STRIDE & DFD

Owner: group 12
Reviewer: Dr: Shaimaa Bajoudah
Contributors: Asayel Alghamdi, Tala Alnabati, Shatha Alamri, Haya Alibrahim
Date Generated: Sun Dec 14 2025

Executive Summary

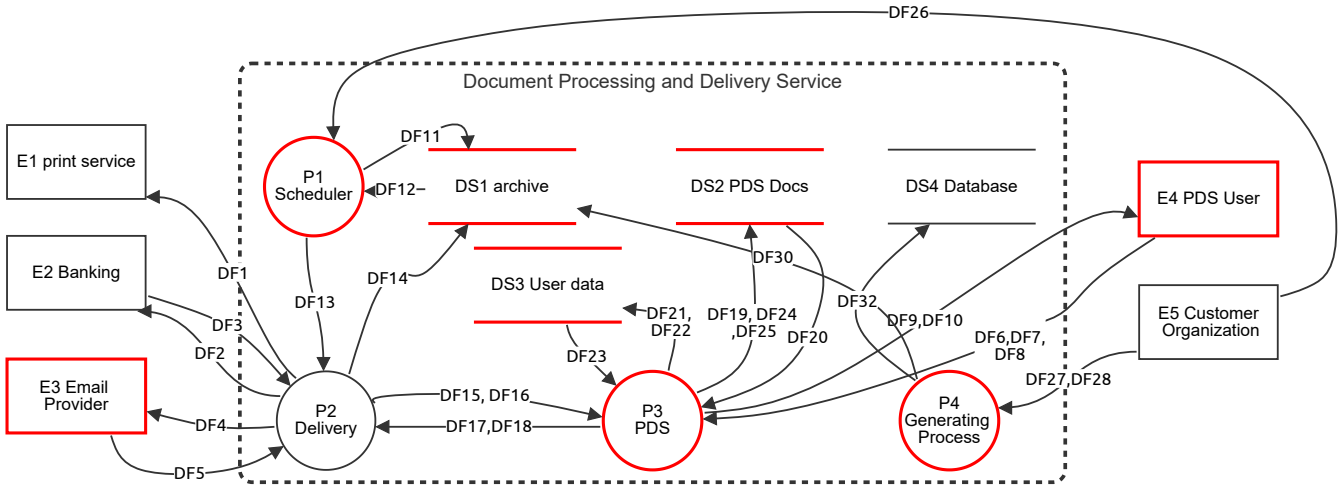
High level system description

The system is designed to generate, deliver, and manage documents through multiple channels such as printing, email, and banking services. It coordinates scheduling, document generation, delivery execution, and user access while storing documents and metadata in dedicated data stores. The system interacts with external entities, including users and service providers, to ensure secure and organized document processing and delivery.

Summary

Total Threats	12
Total Mitigated	0
Not Mitigated	12
Open / High Priority	5
Open / Medium Priority	6
Open / Low Priority	1
Open / Unknown Priority	0

New STRIDE diagram



New STRIDE diagram

P1
Scheduler (Process)

Coordinates delivery operations by retrieving metadata from the Archive (DF12) and scheduling instructions from the Customer Organization (DF26). It sends delivery tasks and triggers to the Delivery process through DF13 process.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
14	Flooding the Scheduler with Excessive Requests	Denial of service	Medium	Open	6	An attacker may overwhelm the Scheduler by repeatedly sending request triggers, causing slowdowns or complete stalls in document handling. This is common when there is no rate-limiting or queue protection.	Add rate limiting, prioritize legitimate tasks, and monitor for abnormal request volumes.
25	No Traceability for Scheduler Actions	Repudiation	Low	Open	4	If the Scheduler executes tasks without associating them with the user who triggered them, no one can be reliably held responsible. This makes it easy for someone to deny that they initiated a process that caused an error or system disruption.	Record all Scheduler actions with user IDs, timestamps, and device identifiers.

P2
Delivery (Process)

Executes document delivery across all channels. It receives scheduling commands, channel-specific responses, and PDS-related data, then dispatches documents to external services (print, email, banking), updates the Archive, and forwards status and data to the PDS.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

P3
PDS (Process)

Handles user document access and interaction. It processes delivery updates, document information, and user-provided requests, then returns documents to the PDS User and updates both PDS Docs and User Data stores accordingly.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
16	Privilege Escalation in PDS Process	Elevation of privilege	High	Open	8	An attacker may exploit a vulnerability in the PDS (P3) process to gain higher privileges than intended. By abusing weak access controls or software flaws, the attacker could access restricted document data, perform unauthorized actions, or manipulate delivery and user data beyond their assigned role.	•Enforce Role-Based Access Control (RBAC) • Apply the principle of least privilege • Isolate and sandbox the PDS process • Validate and sanitize all user inputs • Apply regular security patching and vulnerability updates
17	PDS User Denying Submitted Requests	Repudiation	Medium	Open	5	A PDS user may deny having submitted a specific request if the system does not maintain verifiable and tamper-resistant records. In the absence of reliable evidence, the user can claim they never initiated the request that triggered document generation, delivery, or other system actions.	• Maintain tamper-proof audit logs • Record trusted timestamps for all requests • Apply digital signatures tied to user accounts •Ensure that logs generated by the PDS process cannot be modified or accessed by unauthorized users

Number	Title	Type	Priority	Status	Score	Description	Mitigations
26	PDS Process Overload Attack	Denial of service	Medium	Open	7	An attacker may overwhelm the PDS (P3) process by sending a large number of document generation or delivery requests in a short period. This excessive load can cause the PDS process to become unresponsive, This prevents real users from completing normal operations.	• Apply request throttling and rate limiting • Deploy Web Application Firewall (WAF) rules • Detect and block repeated automated submissions • Monitor system load and trigger alerts

E1 print service (Actor)

Handles print-ready documents received from the Delivery process (DF1). Its role is limited to producing physical outputs without sending additional data back into the system.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

E2 Banking (Actor)

Receives financial or payment-related documents through DF2 and returns processing status or results to the Delivery process via DF3.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

E3 Email Provider (Actor)

Accepts email-bound documents from the Delivery process through DF4 and returns delivery confirmations or status updates via DF5.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Impersonating the Email Provider	Spoofing	Medium	Open	6	An attacker could send forged emails that look like they originated from the official email provider, especially if the domain lacks proper email authentication mechanisms. This can trick the system or staff into sending sensitive documents to the attacker.	Enable SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance), and use signed communication channels.

DS1 archive (Store)

Stores archived documents received from the Scheduler (DF11), Delivery (DF14), and Generating Process (DF30). Provides archived data back to the Scheduler through DF12.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
24	Unauthorized Modification of Archived Files	Information disclosure	High	Open	9	The Archive stores final document files. If access is not properly controlled, unauthorized users may view confidential documents or modify archived files, which can compromise data integrity and confidentiality.	1- Apply strict access control to limit who can read or modify archived documents. 2- Encrypt archived files to protect sensitive information.

DS2 PDS Docs (Store)

Maintains user-specific documents delivered through the PDS. It receives updates from the PDS (DF19, DF24, DF25) and returns stored documents to the PDS when requested (DF20).

Number	Title	Type	Priority	Status	Score	Description	Mitigations
13	Editing PDS Documents Stored in the System	Tampering	Medium	Open	7	PDS Docs stores user-specific documents. An attacker may modify, delete, or replace documents, which can result in incorrect or misleading information being presented to users.	1- Implement role-based access control to restrict document modification. 2- Use integrity checks (e.g., hashing) to detect unauthorized changes.

DS3 User data (Store)

Holds user preferences and PDS-related metadata. It receives updates from the PDS (DF21, DF22) and provides required user data back to the PDS via DF23.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	Exposure of User Personal Data	Information disclosure	High	Open	9	User Data contains sensitive user information and preferences. Unauthorized access may lead to data leakage, privacy violations, or misuse of personal data.	1- Encrypt sensitive user data at rest. 2-Enforce strong authentication and authorization mechanisms.

E4 PDS User (Actor)

Interacts with the PDS by submitting authentication and access requests (DF6, DF7, DF8) and receiving requested documents or responses from the PDS (DF9, DF10).

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	Spoofing the PDS User Identity	Spoofing	High	Open	8	The PDS user interacts directly with the system to request documents and services. An attacker may impersonate a legitimate user by using stolen or weak credentials. If successful, the attacker gains unauthorized access to system functions and sensitive data while being treated as a trusted user.	Using multi-factor authentication reduces the risk of impersonation even if credentials are compromised. Strong password policies and monitoring login behavior further help detect and prevent unauthorized access

E5 Customer Organization (Actor)

Provides templates, structured input data, and scheduling directives that drive both the Generating Process and the Scheduler.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF4 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF1 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF5 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF13 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF2 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF3 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF14 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF17,DF18 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF15, DF16 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF23 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF19, DF24 ,DF25 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF21, DF22 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF20 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF9,DF10 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF12 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF11 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF27,DF28 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF30 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF6,DF7,
DF8 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF32 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF26 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

P4
Generating
Process (Process)

Generates final documents using templates and structured data provided by the Customer Organization (DF27, DF28). It stores completed documents in the Archive (DF30) and writes metadata to the Database (DF32).

Number	Title	Type	Priority	Status	Score	Description	Mitigations
21	Data Leakage Through the Generating Process	Information disclosure	Medium	Open	7	The generating process handles sensitive data while creating documents. During this process, data may be temporarily stored in memory or in temporary files. If these are not properly protected, unauthorized access may occur, leading to data leakage.	Running the process in an isolated environment and securing temporary files limits unauthorized access. Encrypting sensitive data during processing further reduces exposure risk.
28	Privilege Escalation Inside the Generating Process	Elevation of privilege	High	Open	8	The generating process relies on templates and inputs to produce documents. If these inputs are not strictly validated, an attacker may exploit them to execute actions with higher privileges than intended, potentially affecting system integrity.	Applying the principle of least privilege ensures the process operates with minimal permissions. Sandboxing and strict input validation prevent misuse of templates and unauthorized execution.

DS4 Database (Store)

Stores generated document metadata and related information provided by the Generating Process through DF32, supporting later retrieval and system queries.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

LINDDUN

Owner: Group12
Reviewer: Shaimaa Bajoudah
Contributors: shatha alamri, Tala Alnabati, Asayel Alghamdi, Haya Al Ibrahim
Date Generated: Sun Dec 14 2025

Executive Summary

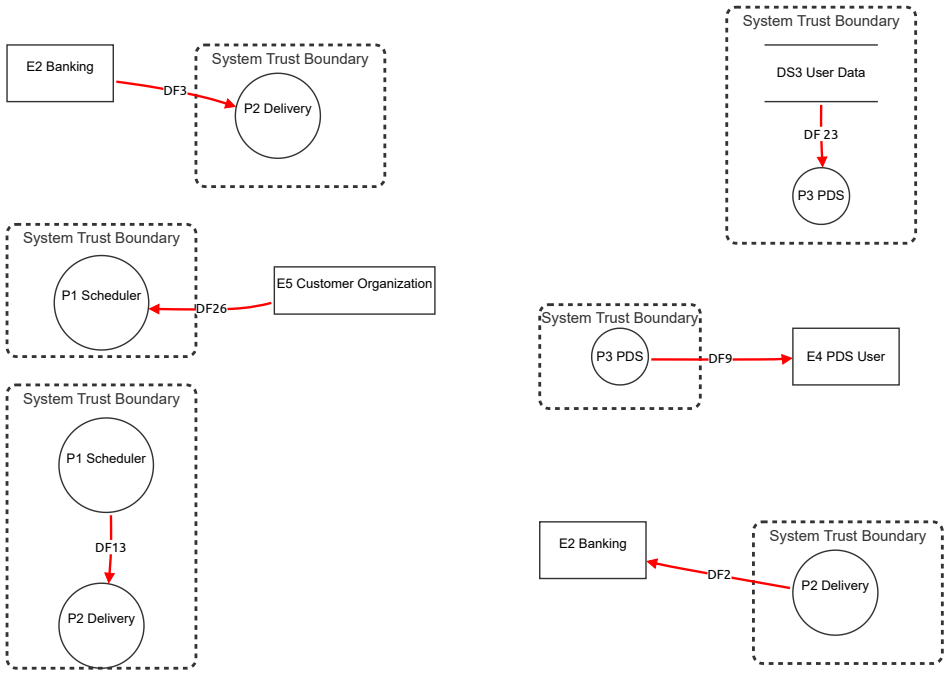
High level system description

This system automatically generates and
delivers documents, allowing organizations to outsource the generation and
delivery of documents such as invoices
and pay slips.

Summary

Total Threats	6
Total Mitigated	0
Not Mitigated	6
Open / High Priority	0
Open / Medium Priority	5
Open / Low Priority	1
Open / Unknown Priority	0

New LINDDUN diagram



New LINDDUN diagram

DF9 (Data Flow)

Delivers the requested document from the PDS to the user.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
13	Detectable document delivery to POS user	Detectability	Medium	Open	4	When a document is delivered from the PDS process to the user, the delivery event may be observable through network traffic, access logs, or monitoring systems. This allows an observer to detect that a specific document delivery or retrieval event has occurred.	Use encrypted communication (HTTPS/TLS). Avoid detailed access logging where not required. Use anonymized or pseudonymous delivery identifiers. Limit visibility of delivery events to authorized components.

DF 23 (Data Flow)

Returns stored user information and preferences needed by the PDS process.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	Linkability of user preferences through repeated access	Linkability	Medium	Open	5	Stored user information and preferences retrieved from the Personal Data Store may be accessed repeatedly by the PDS process. Over time, these accesses can be linked together, allowing an attacker or insider to infer user behavior, habits, or preferences even without directly identifying the user.	Minimize stored user preference data. Aggregate or generalize preference information. Limit access to the Personal Data Store. Apply strict access control and auditing. Avoid long-term retention of detailed preference data.

DF2 (Data Flow)

Transaction parties may deny sending or receiving financial data.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
15	Lack of non-repudiation in delivery–banking transactions	Non-repudiation	Medium	Open	5	Financial or delivery-related transaction data sent from the Delivery process to the Banking service may lack strong non-repudiation guarantees. In the absence of cryptographic proof, either party may later deny having sent, received, or processed a specific transaction. This can lead to privacy risks, disputes, and accountability issues, especially when financial records are involved.	Apply digital signatures to transaction messages. Maintain tamper-evident and secure audit logs. Use trusted timestamps for transaction records. Restrict access to financial transaction logs. Define clear accountability and verification mechanisms

DF3 (Data Flow)

Returns the transaction or processing status from the bank to the Delivery process.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
11	Profiling of customers through payment activity	Linkability	Medium	Open	5	Financial transaction activity from banking can be linked with delivery behavior. An adversary may infer patterns about customers or organizations based on repeated transfers.	Encrypt financial communication (TLS/HTTPS) to protect data in transit. Minimize shared financial metadata (avoid sharing unnecessary details like exact amounts or timestamps). Avoid storing unnecessary logs to reduce the chance of linking transactions to customers.

DF13 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF2 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF23 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF9 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF26 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF3 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

E2 Banking (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

P2 Delivery (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

E5 Customer Organization (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

P1 Scheduler (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF26 (Data Flow)

Provides scheduling instructions that control when document delivery should occur.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	Scheduling patterns may reveal organizational behavior	Linkability	Low	Open	2	Scheduling data from the customer organization may reveal internal patterns such as business volume, frequency, or peak periods.	Aggregate scheduling information to avoid revealing business patterns. Limit logging of exact scheduling times. Separate operational logs from business-sensitive data.

P2 Delivery (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

P1 Scheduler (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF13 (Data Flow)

Sends delivery scheduling commands and execution details to the Delivery process.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
8	Inference from scheduling triggers	Detectability	Medium	Open	4	Triggers sent from the scheduler to the delivery process may be observed, revealing load patterns and timing behaviors.	Encrypt scheduling triggers and metadata. Remove unnecessary timing details from logs. Restrict access to scheduler and delivery process logs.

DS3 User Data (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

P3 PDS (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

P3 PDS (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

E4 PDS User (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

E2 Banking (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

P2 Delivery (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

P1 Scheduler (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

P2 Delivery (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

E5 Customer Organization (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

E2 Banking (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DS3 User Data (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

P3 PDS (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

E4 PDS User (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

LINDDUN Threat Table

S	Fl	R	Location	Characteristics	Description
E2	DF3	P2	DF3	L.2.2.1, L.2.2.2	Bank transaction metadata could reveal user behaviour
E5	DF26	P1	DF26	I.2.1, I.2.2	Scheduling patterns could reveal organisational behaviour
P1	DF13	P2	DF13	D.3	Delivery response exposes activity timing
DS3	DF23	P3	DF23	I.2.1, I.2.2	User data and preferences may be linkable over time
P3	DF9	E4	DF9	D.1,D.2	Document delivery to user is detectable
P2	DF2	E2	DF2	Nr.1.1	Transaction parties may deny sending or receiving financial data.