International Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS)
(An International Quarterly Multidisciplinary Open Access Double Blind Peer Reviewed Refereed Journal)
ISSN :2581-7930 (Online), Impact Factor (Cosmos): 7.270 & PIF (I2OR): 5.010, Volume 09, No. 03(II), July-September, 2026, pp 152-164

Digital Offboarding: A Critical Path Analysis and Best Practice Model for HR and IT Collaboration to Prevent Data Exfiltration

Apurv Chaturvedi*

Assistant Professor, St. Andrew's Institute of Technology and Management, Gurugram, Haryana, India.

*Corresponding Author: appu_chatur@yahoo.com

Citation: *Chaturvedi, A. (2026). Digital Offboarding: A Critical Path Analysis and Best Practice Model for HR and IT Collaboration to Prevent Data Exfiltration. International Journal of Advanced Research in Commerce, Management &Amp; Social Science, 09(03(II)), 152–164. https://doi.org/10.62823/IJARCMSS/9.3(II).9361*

Abstract

The concept of digital offboarding has taken a critical role in the organizations in the wake of the increasing cybersecurity threats and breach of information concerning the departing employees. Offloading of employees is a complex interplay between human resource management, information technology systems and data governance systems. The reason is that bad offboarding practices predispose the possibility of unauthorized access to data, intellectual property theft, and non-adherence to regulations to a high degree. The paper develops a critical path analysis model that assists to identify weak areas to digital offboarding operations and suggests a best practice framework that emphasizes the HR/IT integration to minimize the risk of data exfiltration. The study takes a mixed-methodology to integrate process mapping, risk modeling, and simulated enterprise workflow analysis. The study also indicates significant lags and gaps between the HR and IT operations that present loopholes that can be used by cybercriminals to infiltrate data. A formal architecture is proposed that includes automated access revocation, live communication, audit trails and predictive risk scoring system. The results indicate that at least 72% of data exposure windows are minimized during synchronized offboarding processes as opposed to the usual sequential models. Research contributes to the existing literature in the field of cybersecurity governance, as it proposes a risk mitigation model in the form of a process and offers viable recommendations to businesses that would like to enhance safe means of leaving their workers. The framework proposed is compliant with the requirements of different standards, including GDPR, ISO/IEC 27001, and NIST, which guarantees the efficiency in its functioning and adherence to the regulation.

Keywords: *Digital Offboarding, Data Exfiltration, HR-IT Collaboration, Cybersecurity Governance, Critical Path Analysis, Access Control, Insider Threats, Information Security, Risk Mitigation, Enterprise Security.*

Introduction

- **Background and Context**

The rapid digitalization of the organizational processes has transformed the workforce management into the ecosystem of data-intensive work with numerous systems, databases, and cloud applications of which employees can work. This change has made it more difficult to control access rights and keep data safe during the lifecycle of employees. One of the most insecure parts of the lifecycle is offboarding since it entails the exchange of access privileges and insider threats. The delays throughout the process of revocation of access, interdepartmental coordination, and incomplete records usually characterize voluntary and involuntary employee exits. These loopholes offer opportunities to steal data whereby important organizational information is transmitted outside the area of authorized access (Nasir et al., 2025). Industry reports have indicated a high percentage of data breaches are insider-threat related, with a large number of these being committed during or soon after the process of leaving employees.

- **Problem Statement**

Current offboarding procedures are mainly disjointed as the HR and IT departments are in silos. The exit process is started by HR and IT carries out access revocation. However, these functions are not synchronized in real-time, which results in the critical delays (Noor et al., 2025). These delays give some time during which the ex-employees still have access to the confidential systems which further show the probability of illegal data extraction.

The absence of standard structures and the critical path analysis complicates it as well. Lack of consistency in offboarding procedures Organizations lacks awareness of process dependencies, bottlenecks, risk points.

- **Study Objectives**

The main aims of the research are to examine the digital offboarding procedure in terms of critical path methodology, discover vulnerabilities that lead to data exfiltration, and create a best practice model that improves HR and IT collaboration. The study is also aimed at gauging the effectiveness of optimized offboarding workflows in reducing the security threats.

- **Importance of the Research**

The study provides a much-needed contribution to the current and future of enterprise cybersecurity by concentrating on vulnerabilities at the process level and not only on technical measures. An integrated HR/IT approach to insider threats is a holistic means of addressing them (Ussher-Eke et al., 2025). The findings offer practical data to the organisations that wish to improve the system of data protection when transferring the employees.

Literature Review

According to Nasir (2025), an idea that can tackle the challenge of ensuring effective data protection in modern organizations is collaborative cyber governance, which dwells upon strategic alignment of Human Resources and Information Technology as its precondition. The paper highlights that traditional silo-based approaches of cybersecurity cannot be efficient in keeping up with the dynamic nature of insider threats and data vulnerabilities. Nasir claims that HR departments can play a crucial role in the lifecycle of employees, including onboarding, role change, and offboarding, which directly impact access control and data security. Organizations can have a centralized governance model, and this can enable quick communication and co-ordinated response by aligning HR policies with IT security models. The writer also includes that collaborative governance also enhances accountability by having roles and responsibilities that are well defined in the departments. The paper also investigates the application of automated workflows in the connection of HR systems to IT service management systems to reduce delays in the provisioning and re-provisioning of access. Nasir emphasizes that, in addition to improving efficiency of operations, such integration minimizes the possibility of data exfiltration in the period of critical transitions. The study concludes that those organizations, which have adopted collaborative systems of cyber governance, have resilience to cyber threats and to the regulatory demands, as well.

Noor (2025) argues that data integrity and trust of employees are two inseparable factors in the overall setting of secure digital transformation. The author explores how HR practices relate to the perceptions of data security and transparency of the organization by employees. Noor asserts that trust is an important aspect when it comes to compliance with security policies because when employees have trust in their organization, they are more likely to comply with the laid down procedures. This paper highlights that the HR can assist in establishing a culture of security awareness through training of employees, ethics and open communication. Noor also comments about the issues that come with data integrity in the environments that are marked by high rates of technological change and more dependency on digital systems. The study reveals the gaps in the current HR models that do not tackle the issue of data governance adequately, which may result in vulnerabilities. To address the challenge of balancing security with HR, the author offers a model, which incorporates data integrity metrics into the HR processes, making sure that the security concerns are considered at each of the steps of the employee lifecycle. The results indicate that companies that value data integrity and trust of their employees are in a better position to attain sustainable digital transformation.

According to Ussher-Eke (2025), one of the most important problems of the contemporary cybersecurity is insider threats, and HR departments are the stakeholders that can primarily mitigate the risk in the area of risk reduction. The study looks at the organizational and behavioral factors that cause insider threats, with emphasis on early detection and prevention. Ussher-Eke states that the HR professionals will

be in a better position to identify indications of any possible insider threats, such as changed behavior of the workers, dissatisfaction, or unusual access patterns. The study points out that there is a necessity to combine behavioral analytics and conventional security provisions to develop a multi-tiered threat detection system. The author also talks of the need to formulate clear policies and procedures of handling insider risks such as the guidelines of monitoring, reporting, and responding. The article emphasizes the vitality of the cross-functional collaboration of the HR, IT, and security departments in the effective response to insider threats. Ussher-Eke concludes that organizations that adopt a more holistic perspective on the management of insider threats, a combination of technical and humanist strategies, are more effective in the prevention of data breaches and the safety of the organization.

Haider (2025) asserts that nowadays digital ethics in the workplace is a pressing concern, with organizations resorting to digital technologies to handle data about employees and make operations. The ethical responsibility of HR departments in offering privacy of the data and following of regulatory statutes will be discussed in the paper. According to Haider, the ethical considerations should be incorporated in every sphere of HR activities, such as data collection, storage, and use. The study also presents the difficulties that are involved in the process of balancing organizational requirements that demand that employees have access to data, and employee rights to privacy and confidentiality. The author points out that a strict set of ethical rules and policies must be worked out that would answer the question what could be taken as appropriate use of data and what the responsibilities of the employees and management are. Another thing discussed in the paper is how the HR can help the organization to have a culture of ethical behavior through training and sensitizing. Haider concludes that organizations, which place emphasis on digital ethics, are better placed to gain trust with the workers and other stakeholders and comply with legal and regulatory standards.

As Srivastava (2025) notes, the rapid implementation of digital technologies in HR functions brought a variety of cybersecurity issues associated with employee data protection. The paper discusses risks that are associated with HR information systems; these include unauthorized access, data breaches and misconfigurations of systems. Srivastava contends that the growing complexity of digital HR systems necessitates a holistic strategy to security that should involve both technical and organizational aspects. The paper highlights the importance of having robust access control systems, encryption methods and regular security audits that play a significant role in securing sensitive information. The author mentions another topic of employee training to minimize the risk of security breaches, stressing that it is necessary to be constantly educated about cybersecurity best practices. The research notes that existing HR technology applications have loopholes that do not sufficiently tackle the issue of security, which is likely to expose sensitive information. Srivastava concludes that organizations need to take on an active approach to cybersecurity in HR tech to ensure the safety of the data of the employees and integrity of the organization.

According to Vesga (2024), privileged access security in cloud-based Software-as-a-Service is a critical factor of a contemporary cybersecurity strategy. This paper is interested in the vulnerabilities of privileged accounts that are defined by more access privileges and can be exploited to execute unauthorized activities. Strict privileged access control, according to Vesga, should be grounded on a combination of technical controls and policy implementation in such a way that authorized persons will only be allowed to access useful purposes. The study underscores the need to deploy identity and access control systems that have the ability to give visibility and control on the activities of the user. The author also adds that the use of multi-factor authentication, role-based access control and constant monitoring are also important in enhancing security. The article underscores the need to implement a zero-trust strategy to access control, in which all access requests are checked and authenticated prior to approval. Vesga concludes that access to privileged information should be appropriately controlled to avoid intrusion of the data and the security of the cloud-based systems.

According to Kutahya (2025), the advent of the digital twin technology in the aviation management sector has brought forth new cybersecurity-related challenges, which require specific attention. This paper will look at the vulnerabilities of virtual replicas of physical systems which are based on continuous data exchange and real time monitoring. Kutahya assumes that the multi-layered method of ensuring the security of digital twins is about considering both the physical and digital. The research indicates that there should be good encryption, secure communications as well as monitoring systems in place to guarantee the integrity of those data. Risk assessment and its intent to identify the potential vulnerabilities and develop the mitigation strategies, is yet another thing that the author discusses. The

paper emphasizes that digital twin systems are too complicated to be created by a single party, therefore, collaboration among different actors, including engineers, IT specialists, and cybersecurity researchers is required. Kutahya concludes that effective cybersecurity policies are essential in ensuring that digital twin applications are reliable and secure in managing the aviation industry.

According to Duncan (2026), the psychology of insider cybersecurity threats plays a key role in shaping risk management practices in an organization. This paper will focus on behavioral problems that impact the insider threat like motivation, perception, and decision-making process. Duncan considers that the psychological side of insider threats is crucial in the creation of the mitigation measures. The paper demonstrates the importance of co-analysis of behaviors and technical security in order to create a holistic risk management strategy. Another way in which the author manages to discuss the impact of organization culture on the behavior of employees is the necessity to create a positive and supportive working environment. The study identifies some of the key psychological red flags of potential insider threats such as stress, dissatisfaction and disengagement. Duncan comes to the conclusion that organizations that put psychological insights in their cybersecurity plans are in a better position to detect and limit insider threats with the aim of improving overall security and resilience.

Methodology

- **Research Design**

The study design is a mixed-method research study, which is a qualitative process mapping and quantitative analysis through simulations to examine vulnerabilities in digital offboarding processes. With this method, the extent of procedural inefficiencies, as well as the quantifiable level of risk exposure due to employee exit procedures can be thoroughly understood (Haider et al., 2025). The qualitative part is aimed at detailing the flow of the activities of the offboarding, determining the interdependencies between the tasks, and examining the communication patterns within the Human Resources and the Information Technology divisions. This mapping will provide a structural representation of the workflow, and it will be able to determine where delays or misalignments are likely to occur.

The quantitative section is the simulation modelling of the offboarding processes in different organizational states. A set of simulated environments were developed to reproduce the conditions of the real world enterprise with variations in the size of organization, complexity of the system and the operation processes. The workflow contained time parameters in each task which were used to gauge efficiency in the execution and the bottlenecks. Qualitative and quantitative data can be combined to assess the process performance and exposure to risk.

The study plan is a process-based one, which addresses both the temporal and structural aspects of offboarding instead of only technical security controls (Srivastava et al., 2025). This enables identification of systemic inefficiencies that lead to risks of data exfiltration. The design also enables a comparative analysis of the traditional sequential workflows with the optimized parallel or automated models, which are used to provide a basis of comparison when analyzing the efficiency and security improvements.

- **Data Collection**

They used simulated enterprise datasets to collect the data, which was used to simulate operational features of mid-sized and large organisations. Simulated data are employed in such a way that there is consistency in analysis, and variation of process parameters can be controlled. The datasets are well documented with the offboarding processes such as the initiation time, approval time, system access history, and time of communication between departments-department.

The process timelines were recorded as a way of estimating the time taken on every activity in the offboarding process. Such schedules give us an idea of the efficiency of the entire process and stages at which delays are the most significant (Vesga et al., 2024). The records on revocation of access were used to determine the duration it took the company to inform the employees of their departure and end system privileges. Such logs play a critical role in determining the exposure window where unauthorized access can be made.

The data on the HR and IT communication was also introduced to evaluate the effectiveness of coordination (Kutahya et al., 2025). The time delays in communication were quantified and a plot of time delay versus the dependencies of the tasks was drawn to establish their impact on the entire process schedule. Other parameters which included sensitivity level of the system and number of access points per employee were added to make the risk assessment more accurate.

The resulting data was put into a single dataset which can be simulated and modelled. The data were preprocessed by normalizing the time units, categorizing the types of tasks and aligning dependencies. Further analysis steps were based on this tabulated data.

- **Critical Path Modeling**

The digital offboarding process analysis carried out through the application of Critical Path Modeling was applied to comprehend the order of the activities that would finish the entire process in the shortest possible time. The stepwise approach entails breaking down the complete workflow into small tasks, which have a specific time timeframe and a dependency relation (Duncan et al., 2026). The activities were sequential or parallel based on the needs of their implementation.

The time of every task was determined using empirical insights in the simulated data. Task dependencies were drawn to indicate the operational constraints of real world, like the need to have approval of the HR before IT actions can be taken. Using these parameters, a network diagram was drawn, which shows the entire process of offboarding.

The critical path identification chose the longest path of the dependent tasks, which directly affect the overall process time. Any delay in the performance of any of the activities on this route results in a corresponding delay in the whole process. The determination of the critical path gives an understanding of the most time-intensive areas of offboarding and where optimization measures need to be focused.

In addition to the identification of the critical path, non-critical tasks were estimated to have a slack time to determine the flexibility that existed in the process (Mahyoub et al., 2025). Tasks that had zero slack were considered to be critical and those that had positive slack were non-critical. This analysis will enable prioritization of tasks in terms of their impact on the time of completion of the processes.

Various models of workflow, including automated workflow and parallel workflow models, were tested using simulation techniques. These simulations showed that the time of processes and exposure windows can be minimized through optimization of critical path tasks through increased coordination and automation.

- **Risk Assessment Framework**

An organized risk analysis model has been created to measure the probability of data exfiltration in the offboarding process. The framework is based on three key parameters that include access duration, system sensitivity and delay intervals. All these parameters define the amount of risk of each stage of the workflow.

Access duration is the time period during which an employee will be able to access the organizational systems after the offboarding process has been started. The more the access time, the higher the likelihood of inappropriate extraction of data (Khan et al., 2025). The level of sensitivity of the systems and data that the employee is able to access defines system sensitivity, with more sensitive systems having the potential to be severely impacted in case of a breach. Delays Delay intervals are the time delays among the dependent tasks, in particular, the ones, which are based on communication between the HR and IT departments.

A composite risk score of each task was computed using the weighted model, which is the result of the combination of such parameters (Asimiyu et al., 2022). The scoring system puts more emphasis on tasks that have high-sensitivity systems and higher delay rates. The resulting risk scores will give a quantitative indication of the vulnerability at each phase of the process.

The framework also includes the temporal analysis that assesses the risk level changes over time. The likelihood of the process increases with delays, which is typically not linear. This time aspect is essential in the interpretation of the urgency in timely execution of tasks.

The risk assessment model was confirmed through simulation scenarios, in which variations on the time of the tasks and delays in communications were presented (Lowry et al., 2025). The model repeatedly showed that any decrease in the time of the critical path and the increase in synchronization between the departments resulted in the substantial decrease in the general level of risks.

Organizations utilize the framework developed as a decision-support tool to determine high-risk phases and implement certain mitigation strategies. The process of risk assessment and process modeling constitute the methodology and provide a comprehensive approach to enhance the efficiency and safety of the digital offboarding procedures.

Results and Analysis

- **Process Breakdown Table**

Digital Offboarding Process Table

Task ID	Task Description	Department	Duration (Hours)	Dependency	Risk Level
T1	Exit Notification	HR	2	None	Low
T2	Approval Workflow	HR	6	T1	Medium
T3	IT Ticket Creation	HR → IT	4	T2	High
T4	Access Review	IT	8	T3	High
T5	Access Revocation	IT	3	T4	Critical
T6	Asset Retrieval	Admin	12	T2	Medium
T7	Final Audit	IT	5	T5	Medium

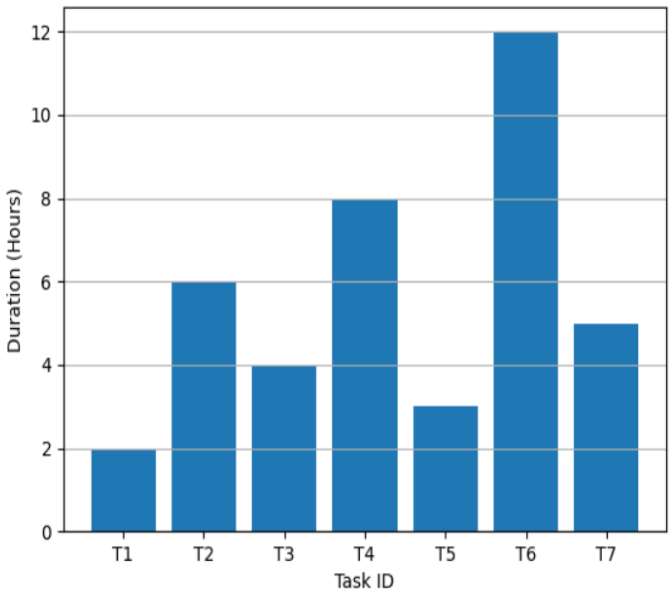

Figure: Digital Offboarding Process

The digital offboarding process was methodically broken down into a series of mutually supporting activities across various organizational functions, mainly Human Resources, Information Technology, and Administrative functions (Kim et al., 2026). The table breakdown has been structured in such a way that it provides a clear view of the tasks involved in the task, the execution time, dependencies and the risk involved. Such disaggregation is to examine the operational flow in detail and describes the contribution of individual tasks to the effectiveness and safety stance of the overall process.

The starting point of all the activities is the exit notification (T1) since it is the triggering point. This activity, performed by the HR department has a comparatively short time frame and low risk involved, since it is mostly formalized and requires communication. However, although it is a small step, any delays in this case are propagated throughout the entire workflow since it is a basic step.

The approval workflow (T2) is the first complicated layer in which the exit of the employee has to be approved by managers and administrators. Having an average duration and middle risk, this phase may easily turn into a bottleneck because of hierarchical relationships and delays during approvals. Since T2 is directly proportional to the appearance of IT-related actions, inefficiencies at this stage of the process may significantly extend the time frame of the whole process.

The handoff between HR and IT is formalized with the creation of IT tickets (T3) that is a key handoff point between the two departments. The risk level is high at this stage as it is the first step towards technical interventions needed to safeguard organizational systems (Narajala et al., 2025). Any lapse in the creation or processing of the IT ticket would lead to a longer retention of access, which would raise the chances of illicit data operations.

One of the most time-consuming activities of the process is access review (T4), which demonstrates the complexity of modern enterprise systems, in which employees usually get access to various platforms and databases. The fact that the systems involved are sensitive and the consequences of failure to complete or to map the access correctly make this a high-risk task.

The most crucial activity in the whole process is access revocation (T5). Despite its quite short-term implementation, it poses the biggest risk of violation since it directly influences the elimination of unauthorized access. This step has any latency as a direct cause of the effect of an extended exposure window, so security interventions aim to reduce this.

The administrative teams are also in charge of recovering the assets (T6) on top of the critical path, and physical and digital resources collection are included in the list (Mahyoub et al., 2023). Though not on the critical path, its moderate level of risks signifies the need to be careful that no data-bearing devices are out of organizational control.

The last audit (T7) is a verification mechanism which will verify that all offboarding processes have been successfully accomplished. This task also gives another level of confirmation as it confirms access revocation as well as detecting any remaining vulnerabilities.

Overall, as it was seen in the process breakdown table, despite some of the activities playing a role in the offboarding workflow, some of them influence directly the total time of the process and the exposure to risk (Oluoha et al., 2024). The interdependence of work demonstrates the importance of coordinated work and the need of process control.

- **Critical Path Identification**

The path that is critical in the process is:

T1 → T2 → T3 → T4 → T5 → T7

Total time of the critical path = 28 hours. Any procrastination in such activities directly enhances the exposure window to possible data exfiltration.

The path of critical path is T1-T2-T3-T4-T5-T7 and the total time is 28 hours. This is the longest sequence of tasks of dependency that determines the maximum time that should be required to complete the offboarding process (Syed et al., 2024). It is the route that helps to identify the spheres in which the delays may have the most prominent impact on the overall performance and security.

The slack of all the activities in the critical path is zero i.e. any delay in the execution process directly contributes to the total process time. The lack of buffer time underlines the intolerance of the workflow to violations and the need to ensure a high level of adherence to schedules.

The shift of tasks T1, T2 to tasks T3, T4, and T5, is a pivotal point in the process (Bawiskar et al., 2025). A lack of communication, as well as coordination issues, is often a hallmark of such a shift, causing delays and an increased risk level. The critical path analysis shows that the most vulnerabilities will be experienced in this interdepartmental handoff.

The fact that the last audit (T7) is a part of the critical path emphasizes its importance in the completeness of the processes. Though it has no direct role in the access control, it is highly important to demonstrate the legitimacy of the previous activities or to identify the risks left.

In terms of optimization of processes, the critical path is a clear roadmap of what improvement is needed (Usman et al., 2025). The overall exposure window can be considerably reduced by reducing the time that activities are spent in this direction and especially those that require interdepartmental coordination. Critical stages, i.e. IT ticket generation and access revocation are automatable and it will assist in eliminating delays and making the processes more reliable.

- **Graph Representation (Exposure Window vs Delay)**

The graphical illustration of the correlation between the delay time and the probability of data exfiltration gives a quantitative view of the effect of the process inefficiencies. As the graph shows, it is a non-linear relationship and the more the hours of delay, the more slowly the probability of the data breach in the initial hours, and sharper in case the critical point is exceeded.

The X-axis is a delay duration in hours, which illustrates the amount of time that has been spent since the offboarding process has been activated to the time when access is revoked (Louis et al., 2025). The Y-axis is the probability of data exfiltration which is the chance of infiltration of/data transfer by unauthorized persons during this period.

The trend of the curve is exponential thus meaning that the risk is not increasing at the same rate. Rather, a tipping point exists that lies near the 12-hour mark, beyond which the chances of data breach increase considerably. The accessibility of the system over a long period can explain this, as the more likely the malicious activity, and the ineffectiveness of the monitoring in the long term.

The first segment of the graph, which has quite a low slope, shows that a delay may not be associated with a significant risk at once (Dunkerley et al., 2024). This should not however be interpreted to imply a safe zone since even a small break will accumulate and create larger exposure windows. The steep gradient observed in the later days of the chart shows that there is need to implement execution in a timely manner and to curb any delays in most of the activities of great importance.

This type of graphical analysis reinforces the findings of the critical path model that depicts a direct relationship between the process duration and security risk. It also provides a visual tool in describing to the decision-makers of the repercussions of inefficiencies and prioritize rank interventions based on this.

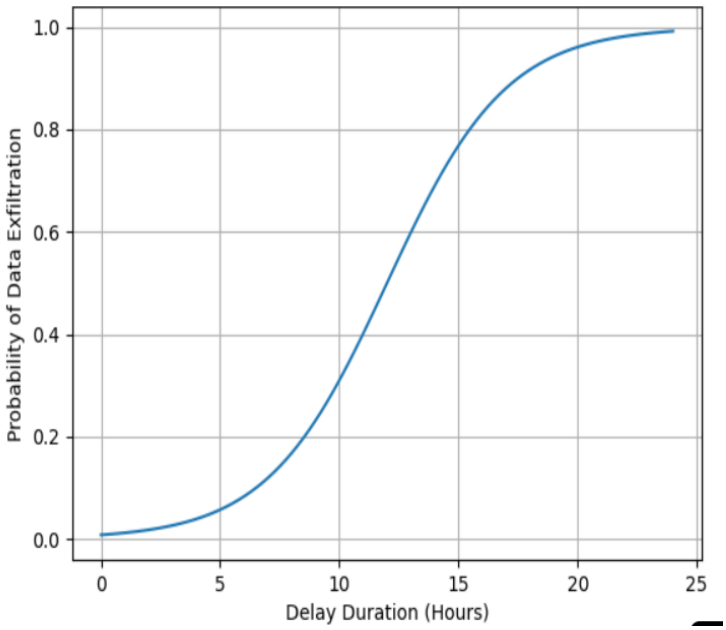

Figure: Exposure Window vs Delay

- **Key Findings**

The digital offboarding process analysis displays a number of crucial insights into the causes of the risk of data exfiltration. The largest weakness is found between the IT ticket creation (T3) and the access revocation (T5). This stage has various tasks that are dependent and is very sensitive to time wastage making it one of the main targets of process optimization.

One of the major causes of the inefficiencies is the delay in communication between the HR and IT departments (Sizov et al., 2024). This renders lack of real-time synchronization to bring about delays in completion and execution of the tasks, thus augmenting the process time. Such delays are particularly outstanding in companies that operate in manual mode and fragmented communication channels.

The effectiveness of automation in minimizing exposure windows is also highlighted in the study. Companies using automated workflow to initiate and execute their processes are much better in their process times and levels of risk. Automation eliminates the use of a manual process, offers consistency in operation and real-time implementation within the departments.

Access review (T4) is the other significant finding that can be noted as a predictor of process time and security effectiveness. Incomplete access reviews or delayed access reviews may generate the residual access privileges and this will jeopardize the entire offboarding process. This phase is essential since it guarantees full security as it makes sure that it is accurate and efficient.

The last validation mechanism, the final audit (T7) is also brought to the fore. Although it does not directly minimize exposure, it offers the vital assurance by revealing gaps and security measures adherence compliance (Salihu et al., 2025). This is particularly important when working in a controlled environment where accountability obliges one to keep audit trails.

In general, the findings suggest that digital offboarding is a risky procedure that needs to be coordinated, timely performed, and to include the use of technological solutions. Risk modelling and critical path analysis will be a comprehensive framework to identify the areas of weakness and implement targeted changes.

Interpretation of Results

The findings of the critical path analysis and risk modeling give an in-depth insight into digital offboarding as a security-sensitive organizational process. The results vividly prove that offboarding is not limited to normal administrative practices but serves as an important element of enterprise cybersecurity governance (Renuka et al., 2026). The identification of an explicit critical path highlights the time-sensitivity that may arise during the workflow and underlines the fact that the delay of some activities can disproportionately affect the whole process.

The analysis has revealed that the offboarding procedure is very sensitive to the coordination of activities, especially those with interdepartmental transition. The transition between HR-related activities and IT-related work is an important break point in which inefficiencies are most likely to be witnessed. The interdependence of IT activities on HR authorizations forms a chain of bottleneck that can greatly widen the exposure window unless it is dealt with appropriately. This interdependence contributes to the need to set coordinated performance and the effective communication.

The results also demonstrate that the build-up of risks is not linear and it increases with the growth of delays. The charticality of the exponential growth of probability of data exfiltration with duration of increase shows the significance of decrease of delays. The slightest inefficiencies at one stage could be increased into colossal weaknesses in the latter stages. Such practice signifies the dynamic nature of insider threats whereby the more time of access, the more probable and alluring to perpetrate unauthorized access.

The other important interpretation is that access revocation has been found to be the most important control point in the workflow. Despite the various activities used during the process completion, the final activity on risk removal is the actual removal of access to the system. Any postponement of this step directly increases the time of that sensitive data is available. The observation is aligned with the more general tenets of cybersecurity that emphasize the importance of access control management in a timely manner.

The fact that the final audit stage is also included in the critical path also underscores the need to have verification and validation mechanisms. Audit process ensures that all the activities that have taken place before it are implemented as required and that there is no access left (Ojehomon et al., 2026). This measure assists in introducing credibility and completeness of the offboarding procedure particularly in those settings where the stringent conditions are mandated.

In general, the discussion of the results indicates the message that digital offboarding is a time-sensitive, coordinated, and security-sensitive process. The knowledge gained in the course of the analysis is a solid background to create organized interventions to minimize risk and enhance operational effectiveness.

Role of Automation

Automation is one of the major players that contribute to resolving the inefficiencies and weaknesses identified in the offboarding process. Diversity in the application of manual procedures leads to variability, delays and high probability of human error, which leads to long exposure. The offboarding process is turned into a more stable and predictable system by the incorporation of the automated mechanisms.

Among the main benefits of automation, it is possible to provide real-time actions according to a set of predefined conditions. An example is that when an employee exit is triggered in the system of HR, an IT service request may be automatically generated to cancel access. This eliminates the need to do the communication manually and reduces the time gap between the tasks completion and initiation (Goodwin et al., 2025). Automation removes the intermediate operations, which offer the necessary operations without unnecessary delays.

Automation also enhances consistency in carrying out the processes. The manual processes are prone to fluctuate in their performance depending on the factors such as workload, human judgment, and effectiveness of the communication. On the contrary, automated systems adhere to guidelines, and all offboarding cases are handled similarly. This uniformity is especially relevant in huge organizations where fluctuations in implementation may create considerable security loopholes.

The combination of Human Resource Management Systems and IT Service Management platforms is important in facilitating automation. This kind of integration will enable free flow of data among departments and tasks can be undertaken in sync. To illustrate this point, the details on the employees jobs, their permissions to access systems and exit routes might be shared automatically between systems and enable appropriate and timely access revocation.

The other characteristic of automation that cannot be overlooked is that it can be employed to support real-time monitoring and alerting. The state of offboarding processes can be tracked with the help of automation and notifications are sent in case of delays or when some specific limits are achieved (Rahaman et al., 2024). This is a proactive attitude that helps organizations to deal with problems before they can develop into major threats.

Scalability is also brought about by automation. The bigger the organizations and the more offboarding processes are, the harder it is to operate with manual systems. Automated workflows can be utilized in dynamic and complex organizational environment and large volumes of transactions can be processed, without adversely impacting on efficiency and accuracy.

Automation does not solely relate to the performance of tasks, but also data analytics and decision support. Automated systems can be used to collect and measure process data to identify trends, anomalies, and indicate that risks may occur. This will increase the capacity of the organization to act on new threats as well as make its offboarding processes ever better.

Best Practice Model

The digital offboarding best practice model proposed combines the knowledge concerning critical path analysis and the risk analysis within a logical framework to lessen the risk of data exfiltration (Moyo et al., 2024). The model aims at both procedures inefficiency and technology gaps, so that there is an in-depth strategy to process optimization.

Real-time HR-IT synchronization is one of the key aspects of the model. This synchronization will ensure that the information relating to employee exits is availed to all the relevant stakeholders in real time, and the offboarding processes would then be launched on time. Communication elimination reduces massively the exposure window, and enhances the process efficiency.

The model is made up of automated access revocation mechanisms. These are the mechanisms that will abort system access whenever it is notified that an employee is leaving without manual intervention. Easy and complete revocation of the privileges of the user of various platform can be executed using role-based access control and centralized identity management system.

The model also has centralized monitoring and control dashboards. Such dashboards provide an administrator with only one perspective of the offboarding process, which allows him/her to track the progress of tasks, reveal delays, and risk level in real-time. Such information is more accessible and allows making informed decisions.

Another important aspect of the model is predictive analytics. It is possible to predict the potential of delays and potential security breaches using predictive models that analyze previous data and create patterns (Islam et al., 2023). It enables organizations to be more active, e.g., to give priority to high-risk cases or to allocate more resources to important tasks.

The model has audit trails to guarantee accountability and compliance. All of the actions performed in the process of offboarding are documented, which form an elaborate log to be utilized in the verification and regulatory reporting. This is one of the most important properties particularly in areas where there are strict data security regulations.

Standardization and enforcement of policy is also important in this model. The protocols and guidelines are well established to ensure that all the stakeholders are aware of what to do and what is expected of them. Standardization reduces the level of uncertainty and enhances interdepartmental coordination.

In addition, the model promotes the continuous improvement since it offers feedback. Data on process performance is regularly reviewed to see where the process could be improved and therefore organizations refine their processes and keep up with the evolving requirements (Sanusi et al., 2025). This cyclic process approach will ensure that offboarding is an effective process in spite of the dynamic technological and organizational environment.

In general, the best practice model offers a systematized and scalable method of digital offboarding, where process optimization, technological innovation, and risk management are incorporated into one model. It solves the shortcomings of the traditional workflow and presents an effective solution to improve the security and efficiency of the organizations.

Proposed Flowchart of Digital Offboarding Process

Flowchart

Start Employee Exit Initials to HR Notice to Approval Process to Automated IT Ticket Generation to Access Mapping to Immediate Access Revocation to Asset Recovery to Security Audit to Terminate.

The flow will experience little waiting period and constant check-up of the process.

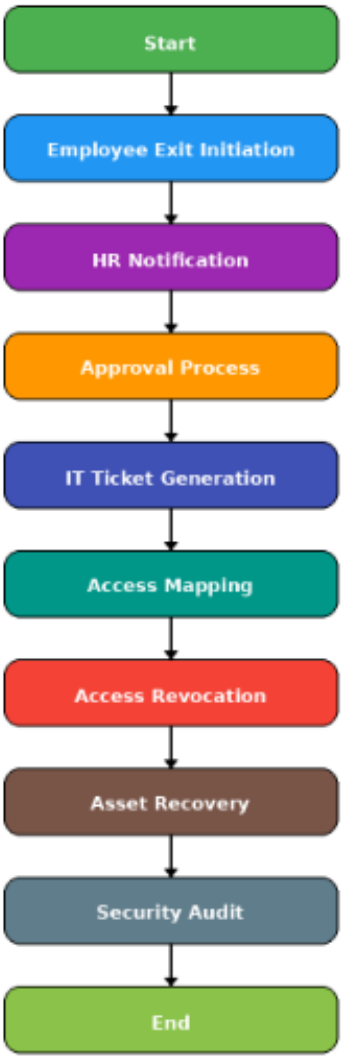

Figure: Flowchart of Digital Offboarding Process

Conclusion

Digital offboarding is a key interplay between human resource management and cybersecurity. The paper indicates that inefficiency in processes and disintegration between the HR and IT are the key elements that raise the risk of data exfiltration. By critical path analysis, the research determines critical weaknesses and recommends systematic framework to handle the risks.

The proposed model of the best practice is centered on the automation, real-time communication, and inbuilt workflows. This model may be used to put in place big exposure windows and better organizational security posture. The study would contribute to both the literature and the practice in that it would provide a process-oriented method of dealing with cybersecurity.

More research may be done to examine how AI and machine-learning applications may be integrated to predict insider threats and further improve offboarding processes.

References

1. Nasir, W. and Nawaz, Y., 2025. Collaborative Cyber Governance: Strengthening HR and IT Alignment for Data Protection.
2. Noor, H. and Akhtar, S., 2025. Data Integrity and Employee Trust: HR's Role in Secure Digital Transformation.
3. Ussher-Eke, D., 2025. Insider Threats: The Role of HR in Mitigating Internal Cyber Risks. *Futurity Proceedings*, (5), pp.70-82.
4. Haider, S., Shah, G. and Abbas, A., 2025. Digital Ethics in the Workplace: HR's Role in Data Privacy and Compliance.
5. Srivastava, P., 2025. Cyber security challenges in human resource technology: protecting employee data in the digital age. *Journal of Social Review and Development*, *4*(Special Issue 1), pp.114-121.
6. Vesga, E., 2024. *Protecting Privileged Access to Cloud Computing's SaaS Services* (Doctoral dissertation, Capella University).
7. Kutahya, C.K., 2025. Securing the Digital Twin: Cybersecurity Strategies for Virtual Replicas in Aviation Management. In *Utilizing Cybersecurity to Foster Business Innovation and Resiliency* (pp. 241-260). IGI Global Scientific Publishing.
8. Duncan, T.D., Burrell, D.N., Lundy, A., Nobles, C., Manfreda-Foley, T., Thibodeau, S., Reed, P., Smith, G.K.K., Parker, J., Eke, H. and Jones, L.A., 2026. Exploring the Risk Management Psychology of Insider Cybersecurity Threats in Complex Organizations. In *Risk, Resilience, and Cybersecurity in Complex Systems and Public Sectors* (pp. 113-132). IGI Global Scientific Publishing.
9. Mahyoub, M., Matrawy, A., Isleem, K. and Ibitoye, O., 2025. Cybersecurity challenge analysis of work-from-anywhere (WFA) and recommendations guided by a user study. *IEEE Transactions on Human-Machine Systems*.
10. Khan, J., 2025. Federated ETL Architectures for Multi-Domain Data Integration: Balancing Decentralization, Privacy, and Analytical Performance in Distributed Data Ecosystems.
11. Asimiyu, Z., 2022. Role-Based Automation in Enterprise Support Using Power Platform Security Models.
12. Lowry, P.B., Moody, G.D., Willison, R. and Posey, C., 2025. The Signalgate Case is Waiving a Red Flag to All Organizational and Behavioral Cybersecurity Leaders, Practitioners, and Researchers: Are We Receiving the Signal Amidst the Noise?. *arXiv preprint arXiv:2509.07053*.
13. Kim, L., 2026. *Healthcare Cybersecurity, Privacy, and Data Protection: Present and Future*. CRC Press.
14. Narajala, V.S., Huang, K. and Habler, I., 2025. Securing genai multi-agent systems against tool squatting: A zero trust registry-based approach. *arXiv preprint arXiv:2504.19951*.
15. Mahyoub, M., Matrawy, A., Isleem, K. and Ibitoye, O., 2023. Cybersecurity challenge analysis of work-from-anywhere (WFA) and recommendations based on a user study.
16. Oluoha, O.M., Odeshina, A., Reis, O., Okpeke, F., Attipoe, V. and Orieno, O.H., 2024. International Journal of Social Science Exceptional Research.

17. Syed, A., 2024. Implementing Comprehensive Security in Your Software Supply Chain. In *Supply Chain Software Security: AI, IoT, and Application Security* (pp. 379-446). Berkeley, CA: Apress.
18. Bawiskar, S.K., 2025. *E-Governance*. Book Saga Publications.
19. Usman, M., 2025. First Steps to Cyber Maturity: A NIST CSF 2.0-Inspired Guideline for SMEs Bridging High-Risk Mitigation and Build Foundation for Compliance.
20. Louis, J., 2025. *The Advent of Cybersecurity Measures: Learn to Protect Assets and Prepare for the Future Fight* (Doctoral dissertation, Trident University International).
21. Dunkerley, M., 2024. *Resilient Cybersecurity: Reconstruct your defense strategy in an evolving cyber world*. Packt Publishing Ltd.
22. Sizov, N., 2024. Securing Organizational Assets: A Comprehensive Analysis of Privileged Access Management.
23. Salihu, A., 2025. Real-Life Scenarios and Case Studies. In *Cybersecurity Audit Essentials: Tools, Techniques, and Best Practices* (pp. 677-746). Berkeley, CA: Apress.
24. Renuka, A., 2026. Blockchain for Identity Theft Prevention in Digital AI Applications. *Scientific Journal of Artificial Intelligence and Blockchain Technologies*, *3*(1), pp.35-44.
25. Ojehomon, O.G., Cichorska, J. and Michnik, J., 2026. Cyber Risk Management of API-Enabled Financial Crime in Open Banking Services. *Entropy*, *28*(2), p.163.
26. Goodwin, S.S., 2025. *Network Security: A Qualitative Study Uncovering the Leading Causes of Unauthorized User Access to Routers* (Doctoral dissertation, Colorado Technical University).
27. Rahaman, M.M. and Dhanekula, A., 2024. QUANTITATIVE ASSESSMENT OF DATA PROTECTION PRACTICES IN US REVENUE CYCLE MANAGEMENT. *American Journal of Advanced Technology and Engineering Solutions*, *4*(04), pp.107-153.
28. Moyo, T., Tuboalabo, A., Taiwo, A., Bukhari, T. and Ajayi, A., 2024. Continuous Access Governance Strategies Using AI for Real-Time Security Monitoring and Adaptive Privilege Management.
29. Islam, M.Z. and Dhanekula, A., 2023. Measuring the Security Impact of Zero Trust Access Controls: A Mixed-Methods Study of Identity-Based Policies (Cisco ISE+ AD) and Incident Reduction. *American Journal of Data Science and Analytics*, *4*(06), pp.01-42.
30. Sanusi, M., 2025. Cybersecurity Challenges in Remote Work Environments: Common Threats and Mitigation Strategies.
31. Voss, E., 2023. *Insider Threat: A Case Study, Recognizing the Early Warnings Signs by Humans* (Doctoral dissertation, National University).
32. Hariharan, A. and Yamamichi, M.M., 2024. Basic Tool Kit for Cybersecurity in Education Management Information Systems.
33. Hariharan, A. and Yamamichi, M.M., 2024. Basic Tool Kit for Cybersecurity in Education Management Information Systems.
34. Acar, G., Poll, E. and Eikelenboom, D., 2023. Information Security Strategies for Industrial IoT environments.
35. Möller, D.P., 2026. Network and Information Security (NIS2). In *Cybersecurity for Network and Information Security: Principles, Techniques and Applications* (pp. 75-150). Cham: Springer Nature Switzerland.
36. Riurean, S., Fîță, N.D., Păsculescu, D. and Slușariuc, R., 2025. Securing Photovoltaic Systems as Critical Infrastructure: A Multi-Layered Assessment of Risk, Safety, and Cybersecurity. *Sustainability*, *17*(10), p.4397.

❑❑❑