, and how the data will be used fosters trust and informed consent. Surveillance should also adhere to the principle of proportionality, ensuring that monitoring is limited to what is necessary for legitimate security purposes. For example, instead of blanket screen recording, systems could rely on anomaly-based alerts that only trigger reviews when irregular activity is detected [16].

Organizations should also promote psychological safety by encouraging employees to report mistakes or suspicious activity without fear of punishment. User-centric training programs that use interactive simulations, personalized feedback, and gamified learning can reinforce secure behavior more effectively than generic awareness sessions. Additionally, behavioral insights from monitoring data should be used not only for enforcement but to identify usability issues or training needs, such as frequent password resets indicating design flaws rather than carelessness.

Implementing ethical oversight is equally important. Internal data governance committees or ethics boards should review surveillance practices to ensure they are fair, legal, and consistent with organizational values. Differentiated monitoring strategies based on risk profiles can also help balance security and privacy, for instance, more stringent monitoring for users with elevated privileges and less intrusive methods for general staff.

Ultimately, while continuous surveillance offers substantial benefits in identifying and mitigating cybersecurity risks, it must be deployed thoughtfully. When grounded in behavioral science and ethical principles, surveillance can support rather than suppress a culture of security. By designing monitoring systems that respect privacy, foster trust, and promote user accountability, organizations can turn their workforce into a proactive and engaged line of defense against evolving threats.

2.5 Legal and Regulatory Compliance

Continuous evaluation programs must comply with all relevant laws and regulations, including those related to privacy, civil liberties, and equal employment opportunity. It is important to carefully consider the legal and ethical implications of the program, and to implement appropriate safeguards to protect individuals' rights and privacy. When creating a cybersecurity continuous user management system, ensuring compliance with relevant laws and regulations is essential. Various standards and frameworks provide guidance on this, such as ISO/IEC 27001 and the NIST Cybersecurity Framework. These frameworks offer a structured approach to managing cybersecurity risks while adhering to legal requirements, focusing on privacy, access controls, and data protection.

Data Protection Laws: Laws such as the General Data Protection Regulation (GDPR) in Europe and California Consumer Privacy Act (CCPA) in the U.S. impose strict rules on managing user data, with the goal of protecting the privacy and security of individuals' personal information [17]. These laws mandate clear policies for data collection, storage, and access, ensuring that personal data is only accessible to authorized personnel and is handled securely, in accordance with established policies and procedures.

The GDPR, in particular, sets a high bar for data protection and privacy, and imposes significant fines and penalties for non-compliance. It applies to all organizations that process the personal data of EU residents, regardless of where the organization is located, and requires organizations to obtain explicit and informed consent from individuals before collecting and processing their personal data [18]. It also gives individuals the right to access, rectify, erase, and restrict the processing of their personal data, and requires organizations to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

The CCPA, on the other hand, applies to for-profit organizations that do business in California and collect personal information from California residents, and gives individuals the right to know what personal information is being collected, used, and disclosed, and to opt-out of the sale of their personal information [19]. It also requires organizations to implement reasonable security measures to protect personal information against unauthorized access, destruction, use, modification, or disclosure.

Both the GDPR and CCPA emphasize the importance of transparency, accountability, and individual rights, and require organizations to document and demonstrate their compliance with the regulations. They also require organizations to conduct regular risk assessments, data protection impact assessments, and data protection audits, and to implement incident response plans and data breach notification procedures.

Access Control and Authentication: Identity and access management (IAM) systems play a critical role in cybersecurity, as they help organizations to manage user identities, access rights, and authentication methods in a secure and controlled manner. IAM systems must comply with regulations that emphasize the principle of least privilege and separation of duties, ensuring that users are granted the minimum level of access and permissions necessary to perform their job functions, and that access is distributed among multiple users to prevent fraud, error, and misuse [20]. This will minimize the risk of users operating in unintended ways.

Access to sensitive information should be restricted based on roles, and mechanisms like multi-factor authentication (MFA) are often recommended or required by standards such as NIST, to ensure that only authorized and authenticated users can access sensitive information [20]. MFA combines something the user knows (a password or PIN), something the user has (a security token or smart card), and something the user is (a biometric factor like a fingerprint or facial recognition), providing an additional layer of security and reducing the risk of unauthorized access.

IAM systems should also provide role-based access control (RBAC), where access rights and permissions are assigned based on the user's role within the organization, rather than on individual users [20]. This helps to reduce the complexity and administrative burden of managing access rights and ensures that users have the appropriate level of access and permissions based on their job functions.

Cyber Incident Reporting: Many jurisdictions, such as the U.S. under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), require organizations to report data breaches or cyber incidents within a specific time frame [17]. This requirement is designed to ensure that organizations promptly notify affected individuals, regulators, and law enforcement agencies of potential security incidents, and provide them with the necessary information to take appropriate action.

The CIRCIA, for example, requires certain critical infrastructure sectors, such as energy, financial services, and healthcare, to report significant cyber incidents to the Department of Homeland Security within 72 h of discovery [21]. Failure to comply with this requirement can lead to significant fines, as well as reputational damage and legal liability.

Regular Audits and Updates: Compliance with laws and regulations isn't a one-time effort, but rather an ongoing process that involves conducting regular audits, updating policies to reflect changing legal landscapes, and ensuring that all systems are aligned with the latest regulatory requirements. Regular audits are essential to ensuring compliance, as they help organizations to identify potential weaknesses and gaps in their security posture, and to implement corrective actions and preventive measures to prevent security incidents and breaches [22]. Audits can be conducted internally, by the organization's security personnel, or externally, by third-party auditors, and should be based on established frameworks, standards, and best practices, such as the NIST Cybersecurity Framework, ISO 27001, or COBIT. Updating policies to reflect changing legal landscapes is also critical, as laws and regulations are constantly evolving to address new threats and vulnerabilities, and to keep pace with technological advancements [22]. Organizations should regularly review and update their policies, procedures, and guidelines, to ensure that they remain compliant with the latest regulatory requirements, and that they reflect the organization's current risk profile and security posture.

Regulatory Compliance: The program should ensure compliance with industry regulations, such as the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the U.S., to avoid legal and financial repercussions [17]. These regulations set specific requirements for how organizations manage and protect personal data and impose significant fines and penalties for non-compliance. The GDPR, for example, applies to all organizations that process the personal data of EU residents, regardless of where the organization is located, and requires organizations to obtain explicit and informed consent from individuals before collecting and processing their personal data [18]. It also gives individuals the right to access, rectify, erase, and restrict the processing of their personal data, and requires organizations to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. HIPAA, on the other hand, applies to covered entities, such as healthcare providers, health plans, and healthcare clearinghouses, and their business associates, and requires them to implement administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI) [23]. It also requires organizations to notify affected individuals, the Secretary of the Department of Health and Human Services, and, in some cases, the media, of any breaches of ePHI.

By integrating these regulatory frameworks into the cybersecurity user management system, organizations can mitigate risks and maintain compliance with global standards. This can be achieved by conducting regular risk assessments, data protection impact assessments, and data protection audits, and by implementing incident response plans and data breach notification procedures.

2.6 Impact of GDPR, HIPAA, and CCPA on Continuous User Evaluation Programs

Continuous user evaluation programs must operate within the boundaries of national and international data protection laws, particularly the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the California Consumer Privacy Act (CCPA). Each of these regulations imposes specific obligations that directly influence how user behavior is monitored, how data is collected and processed, and how organizations safeguard personal information.

Under the GDPR, any organization processing the personal data of EU residents is required to obtain explicit, informed consent prior to data collection, implement data minimization practices, and ensure transparency in data handling procedures [18]. For continuous evaluation programs, this means limiting monitoring to necessary data points, clearly communicating monitoring practices to users, and securing the data with robust technical and organizational controls. Organizations must also provide users with rights such as access, rectification, erasure, and the ability to restrict processing. Failure to comply can result in significant financial penalties and reputational harm [18].

HIPAA imposes equally stringent requirements in the U.S. healthcare sector. Organizations designated as covered entities or business associates must safeguard electronic protected health information (ePHI) through administrative, physical, and technical safeguards [23]. For continuous evaluation programs in healthcare settings, this means ensuring that access to ePHI is closely monitored and that all evaluation mechanisms are compliant with HIPAA's Privacy and Security Rules. Additionally, in the event of a breach, affected individuals, regulators, and in some cases, the media must be notified promptly, typically within 60 days, in accordance with HIPAA's Breach Notification Rule [23].

The CCPA governs the use of personal information of California residents and mandates that individuals be informed about what data is collected, how it is used, and whether it is sold or shared. It grants users the right to access their data, request its deletion, and opt-out of data sales [19]. For continuous evaluation programs, the CCPA requires implementing processes for data access and deletion requests, ensuring transparency in monitoring practices, and establishing safeguards against unauthorized data use. The law also necessitates reasonable security measures to prevent breaches of personal data, aligning with the technical expectations outlined in cybersecurity frameworks like NIST.

In summary, compliance with these laws is not optional but foundational to the design and operation of continuous evaluation programs. Organizations must adopt privacy-by-design principles, conduct regular risk and impact assessments, and maintain auditable records to demonstrate regulatory adherence. By aligning evaluation practices with the GDPR, HIPAA, and CCPA, organizations not only reduce legal exposure but also build trust with users by upholding their rights and privacy.

2.7 Training and Awareness

It is important to provide training and awareness to all relevant personnel on the continuous evaluation program, including its purpose, scope, and procedures, as this can help to ensure that the program is implemented effectively and that all personnel understand their roles and responsibilities. This can be achieved through a combination of in-person training sessions, online courses, and awareness campaigns, and should be tailored to the user's role and responsibilities and should be relevant to the user's level of knowledge and experience [13]. The training and awareness programs should cover topics such as the purpose and scope of the continuous evaluation program, the types of data and systems that are being evaluated, the procedures and methods for evaluating user behavior and access patterns, and the consequences of non-compliance [13]. They should also cover best practices for cybersecurity, such as password management, safe browsing, email and social media usage, and physical security.

Promoting cybersecurity awareness is also crucial, as human errors, such as falling for phishing emails or using weak passwords, are a leading cause of security incidents and breaches. By providing regular training and awareness programs, organizations can help to ensure that employees are aware of the risks and threats associated with cybersecurity, and of the steps they can take to protect themselves and the organization. These training and awareness programs should be interactive, engaging, and relevant to the user's role and responsibilities, and should be tailored to the user's level of knowledge and experience.

Implementing a successful cybersecurity awareness and training program involves several critical components that contribute to its effectiveness: Tailored Content: Training programs should be customized to match the specific roles and access levels of employees. For example, system administrators need training on handling privileged accounts, while regular users require instruction on basic security practices like password management and phishing awareness [24]. This ensures that employees receive relevant and practical information that applies directly to their day-to-day activities. Content can be tailored towards user groups as follows [11]:

- Executive Leadership (C-Suite and Senior Management) Focus: High-level awareness and strategic decision-making
- IT and Security Teams Focus: Advanced technical skills and operational security
- General Employees (Non-Technical Staff) Focus: Basic cybersecurity hygiene and awareness
- HR and Finance Departments Focus: Protecting sensitive personal and financial data
- Developers and Software Engineers Focus: Secure development practices and code integrity
- Legal and Compliance Teams Focus: Regulatory compliance and legal implications of cybersecurity
- Remote and Mobile Workers Focus: Securing remote work environments and mobile devices
- Third-Party Vendors and Contractors Focus: Compliance with organizational security policies
- New Hires and Interns Focus: Introduction to organizational security culture and policies
- Board of Directors Focus: High-level oversight and strategic alignment

Engagement and Gamification: Incorporating interactive elements such as serious games, micro-learning modules, and real-time progress tracking, can significantly enhance user engagement and knowledge retention, as they provide a more engaging and interactive learning experience, and allow users to learn at their own pace and in a more personalized manner [25]. The iCAT (Integrated Cybersecurity Awareness Training) model, for example, leverages these tools to improve learning outcomes and adaptability for various types of learners, by providing a more engaging and interactive learning experience, and by allowing users to learn at their own pace and in a more personalized manner. This can help to ensure that users are more engaged, motivated, and better prepared to apply their knowledge and skills in real-world situations, and that they are able to retain and recall the information more effectively. The iCAT model also incorporates gamification elements, such as leaderboards, badges, and rewards, to further enhance user engagement and motivation [25]. These gamification elements can help to create a more positive and enjoyable learning experience, and can encourage users to compete, collaborate, and share their knowledge and skills with others. In addition to these measures, the iCAT model also incorporates real-time progress tracking, where users can track their progress, receive feedback, and measure their performance, and where administrators can monitor user progress, identify potential weaknesses and gaps, and provide targeted feedback and guidance [25]. This can help to ensure that users are able to monitor their progress, stay motivated, and receive the necessary support and guidance, and that administrators are able to identify potential weaknesses and gaps, and to implement corrective actions and preventive measures to prevent security incidents and breaches.

Regular Updates and Reinforcement: Continuous reinforcement of security practices is vital, as cybersecurity threats evolve rapidly, and new threats and vulnerabilities emerge on a daily basis. Regularly updating training materials and ensuring that employees are reminded of best practices can help maintain high levels of awareness over time and can help to ensure that employees are able to recognize, respond to, and prevent security incidents and breaches [26]. Continuous reinforcement can be achieved through a combination of regular training and awareness programs, reminders, and updates, and should be tailored to the user's role and responsibilities and should be relevant to the user's level of knowledge and experience [26]. For example, organizations can provide regular refresher courses, updates on the latest threats and vulnerabilities, and reminders of best practices, such as password management, safe browsing, email and social media usage, and physical security. Regularly updating training materials is also important, as outdated or irrelevant training materials can lead to confusion, misinformation, and misconceptions, and can increase the risk of security incidents and breaches. Organizations should regularly review and update their training materials, to ensure that they reflect the latest regulatory requirements, and that they reflect the organization's current risk profile and security posture [26]. In addition to these measures, organizations should also establish a culture of security, where security is seen as a shared responsibility, and where employees are encouraged to report suspicious or anomalous activity, and to take an active role in protecting the organization's assets and data. This can be achieved through regular communication, feedback, and recognition, where employees are informed of the organization's security posture, are given feedback on their performance, and are recognized for their contributions to maintaining a strong and resilient security posture.

Measurement of Effectiveness: It is important to assess the impact of training programs through metrics like incident reports, phishing simulation results, and surveys, as this can help organizations to evaluate the effectiveness and impact of their training programs, and to adapt the training program as needed based on these evaluations [24]. By integrating these elements, organizations can build a robust awareness and training program that not only educates users but also fosters a proactive security culture, where users are more engaged, motivated, and better prepared to apply their knowledge and skills in real-world situations, and where security is seen as a shared responsibility.

Incident reports can provide valuable insights into the types and frequency of security incidents and breaches and can help organizations to identify potential weaknesses and gaps in their security posture, and to implement corrective actions and preventive measures to prevent similar incidents in the future [24]. By tracking improvements in employee behavior, organizations can evaluate the impact of their training programs on employee behavior and can identify potential areas for improvement and adaptation.

Phishing simulation results can help organizations to evaluate the effectiveness of their phishing awareness and training programs, and to identify potential weaknesses and gaps in their defenses. By tracking improvements in employee behavior, organizations can evaluate the impact of their training programs on employee behavior and can identify potential areas for improvement and adaptation.

Surveys can provide valuable insights into user perceptions, attitudes, and behaviors related to cybersecurity, and can help organizations to evaluate the effectiveness and impact of their training programs, and to identify potential weaknesses and gaps in their security posture, and to implement corrective actions and preventive measures to prevent security incidents and breaches.

By integrating these elements, organizations can build a robust awareness and training program that not only educates users but also fosters a proactive security culture, where users are more engaged, motivated, and better prepared to apply their knowledge and skills in real-world situations, and where security is seen as a shared responsibility [24]. This can help to ensure that users are able to recognize, respond to, and prevent security incidents and breaches, and that they are able to retain and recall the information more effectively. In addition to these measures, organizations should also establish a culture of security, where security is seen as a shared responsibility, and where employees are encouraged to report suspicious or anomalous activity, and to take an active role in protecting the organization's assets and data [10]. This can be achieved through regular communication, feedback, and recognition, where employees are informed of the organization's security posture, are given feedback on their performance, and are recognized for their contributions to maintaining a strong and resilient security posture. Organizations should also establish incident response plans and data breach notification procedures, as part of their overall cybersecurity strategy [24]. These plans should provide clear and concise guidance on how to detect, respond to, and recover from security incidents and data breaches, and should be regularly tested and updated to ensure that they remain effective and relevant.

2.8 Program Maintenance and Adaptation

Continuous evaluation programs should be regularly reviewed and updated to ensure that they remain effective and relevant to the organization's needs and risks. This may involve revising data sources, methods, policies, and procedures as needed, and ensuring that the program is aligned with any changes in the organization's risk profile or regulatory environment. Regularly reviewing and updating a cybersecurity user management program is crucial to maintaining its effectiveness in a rapidly evolving threat landscape. To achieve this, several best practices can be implemented based on peer-reviewed research.

Continuous Monitoring and Feedback: A successful approach to regularly updating cybersecurity programs involves continuous monitoring as outlined by the NIST framework (SP 800-37 and SP 800-137) [27]. These guidelines emphasize the importance of ongoing assessment of security controls and using real-time feedback to adjust policies and technologies as needed [27]. This includes tracking system vulnerabilities, reviewing user behaviors, and adjusting access control protocols accordingly.

Risk Management and Compliance Frameworks: Incorporating frameworks like NIST's Risk Management Framework (RMF) allows organizations to periodically evaluate their security controls in the context of evolving threats and compliance requirements. The RMF provides a structured and systematic approach to managing cybersecurity risks, and includes a set of standards, guidelines, and best practices for assessing, categorizing, selecting, implementing, and monitoring security controls [12]. By incorporating the RMF, organizations can ensure that they have a comprehensive and consistent approach to managing their cybersecurity risks, and that they are able to adapt to evolving threats and compliance requirements. The RMF includes a set of categories and subcategories of security controls, such as access control, awareness and training, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, and system and information integrity [12]. By periodically evaluating these security controls, organizations can ensure that they remain compliant with legal and regulatory changes, and that they are able to adapt to evolving threats and vulnerabilities. Regularly reassessing these controls can also help organizations to identify potential weaknesses and gaps in their security posture, and to implement corrective actions and preventive measures to prevent security incidents and breaches [12]. For example, organizations can reassess their access control policies and procedures, to ensure that they are aligned with the latest regulatory requirements, and that they reflect the organization's current risk profile and security posture [12]. They can also reassess their incident response plans and data breach notification procedures, to ensure that they remain effective and relevant, and that they are able to detect, respond to, and recover from security incidents and data breaches in a timely and effective manner. Incorporating the RMF into the organization's cybersecurity strategy can also help to ensure that the organization is able to maintain a strong and resilient security posture, meet its legal and regulatory obligations, and protect its users' personal information. The RMF provides a comprehensive and consistent approach to managing cybersecurity risks and helps organizations to ensure that they are able to adapt to evolving threats and compliance requirements. Incorporating frameworks like NIST's Risk Management Framework (RMF) allows organizations to periodically evaluate their security controls in the context of evolving threats and compliance requirements. By reassessing these controls regularly, organizations can ensure that they remain compliant with legal and regulatory changes, identify potential weaknesses and gaps in their security posture, and implement corrective actions and preventive measures to prevent security incidents and breaches. By incorporating the RMF into the organization's cybersecurity strategy, organizations can help to ensure that they are able to maintain a strong and resilient security posture, meet their legal and regulatory obligations, and protect their users' personal information.

Automation and Manual Reviews: Automated tools can handle the bulk of security monitoring tasks, such as log analysis, user activity tracking, and anomaly detection, by processing large volumes of data in real-time, and by identifying patterns, trends, and anomalies that may indicate potential security incidents and breaches [27]. By automating these tasks, organizations can improve their efficiency, accuracy, and speed, and can reduce the burden on their security personnel. However, manual reviews are necessary to evaluate the effectiveness of these tools and address areas where human oversight is essential [27]. This dual approach, combining automated tools and manual reviews, ensures that gaps in automated processes are identified and mitigated, and that the organization is able to maintain a strong and resilient security posture. Manual reviews can provide additional context, insight, and expertise, and can help to ensure that automated tools are configured, tuned, and calibrated correctly, and that they are aligned with the organization's risk profile and security posture [27]. Manual reviews can also help to evaluate the effectiveness of the automated tools, and to identify potential weaknesses and gaps in their performance, and to implement corrective actions and preventive measures to prevent security incidents and breaches. Manual reviews can also be used to address areas where human oversight is essential, such as in the evaluation of complex or sensitive systems, in the assessment of insider threats, and in the analysis of advanced persistent threats (APTs) [27]. Manual reviews can provide the necessary level of expertise, experience, and judgement, and can help to ensure that the organization is able to detect, respond to, and recover from security incidents and breaches in a timely and effective manner. By combining automated tools and manual reviews, organizations can build a robust security monitoring program that provides the necessary level of coverage, accuracy, and speed, and that is able to adapt to evolving threats and vulnerabilities [27]. This dual approach can help to ensure that the organization is able to maintain a strong and resilient security posture, meet its legal and regulatory obligations, and protect its users' personal information. Automated tools can handle the bulk of security monitoring tasks, such as log analysis and user activity tracking, but manual reviews are necessary to evaluate the effectiveness of these tools and address areas where human oversight is essential. By combining automated tools and manual reviews, organizations can build a robust security monitoring program that provides the necessary level of coverage, accuracy, and speed, and that is able to adapt to evolving threats and vulnerabilities. By establishing incident response plans and data breach notification procedures, organizations can help to ensure that they are able to maintain a strong and resilient security posture, meet their legal and regulatory obligations, and protect their users' personal information.

Periodic Audits and Metrics: Regular audits play a vital role in evaluating the performance of user management programs in an organization. These audits use clear metrics, such as the number of incidents, user compliance rates, and the effectiveness of access control systems, to assess various aspects of user management [28]. By integrating continuous monitoring, compliance frameworks, and a combination of automated and manual checks, organizations can maintain and improve their cybersecurity user evaluation programs effectively [27]. Continuous monitoring helps detect potential security threats and vulnerabilities in real-time, allowing for quicker response times and more effective mitigation strategies. Adopting industry-standard compliance frameworks ensures that user management programs meet or exceed established security benchmarks. A combination of automated tools and manual reviews provides a more comprehensive assessment of user management programs, as automated tools can help identify patterns and anomalies, while manual checks can provide more in-depth analysis and context [28]. By incorporating these best practices, organizations can ensure a secure and compliant environment for their users and data.

2.9 Discussion Summary

In conclusion, this review underscores the importance of a well-structured continuous evaluation program for addressing insider threats and maintaining robust personnel security. By implementing a continuous user evaluation system, organizations can proactively monitor individuals who have access to sensitive information and systems, ensuring that any potential risks are identified and mitigated in real time. The program's success hinges on the integration of automated monitoring tools, such as SIEM systems, which aggregate data from various sources to provide centralized visibility into potential threats. Additionally, the inclusion of behavioral analytics, anomaly detection, and real-time alert systems can significantly reduce response times to emerging risks. A key component of any successful continuous evaluation program is the clear definition of roles and responsibilities. Senior management, security officers, system administrators, and users must all be aligned in their duties to ensure the program's objectives are met. Moreover, well-defined policies and procedures, based on recognized frameworks like NIST and ISO standards, are crucial for handling potential risks while maintaining compliance with privacy, civil liberties, and equal employment opportunity laws. Furthermore, the review highlights the importance of ongoing training and awareness programs to ensure that all personnel understand their roles and responsibilities within the security framework. A culture of accountability and security awareness is essential for fostering responsible behavior among users. Finally, the need for continuous review and adaptation of the program is emphasized, given the constantly evolving nature of cybersecurity threats. Regular updates to policies, technologies, and compliance measures will ensure that the organization remains resilient against both internal and external risks. Through this multi-layered approach, organizations can strike a balance between safeguarding sensitive information and upholding individual rights.

3 Methods

This literature review was designed to explore the implementation and effectiveness of continuous evaluation programs as a proactive measure for managing and mitigating insider threats within organizations. Insider threats are particularly challenging due to their complex nature and the potential for significant harm to organizational assets, data, and reputation. Continuous evaluation programs address this by providing an ongoing, real-time assessment of user behavior and access patterns, aiming to detect potential risks before they materialize into security incidents.

This comprehensive literature review focuses on examining current literature to identify best practices, tools, and strategies that not only enhance personnel security but also align with broader organizational objectives. Key aspects explored include the technological infrastructure required for effective monitoring, such as SIEM systems and behavioral analytics, as well as the role of policy frameworks and compliance measures in supporting ethical and legally sound monitoring practices. Additionally, this review considers factors such as organizational buy-in, resource allocation, and training initiatives, all of which are essential for the successful deployment and long-term sustainability of continuous evaluation programs. Through this analysis, the literature review aims to provide a comprehensive understanding of how continuous evaluation can be integrated into existing cybersecurity practices. By identifying both successful implementations and common challenges, this review offers organizations practical insights for developing continuous evaluation programs that balance security needs with user privacy and trust, ultimately contributing to a more resilient cybersecurity posture.

The review was conducted using a comprehensive search across various academic and professional databases, including IEEE Xplore, SpringerLink, and Google Scholar. These databases were selected for their extensive collections of peer-reviewed articles and conference papers in the fields of cyber-security, information technology, and organizational security, ensuring access to high-quality, relevant research. To capture a wide range of perspectives on continuous evaluation programs, the search utilized Boolean search terms like ("continuous evaluation" OR "continuous monitoring") and ("insider threats" OR "cybersecurity") ("user behavior monitoring" OR "behavioral analytics") and ("security" OR "cybersecurity") ("SIEM" OR "Security Information and Event Management") and ("cybersecurity" OR "threat detection") ("insider threat management" OR "insider threat mitigation") and ("cybersecurity" OR "security"), refining the search results to focus specifically on articles related to continuous user monitoring and insider threat mitigation. By limiting the publication range from 2015 to 2023, the review prioritizes research that reflects current trends, technologies, and challenges in contemporary cybersecurity practices.

The review applied rigorous inclusion and exclusion criteria to ensure relevance and maintain a high standard of evidence. Studies were included if they addressed continuous evaluation within the context of cybersecurity, particularly focusing on insider threat mitigation, user behavior monitoring, or organizational security policies. Eligible studies provided insights into how continuous evaluation can be implemented and its effectiveness in identifying or mitigating insider threats. Only articles published in peer-reviewed journals or conference proceedings were selected, ensuring that the review is grounded in verified, credible sources.

Exclusion criteria were equally strict to maintain focus. Studies were excluded if they were unrelated to cybersecurity or focused exclusively on external threat mitigation rather than internal (insider) threats. Additionally, articles not published in peer-reviewed journals or credible conference proceedings were omitted to avoid reliance on unverified or non-scholarly sources. This structured approach to inclusion and exclusion ensured a focused, high-quality literature base from which to draw meaningful insights into the implementation and impact of continuous evaluation programs within organizational settings.

A rigorous multi-stage screening process was conducted to ensure that only the most relevant and high-quality studies were included in the review. The initial stage involved a thorough review of titles and abstracts to quickly filter out studies that were not directly relevant to the topic of continuous evaluation programs for insider threat management. This initial screening allowed for a broad yet focused selection, capturing studies that appeared to meet the criteria based on keywords, scope, and preliminary objectives. Following the title and abstract review, articles that passed this first screening were then examined in full text. This deeper review stage involved assessing each article for its specific alignment with the review's objectives, including the study's relevance to insider threat mitigation, continuous monitoring, and organizational security practices. During this stage, each study's methodology, findings, and relevance to cybersecurity best practices were evaluated to determine whether it provided substantial insights into continuous evaluation programs. Articles that did not directly contribute to these areas or lacked methodological rigor were excluded to maintain the integrity and focus of the review. To facilitate the organization and systematic management of the selected articles, Overleaf was used as a collaborative tool, enabling efficient organization, annotation, and tracking of sources throughout the review process. This tool was essential in preventing duplication, ensuring that each source was only considered once, and streamlining the workflow for categorizing articles based on themes, findings, and quality. By implementing this structured approach to screening, the review maintained a high standard of relevancy and consistency across selected studies, ensuring that the final analysis was grounded in the most pertinent and credible sources.

Key information was meticulously extracted from each study to capture essential details and enable a structured comparison across the body of research. For each study, core elements were recorded, including the author(s), publication date, and specific focus of the study, such as the type of continuous evaluation method, insider threat mitigation strategies, and relevant organizational security measures. This information provided foundational context for understanding each study's unique perspective and relevance to the literature review's objectives. In addition to basic bibliographic information, the extraction process involved capturing the key findings of each study, highlighting critical insights into the effectiveness, challenges, and outcomes associated with continuous evaluation programs. These findings included specific metrics or observations about the success of different monitoring tools, risk mitigation techniques, and user behavior analytics, offering a granular view of how various approaches impact organizational security and insider threat management. Limitations identified within each study were also documented to provide a balanced understanding of the research landscape. Recording these limitations allowed for a critical analysis of potential biases, methodological constraints, and areas where further research is needed. Common limitations included sample size restrictions, technological limitations, and challenges in generalizing findings to different organizational contexts. The extracted data was systematically organized into a comprehensive summary table, facilitating an at-a-glance comparison of each study's contributions and allowing for an efficient cross-analysis of approaches and findings. By categorizing studies based on their focus, findings, and limitations, the summary table supported a thematic analysis, helping to identify trends, gaps, and areas of consensus or divergence within the literature. This structured organization provided a foundation for deeper comparative analysis, enabling the review to synthesize complex findings into cohesive themes and actionable insights.

A thematic analysis approach was applied to systematically synthesize findings across the selected studies, allowing for the categorization of insights into key themes relevant to continuous evaluation programs for insider threat mitigation. This analysis aimed to uncover overarching trends and patterns, making it possible to distill complex information into digestible themes that capture the core focus areas of the literature. Themes identified during this process included risk management, insider threat mitigation strategies, automated monitoring tools, and user accountability. Each theme represented a critical component of continuous evaluation programs, and grouping findings into these categories provided a structured way to compare and contrast approaches, tools, and recommendations across studies.

Risk Management: Studies within this theme explored the frameworks and methodologies used to assess and manage risks posed by insider threats. The literature emphasized strategies for identifying high-risk users, assessing behavioral indicators, and implementing mitigation measures to reduce potential threats. Recurring practices in this theme included risk prioritization, where resources are focused on users with elevated access privileges or those exhibiting anomalous behavior, allowing for targeted intervention.

Insider Threat Mitigation Strategies: This theme focused on various strategies and protocols designed to identify, monitor, and respond to insider threats. Studies discussed preventive measures such as behavior analysis, real-time access monitoring, and regular training programs to raise awareness of insider risks. By categorizing findings under this theme, the review highlighted best practices in developing comprehensive insider threat programs that include predictive monitoring and response protocols.

Automated Monitoring Tools: A significant portion of the literature examined the role of technology in continuous evaluation programs, particularly automated tools like SIEM systems and user behavior analytics. Findings within this theme detailed the capabilities of these tools in aggregating data, identifying anomalies, and generating alerts for potential insider threats. Thematic analysis allowed for the comparison of tool effectiveness, cost-efficiency, and technological limitations, providing insights into how different organizations deploy automated solutions to enhance security.

User Accountability: This theme focused on creating a culture of security through user accountability and awareness. Studies in this category emphasized the importance of clear policies, employee training, and transparent communication regarding monitoring practices to foster a proactive security environment.

Recurring recommendations included establishing clear guidelines around acceptable use, implementing accountability measures, and promoting a shared responsibility for cybersecurity. By grouping findings under these themes, the thematic analysis allowed for the identification of recurring practices and recommendations that appear consistently across the literature. This approach provided a comprehensive overview of best practices, highlighting where there is consensus in the field, as well as areas of divergence or limited empirical support. It also facilitated the identification of gaps within each theme, pinpointing where additional research or development of new strategies is needed. Overall, this thematic categorization enabled a more in-depth synthesis, making it possible to draw meaningful conclusions from a diverse range of studies on continuous evaluation and insider threat management.

The quality of the references included was systematically assessed for validity and relevance of research. This approach was chosen to provide a comprehensive evaluation of key aspects of research quality, such as study design, methodological soundness, reliability of findings, and alignment with the research question. By applying this appraisal process, only studies meeting a high academic and methodological standard were included in the review, thus enhancing the reliability and trustworthiness of the synthesized findings. Each study underwent evaluation based on specific quality criteria, which included examining the clarity of research objectives, appropriateness of the study design, sample selection, data collection methods, and robustness of analysis. Studies were carefully reviewed to ensure their methodologies supported valid conclusions, sample sizes were adequate and representative, and data analysis techniques were sufficiently rigorous to minimize bias. Those failing to provide clear methodological descriptions or demonstrating weaknesses in these areas were flagged for further scrutiny. The assessment also verified that each study's findings were well-supported by evidence, clearly presented, and aligned with the stated objectives. Studies with ambiguous conclusions, reliance on anecdotal evidence, or notable methodological flaws were excluded from the synthesis to maintain the integrity of the review. Additionally, relevance to the review's focus on continuous evaluation for insider threat management was critical; studies without direct contributions to this area were omitted to prevent dilution of the review's core themes. Through this rigorous appraisal process, the review maintained high-quality standards, ensuring only credible and reliable studies informed the synthesis and analysis. This systematic evaluation minimized bias, grounding the literature review's findings in robust research. This structured assessment process provided a foundation for an accurate and impactful synthesis, enhancing the reliability and practical value of the insights presented in the review.

This review faced several limitations that may impact the comprehensiveness and generalizability of its findings. One notable limitation is the potential for publication bias, as studies that report positive or significant findings are often more likely to be published than studies with neutral or negative results [29]. This bias could lead to an over-representation of successful continuous evaluation implementations, potentially skewing the findings by underrepresenting studies that may have identified challenges or limitations in using such programs for insider threat mitigation [29]. Consequently, the synthesized recommendations may disproportionately reflect successful case studies, which could present a somewhat idealized view of continuous evaluation programs. Another limitation is the review's focus on English-language studies, which may inadvertently exclude important insights from non-English-speaking regions. Continuous evaluation programs are implemented in organizations worldwide, and regional differences in regulations, organizational culture, and technological practices may influence the design and effectiveness of these programs. By limiting the review to English-language studies, there is a risk of missing valuable perspectives, particularly those that reflect diverse cultural or regulatory approaches to insider threat management. This linguistic focus restricts the scope of the review and may limit the applicability of its findings in a truly global context. Restricted access to proprietary databases further limited the scope of this review. Although several major databases, including IEEE Xplore, SpringerLink, and Google Scholar, were utilized, some studies may have been published in specialized or proprietary databases not accessible during this review process. This restriction could result in a narrower pool of studies, potentially omitting research from niche areas or highly specialized fields that contribute unique insights into continuous evaluation methods. As a result, certain advanced or highly innovative approaches may not be represented in the findings, limiting the review's scope in covering all possible approaches to insider threat management. In sum, these limitations highlight potential areas for future research, particularly studies that incorporate multilingual sources, address publication bias through more inclusive review methods, and expand access to proprietary research to capture a broader range of perspectives. The main limitations of this review are also presented below in Table 2. Addressing these limitations in future research could enhance the generalizability and inclusivity of findings, providing a more comprehensive understanding of continuous evaluation programs across varied organizational and cultural contexts.

Table 2: Main limitation summary

Limitation	Description
1. Publication bias	The review may be biased towards studies with positive or significant findings, which could lead to an over-representation of successful continuous evaluation implementations.
2. Linguistic focus	The review only considered English-language studies, which may limit the applicability of the findings in non-English speaking regions.
3. Restricted access to databases	The review may not have had access to all relevant studies, particularly those published in specialized or proprietary databases.
4. Lack of longitudinal studies	There is a lack of longitudinal studies examining the long-term effects of continuous monitoring on security outcomes and employee morale.
5. Limited understanding of psychological and cultural impacts	There is a need for research into the psychological and cultural impacts of continuous evaluation on employees, including how monitoring affects morale, job satisfaction, and perceived fairness.
6. Regional differences	The review primarily focused on studies from North American and European contexts, which may not be representative of other regions or cultural contexts.
7. Limited consideration of technological limitations	The review may not have fully considered the technological limitations and challenges associated with implementing continuous evaluation programs, particularly in organizations with legacy systems.

4 Results

This literature review included studies published from 2015 to 2023, focusing on the effectiveness, implementation strategies, and challenges of continuous evaluation programs within cybersecurity contexts, especially regarding insider threat mitigation. The studies predominantly involved case studies and empirical research in corporate and government settings, with a focus on North America and Europe.

4.1 Thematic Organization of Findings

Effectiveness of Continuous Evaluation Programs Studies consistently indicated that continuous evaluation programs can significantly reduce insider threats by enabling real-time monitoring and early threat detection. The integration of automated monitoring tools, such as SIEM systems, was frequently cited as enhancing program effectiveness through centralized data aggregation and rapid response to anomalies [5,6]. However, several studies noted that program success depends on the balance between robust monitoring and privacy preservation, emphasizing that overly invasive measures can undermine employee trust [2]. Striking this balance is essential to foster a security-conscious culture without compromising individual privacy rights. The literature highlighted various implementation strategies, including:

- Automated Monitoring and Behavioral Analytics: Many studies emphasized the role of automated tools like SIEM systems and behavioral analytics in providing real-time insights into user activity [5]. This will enable organizations to detect and respond to potential insider threats more swiftly and accurately.
- Integration with Cyber Threat Intelligence (CTI): Some studies recommend combining continuous evaluation with CTI to enhance threat prediction and proactive defense against emerging threats [8]. This integration broadens the scope of threat awareness and allows organizations to adapt more dynamically to evolving attack vectors, thereby strengthening overall security posture.
- Role Definition and Access Management: Clearly defined roles and access levels were identified as critical for reducing internal vulnerabilities, with studies suggesting that organizations implement role-based access control and multi-factor authentication as part of the evaluation program to enhance security [13,24]. These measures help ensure that employees access only the information necessary for their roles, reducing the risk of unauthorized access and potential insider threats.

The literature identified several success factors for continuous evaluation programs:

- Organizational Buy-In and Resource Allocation: Studies found that management support and sufficient resources were crucial for program success, highlighting that leadership buy-in helps prioritize security initiatives [11]. Additionally, allocating adequate resources ensures that the program is properly staffed, equipped, and sustained overtime.
- Adherence to regulatory frameworks (e.g., GDPR, HIPAA) was emphasized as necessary for avoiding legal repercussions and ensuring alignment with industry standards [17]. Studies also noted that maintaining compliance helps build employee trust by demonstrating the organization's commitment to protecting personal data and upholding ethical practices.

Barriers included:

- Privacy Concerns: Several studies raised concerns about employee privacy, noting that intrusive monitoring might negatively impact morale and create a culture of distrust [2]. Researchers suggested that organizations implement transparent policies and communicate the purpose of monitoring clearly to mitigate these potential negative effects.
- Comparative Analysis Studies comparing organizations with and without continuous evaluation programs found that organizations with these programs reported lower incident rates of insider threats. Quantitative studies revealed measurable improvements in threat response times and reductions in data breach occurrences. However, organizations with more comprehensive role definitions and tailored training programs demonstrated greater overall program effectiveness compared to those relying solely on automated monitoring [11,27]. These organizations were better able to address specific security needs, empowering employees with the knowledge and skills necessary to recognize and respond to potential threats proactively.

- Technological Limitations: Some organizations faced challenges due to outdated infrastructure or the high cost of implementing advanced monitoring tools, which limited their ability to maintain effective security measures [22]. As a result, many had to prioritize upgrades selectively or seek alternative solutions to balance cost with necessary security enhancements.

4.2 Trends and Patterns

Over time, literature has shifted from focusing solely on the technology of continuous evaluation to emphasizing the integration of human and policy elements. Recent studies highlight the increasing importance of fostering a security-aware culture, where user accountability and organizational transparency play pivotal roles [10,11]. Additionally, studies show a trend toward integrating continuous evaluation with broader cybersecurity frameworks, such as the NIST Cyber-security Framework, to ensure holistic security.

4.3 Gaps in the Literature

This review identified several gaps, including a lack of longitudinal studies that examine the long-term impact of continuous evaluation programs on insider threat rates. Additionally, few studies explored the cultural and psychological impacts of continuous monitoring on employees, indicating a need for research into balancing security with employee wellbeing. Regional differences in program effectiveness were also under explored, as most studies focused on North American and European contexts.

4.4 Summary of Findings

Overall, the literature suggests that continuous evaluation programs are effective in reducing insider threats, particularly when supported by automated tools, clear role definitions, and compliance with privacy standards. Organizational commitment, adequate resources, and a balance between security and privacy emerged as critical factors for program success. However, further research is required to address identified gaps, particularly regarding the long-term and psychological effects of continuous monitoring.

4.5 Interpretation of Findings

The findings from the literature review affirm that continuous evaluation programs are an effective strategy for identifying and mitigating insider threats. By integrating real-time monitoring, behavioral analytics, and automated tools such as SIEM systems, organizations can proactively respond to potential risks [5,16]. This continuous approach contrasts with traditional, periodic evaluation methods, which often allow threats to go unnoticed between assessment intervals [27]. Continuous evaluation, as demonstrated across various studies, enhances security by providing a constant layer of oversight that enables rapid detection and response to anomalies.

However, the literature also highlights challenges associated with implementing these programs. Privacy concerns and the potential for reduced employee morale were recurrent themes, indicating a complex balance between robust security measures and the preservation of user trust [17]. This balance is particularly relevant in regions where data protection laws, such as GDPR and HIPAA, impose strict privacy requirements [18,23]. These legal and ethical considerations underscore the importance of designing programs that are transparent and minimize intrusiveness, fostering an organizational culture of security without compromising employee privacy.

4.6 Implications for Practice

The insights from this review offer valuable guidance for organizations aiming to implement or improve continuous evaluation programs. First, organizational support and resource allocation are essential; studies consistently indicate that adequate funding and management buy-in significantly enhance program efficacy [11,24]. Without sufficient resources, organizations may struggle to maintain the technological infrastructure and skilled personnel required for effective monitoring and analysis.

Additionally, the importance of clearly defined roles and responsibilities within the program cannot be overstated. Organizations that implement role-based access controls, multifactor authentication, and structured access management experience greater success in reducing vulnerabilities [13]. Such controls ensure that access to sensitive information is limited to authorized personnel, reducing the risk of intentional or accidental data breaches.

To address privacy concerns, organizations should consider adopting a layered approach, where user behavior is monitored at varying levels of intensity based on role, risk profile, and access level. This approach, combined with clear communication and training initiatives, can help build a culture of accountability and reduce resistance to monitoring efforts [10]. Moreover, ensuring that continuous evaluation programs comply with relevant legal frameworks not only mitigates legal risks but also builds user trust and enhances organizational reputation.

Organizations operating with legacy systems should expedite modernizing as legacy systems may not be able to sufficiently run modern monitoring tools. Modernizing infrastructure to support the integration of a continuous user evaluation system, begins by adopting a scalable approach to legacy system modernization, emphasizing next-generation data architectures and seamless integration strategies [30]. This involves shifting towards cloud-native and distributed architectures, leveraging microservices, event-driven frameworks, and API-driven ecosystems to enhance modularity and support real-time data processing [30]. A phased transition model, AI-powered automation, and strategic data integration approaches, can reduce risks and minimize errors. Prioritizing security and compliance, implementing robust security measures, and conducting a comprehensive infrastructure assessment are also crucial. Additionally, investing in middleware solutions, API-driven integration, and change management strategies can facilitate a smooth transition, while continuous monitoring and optimization ensure long-term success [30]. By adopting a strategic approach to modernization, organizations can position themselves for sustainable growth and innovation in the digital era.

4.7 Comparative Insights and Emerging Trends

Comparative analysis across organizations with and without continuous evaluation programs highlights the significant benefits of proactive insider threat management. Organizations with continuous monitoring report quicker response times, lower incident rates, and a stronger security posture overall [28]. This trend suggests that as threats evolve, continuous evaluation may become a standard practice in cybersecurity strategies, particularly in industries handling highly sensitive information.

An emerging trend in the literature is the integration of continuous evaluation with broader cybersecurity frameworks, such as the NIST Cybersecurity Framework. This holistic approach allows organizations to align their insider threat management with overall security objectives, promoting a more cohesive and effective strategy. Additionally, advancements in artificial intelligence and machine learning are being incorporated into monitoring tools, enabling more sophisticated and accurate threat detection by analyzing complex patterns in real time [6]. These technologies allow organizations to proactively identify potential risks and respond faster to emerging threats, enhancing overall security effectiveness.

4.8 Limitations and Future Research Directions

This review identified several limitations in the existing literature that point to important areas for future research. First, there is a lack of longitudinal studies examining the long-term effects of continuous monitoring on both security outcomes and employee morale. Such studies would provide valuable insights into the sustainability and effectiveness of these programs over time, allowing organizations to make more informed decisions.

Another gap lies in understanding the psychological and cultural impacts of continuous evaluation on employees. Studies addressing how monitoring affects morale, job satisfaction, and perceived fairness could help organizations refine their approaches to balance security with employee well-being. Additionally, there is a need for region-specific research, particularly in non-Western contexts, to assess how cultural and regulatory differences impact program effectiveness and user perceptions.

4.9 Recommendations

In conclusion, this literature review demonstrates that continuous evaluation programs are an effective, albeit complex, solution for managing insider threats. Organizations implementing these programs should prioritize a multi-faceted approach, incorporating automated monitoring, role-based access, and strong legal compliance. Building a culture of accountability and transparency is essential to addressing privacy concerns and ensuring program success. For organizations considering continuous evaluation, it is recommended to secure adequate resources and management support, define roles and access levels to minimize unnecessary exposure to sensitive information, communicate transparently with employees about monitoring practices to maintain trust, and regularly review and update programs to incorporate new technologies and respond to evolving threats. Further research addressing the limitations identified in this review would provide a more comprehensive understanding of continuous evaluation programs, enhancing their development and application across diverse organizational and regulatory contexts.

5 Conclusions

This report highlights the growing importance of continuous user evaluation programs as a proactive measure for managing insider threats in organizational settings. Through real-time monitoring and automated tools, such as SIEM systems and behavioral analytics, continuous evaluation enhances threat detection and provides organizations with the ability to respond swiftly to anomalies. The reviewed studies underscore that when these programs are supported by clear role definitions, role-based access controls, and compliance with legal standards, they are more effective in reducing insider risk without undermining user privacy.

Key success factors identified in this review include strong organizational support, sufficient resource allocation, and a structured approach to user monitoring and access management. Privacy concerns remain a central challenge, indicating a need for transparent communication and policies that strike a balance between security and individual rights. Integrating continuous evaluation with established cybersecurity frameworks, like the NIST Cybersecurity Framework, has emerged as an effective strategy, providing a structured approach to insider threat management within broader organizational security practices. An example checklist consisting of continuous user evaluation system metrics is included in Appendix A.

While continuous evaluation programs show great promise, several gaps remain in the literature. There is a need for longitudinal studies on the long-term effects of monitoring on employee morale and organizational culture, as well as research into region-specific and cultural factors that influence program implementation. Future research addressing these gaps would allow organizations to refine their approach, making continuous evaluation more adaptable and effective across various contexts.

In summary, continuous evaluation programs offer organizations a robust solution to proactively manage insider threats. By investing in technological resources, clear policies, and a balanced approach to privacy, organizations can cultivate security-aware culture that both safeguards sensitive information and respects employee rights.

Acknowledgement: Not applicable.

Funding Statement: The authors received no specific funding for this study.

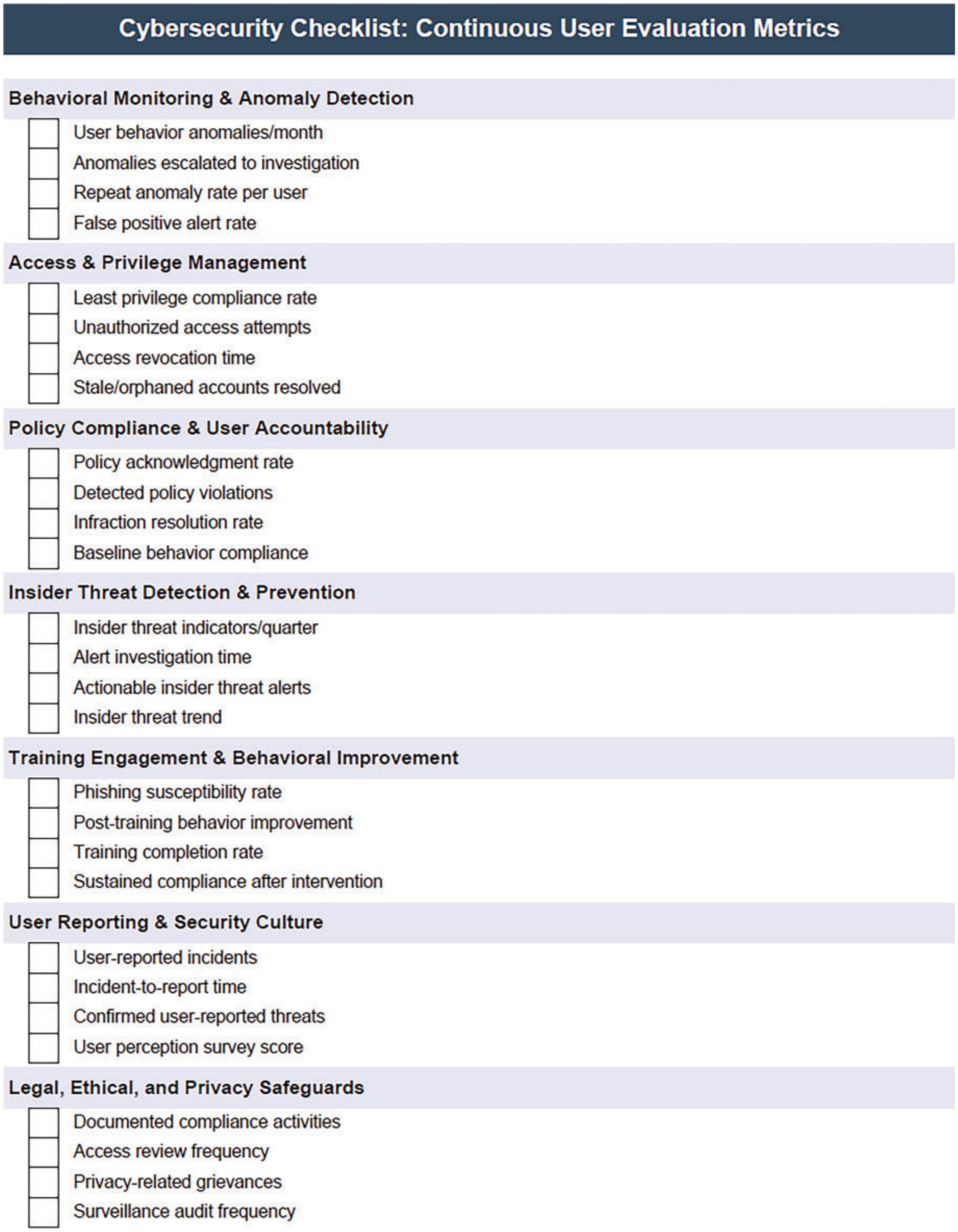
Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Josh McNett; methodology, Josh McNett; writing—original draft preparation, Josh McNett; writing—review and editing, Jackie McNett. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: This article does not involve data availability, and this section is not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

Appendix A



Cybersecurity Checklist: Continuous User Evaluation Metrics

Behavioral Monitoring & Anomaly Detection

□ User behavior anomalies/month
□ Anomalies escalated to investigation
□ Repeat anomaly rate per user
□ False positive alert rate

Access & Privilege Management

□ Least privilege compliance rate
□ Unauthorized access attempts
□ Access revocation time
□ Stale/orphaned accounts resolved

Policy Compliance & User Accountability

□ Policy acknowledgment rate
□ Detected policy violations
□ Infraction resolution rate
□ Baseline behavior compliance

Insider Threat Detection & Prevention

□ Insider threat indicators/quarter
□ Alert investigation time
□ Actionable insider threat alerts
□ Insider threat trend

Training Engagement & Behavioral Improvement

□ Phishing susceptibility rate
□ Post-training behavior improvement
□ Training completion rate
□ Sustained compliance after intervention

User Reporting & Security Culture

□ User-reported incidents
□ Incident-to-report time
□ Confirmed user-reported threats
□ User perception survey score

Legal, Ethical, and Privacy Safeguards

□ Documented compliance activities
□ Access review frequency
□ Privacy-related grievances
□ Surveillance audit frequency

References

1. Rauf U, Mohsen F, Wei Z. Taxonomic classification of insider threats: existing techniques, future directions & recommendations [Internet]. 2023 [cited 2025 Jun 28]. Available from: https://journals.riverpublishers.com/index.php/JCSANDM/article/view/18823.
2. Safitra MF, Lubis M, Fakhrurroja H. Counterattacking cyber threats: a framework for the future of cybersecurity. Sustainability. 2023;15(18):13369. doi:10.3390/su151813369.
3. IAEA. Computer security techniques for nuclear facilities: technical guidance [Internet]. Vienna, Austria: International Atomic Energy Agency; 2021 [cited 2025 Jul 2]. Available from: https://www.iaea.org/publications/14729/computer-security-techniques-for-nuclear-facilities.
4. Nichols L. Cybersecurity architect's handbook: an end-to-end guide to implementing and maintaining ro-bust security architecture [Internet]. Birmingham, UK: Packet Publishing Ltd.; 2021 [cited 2025 Jul 2]. Available from: https://dsu.primo.exlibrisgroup.com/permalink/01SDBOR_DSU/1njvbkr/alma9993943312503642.
5. González-Granadillo G, González-Zarzosa S, Diaz R. Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. Sensors. 2021;21(14):4759. doi:10.3390/s21144759.
6. Salem AH, Azzam SM, Emam OE, Abohany AA. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. J Big Data. 2024;11(1):105. doi:10.1186/s40537-024-00957-y.
7. Ehis AT. Optimization of security information and event management (SIEM) infrastructures, and events correlation/regression analysis for optimal cyber security posture. Arch Adv Eng Sci. 2023:1–10. doi:10.47852/bonviewaaes32021068.
8. Saeed S, Suayyid SA, Al-Ghamdi MS, Al-Muhaisen H, Almuhaideb AM. A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. Sensors. 2023;23(16):2023. doi:10.3390/s23167273.
9. Hakonen P. Detecting insider threats using user and entity behavior analytics [Internet]. 2022 [cited 2025 Jun 16]. Available from: https://www.theseus.fi/handle/10024/786079.
10. Schreider T, SSCP, CISM, C|CISO, ITIL. Building effective cyber-security programs: a security manager's handbook. Brookfield, CT, USA: Rothstein Publishing; 2018.
11. Guttman B, Roback E. NIST SP 800-12: Chapter 3 Roles & Responsibilities [Internet]. csrc.nist.rip. Available from: https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter3.html.
12. Krumay B, Bernroider EWN, Walser R. Evaluation of cybersecurity management controls and metrics of critical infrastructures: a literature review considering the NIST cybersecurity framework. In: Secure IT systems. Cham, Switzerland: Springer International Publishing; 2018. p. 369–84. doi:10.1007/978-3-030-03638-6_23.
13. Cram WA, Proudfoot JG, D'Arcy J. Organizational information security policies: a review and research framework. Eur J Inf Syst. 2017;26(6):605–41. doi:10.1057/s41303-017-0059-9.
14. Edwards DJ. Security policies and procedures. In: Mastering cybersecurity. Berkeley, CA, USA: Apress; 2024. p. 413–34. doi:10.1007/979-8-8688-0297-3_12.
15. Nagata K. Establishing information security policy as an organizational risk management. In: The Future of Risk Management. London, UK: IntechOpen; 2024. doi:10.5772/intechopen.1004563.
16. Moustafa AA, Bello A, Maurushat A. The role of user behaviour in improving cyber security management. Front Psychol. 2021;12:561011. doi:10.3389/fpsyg.2021.561011.
17. Mikolic-Torreira I, Henry R, Snyder D, Beaghley S, Pettyjohn SL, Harting S, et al. A framework for exploring cybersecurity policy options. Santa Monica, CA, USA: Rand Corporation; 2016. doi:10.7249/RR1700.
18. Sharma S. Data privacy and GDPR handbook. Nashville, TN, USA: John Wiley & Sons; 2020. doi:10.1002/9781119594307.
19. Bukaty P. The California consumer privacy act (CCPA). Ely, UK: IT Governance Publishing; 2019. doi:10.2307/j.ctvjghvnn.
20. Glöckler J, Sedlmeir J, Frank M, Fridgen G. A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. Bus Inf Syst Eng. 2024;66(4):421–40. doi:10.1007/s12599-023-00830-x.
21. The Department of Homeland Security. Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) reporting requirements [Internet]; 2024. In: The Federal Register/FIND (Vol. 89, Number 66). Washington, DC,

USA: Federal Information & News Dispatch, LLC, p. 23644. [cited 2025 Jun 16]. Available from: https://dsu.primo.exlibrisgroup.com/permalink/01SDBOR_DSU/k4qanc/cdi_proquest_reports_3032785896.

22. Sulaiman NS, Fauzi MA, Wider W, Rajadurai J, Hussain S, Harun SA. Cyber-information security compliance and violation behaviour in organisations: a systematic review. Soc Sci. 2022;11(9):386. doi:10.3390/socsci11090386.
23. Committee on health research and the privacy of health information: the hipaa privacy rule, Board on Health Sciences Policy, Board on Health Care Services, and Institute of Medicine. Beyond the HIPAA privacy rule [Internet]. Washington, DC, USA: National Academies Press; 2009 [cited 2025 Jun 16]. doi:10.17226/12458.
24. Chew TS. Considerations for developing cybersecurity awareness training. ISACA J. 2023;2(3):2023.
25. Taherdoost H. Towards an innovative model for cybersecurity awareness training. Information. 2024;15(9):512. doi:10.3390/info15090512.
26. Alyami A, Sammon D, Neville K, Mahony C. Critical success factors for security education, training and awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives. Inf Comput Secur. 2024;32(1):53–73. doi:10.1108/ics-08-2022-0133.
27. Hargenrader B. Information security continuous monitoring: the promise and the challenge. ISACA J. 2015;1:1–5.
28. Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, et al. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract. 2022;47(3):698–736. doi:10.1057/s41288-022-00266-6.
29. Dwan K, Gamble C, Williamson PR, Kirkham JJ, the Reporting Bias Group. Systematic review of the empirical evidence of study publication bias and outcome reporting bias—an updated review. PLoS One. 2013;8(7):e66844. doi:10.1371/journal.pone.0066844.
30. Ogunwole O, Onukwulu EC, Joel MO, Adaga EM, Ibeh AI. Modernizing legacy systems: a scalable approach to next-generation data architectures and seamless integration. Int J Multidiscip Res Growth Eval. 2023;4(1):901–9.