PROJEKT Justitia 4.0

INTERN

P042-Hi01 - Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept)

Project platform justitia.swiss from Justitia 4.0

Classification	INTERN
Status	Working (in Arbeit)
Projectnumber	-
Projectlead (PL LB)	-
Version	From template V4.4
Date	04. September 2023
Sponsor	CISO/ISBO Justitia 4.0
Author(s)	CISO/ISBO Justitia 4.0, André Mäder

Table of contents

1 Introduction

1.1 Preamble

An initial version of the ISDS concept was developed to support the tender phase (AP) for the development and technical operation of the "Justitia.swiss" platform. This version was approved by the project management.
The ISDS concept for the "Justitia.swiss" platform will be adapted by the security workstream as the project progresses. The following already foreseeable events are expected to lead to a need for adaptation:

- The precise scope for the implementation of the platform MVP is defined
- The listed business cases do not represent technical requirements to be developed, but serve to derive relevant protection measures.
- The Federal Law on the Platform for Electronic Communication in the Judiciary (BEKJ) and its implementation law are available.
- The implementing law for the Information Security Act (ISG) is available.

1.2 Initial Situation

The "Justitia 4.0" project is shaping the digital transformation of the Swiss justice system in criminal, civil and administrative court proceedings. By 2026, all parties involved in judicial proceedings at the cantonal and federal level will be able to exchange data electronically with the approximately 300 courts, public prosecutors' offices and correctional authorities via a secure central platform ("Justitia.Swiss").
The project will procure the central platform, which will support electronic file inspection (eAE) and electronic legal transactions (ERV) in the Swiss justice system in the future, on the market.

1.3 Objectives and General Conditions

The digitalization of the Swiss justice system must meet the highest requirements in terms of information security and data protection (ISDS). This ISDS concept is the constituent document in the area of information security and data protection and is intended to answer the following questions:

- What are the legal requirements regarding information security and data protection to be considered?
- How extensive is the protection requirement for Justitia.swiss?
- What are possible scenarios that cause damage and what would be the scope of these events?
- Which security risks need to be addressed?
- Which security measures (organizational, applicational and technical) have to be taken?
- What residual risks remain after these measures have been implemented?

In particular, the security measures should ensure that the attack surfaces of the technical solution are minimized ("security by design") and that the organizational foundations for a functioning security management are created. In doing so, they must conform to the requirements of the Federal Act on the Platform for Electronic Communication in the Judiciary (BEKJ) and its implementing legislation.

1.4 Scope

The scope of the present ISDS concept comprises of the platform "Justitia.Swiss" with its data, user groups, system components, interfaces and use cases:

- All data processed on the platform or transferred via the platform.
- The operational use cases (e.g. submission), the administrative use cases (e.g. organization and user management), and the system operation.
- The platform "Justitia.swiss" with all components and interfaces to external providers, such as identity providers, signature services, and notification services.

1.5 Delimitation

Not contained in the scope of this ISDS are:

- The IT systems of authorities conducting the proceedings and of organizations involved in the proceedings (including the future judicial file application JAA).
- The end devices of participating organizations and private individuals.

1.6 Governance

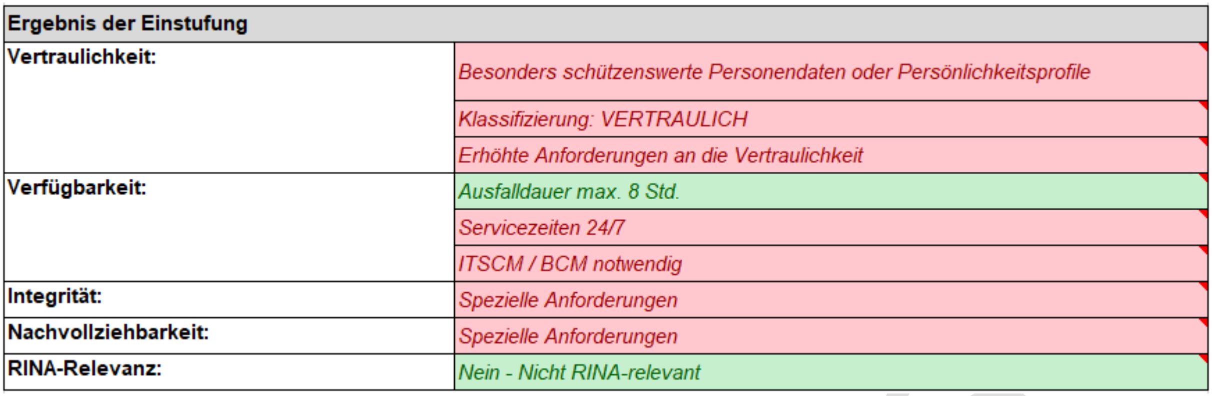
The ISDS concept for the platform "Justitia.swiss" will be maintained and updated by the CISO (person responsible) and its associates of the information security workstream.

1.7 Validity of the document

The validity of the ISDS-concept is maximum 5 years.

2 Classification – Protection needs analysis (Schuban)

The classification was done using the template “P041 – Hi01 : Schutzbedarfsanalyse – Version 4.5”:



Ergebnis der Einstufung	
Vertraulichkeit:	Besonders schützenswerte Personendaten oder Persönlichkeitsprofile
	Klassifizierung: VERTRAULICH
	Erhöhte Anforderungen an die Vertraulichkeit
Verfügbarkeit:	Ausfalldauer max. 8 Std.
	Servicezeiten 24/7
	ITSCM / BCM notwendig
Integrität:	Spezielle Anforderungen
Nachvollziehbarkeit:	Spezielle Anforderungen
RINA-Relevanz:	Nein - Nicht RINA-relevant

Manual translation into EN:

Confidentiality	Personal data requiring special protection or personality profiles
	Classification: Confidential
	Increased requirements for confidentiality
Availability	Max. downtime 8h
	Service 24/7
	ITSCM / BCM required
Integrity	Special requirements
Non-repudiation	Special requirements
RINA-relevance	No – Not RINA-relevant

3 Likelihood and impact matrices

In the following we classify the likelihood and the impact of an incident affecting the information security and data protection of the Justitia.swiss platform.
The initial structure was chosen in accordance to HERMES and adjusted to fit the scope of the Justitia.swiss platform.
Both the likelihood and impact of an occurence are rated using matrices containing six level (ranging from "very unlikely" to "very likely").

3.1 Likelihood of an Incident

The likelihood of an event affecting the information security and data protection is determined by the complexity of the corresponding attack, the size and motivation of potential attackers, etc. In general the likelihood of an event can only be roughly estimated.

Level	Probability	Description
6	very likely	more than twice a year
5	likely	twice a year
4	possible	once a year
3	rare	every 1 to 2 years
2	unlikely	every 2 to 13 years
1	very unlikely	less than every 3 years

3.2 Impact of an Incident

The impact of an event is typically evaluated based on the dimensions
"loss of confidentiality", "loss of integrity", "loss of availability", and "loss of non-repudiation".

The impact is determined by evaluating the type and amount of data that is affected by the event.

Level	Finance [CHF]	Reputation	Business process
6 critical	> 10 Mio.	International multi-year media presence Serious political or economic consequences Sanctions (e.g., blacklists, embargo, ...)	Interference with critical core business processes in several areas for more than 14 days. Proceedings can be deliberately influenced by the manipulation of file documents, so that the integrity of the Swiss judiciary is no longer guaranteed. Blockage of government activity, state crisis. Penalty by the authorities based on data-protection-law.

5 high	1 – 10 Mio.	International and national media presence up to one year Political or economic consequences Options for action of the federal council restricted	Impairment of a critical business process for 7-14 days. Many processes can be observed and, if necessary, influenced by third parties. The information gained can be misused for blackmail or other targeted damage. Many ongoing proceedings are affected. The violation of data protection for numerous parties to the proceedings jeopardises trust in the Swiss judiciary. Judicial proceedings are delayed throughout Switzerland because alternative communication channels (e.g. fax, letter post, secure e-mail) have to be used. Negative impact on other critical processes. Options for action of the federal council restricted. Penalty by the authorities based on data-protection-law.
4 substantial	500k – 1 Mio.	National and in some cases international media presence for up to one year Credibility of the federal council impaired	Impairment of a critical business process for 3-7 days. Individual participants in proceedings or judicial authorities may be damaged in their reputation or disadvantaged in proceedings Important and/or critical ongoing procedures will be impacted because the file items will need to be re-sourced and reviewed.
3 moderate	100k – 500k	National, nationwide media presence for up to one month	Impairment of a non-critical business process for more than 3 days, or of a critical business process for 0.5-3 days Individual parties to proceedings or judicial authorities may be disadvantaged in proceedings.

2 low	10k – 100k	Regional media presence for up to one week	Interference with a non-critical business process for 1-3 days, or with a critical business process for up to 0.5 day. A single procedure can potentially be affected.
1 very low	< 10k	Isolated critical reactions in local or regional media	Interference with a non-critical business process for up to one day. A single procedure can potentially be affected. Random errors are detected and require a cleanup effort.

3.3 Risk Matrix

Based on the previous two metrics, the HERMES framework suggests the following risk matrix:

Likelihood / Impact	**1 – very unlikely**	**2 – unlikely**	**3 – rare**	**4 – possible**	**5 – likely**	**6 – very likely**
6 – critical	6	12	18	24	30	36
5 – high	5	10	15	20	25	30
4 – substantial	4	8	12	16	24	28
3 – moderate	3	6	9	12	15	18
2 – low	2	4	6	8	10	12
1 – very low	1	2	3	4	5	6

3.4 Legend

Legend	**Description**	**Value range**
High	Significant risks whose effects are critical to catastrophic. It is imperative to reduce these risks.	>= 18
Medium	Risks whose effects are considerable and therefore must be reduced.	8 – 17
Low	Are risks that are either inherent (in the protected object as such) or can be neglected. These risks should be further minimised with simple measures.	<= 7

4 Risik analysis

4.1 Generic risks

Ref	Summary	Description	Risk rating	Mea-sures	Residual risk
GEN-R1	Disaster situation	The Justitia.Swiss platform can no longer be used due to a disaster situation (e.g., fire in the datacenter). The following is considered a disaster situation: fire, water, natural disasters, pollution, dust, corrosion.	8 - medium	2	6 - medium
GEN-R2	Power or communication outage	Due to failure or malfunction of infrastructure components (e.g., power failure or communication network failure) or an error on the part of the platform operator, the Justitia.Swiss platform can temporarily not be used.	8 - medium	2	8 - medium
GEN-R3	Outage of service provider	Due to failure or disruption of service providers (e.g., subcontractors of the software supplier or the platform operator), the Justitia.Swiss platform cannot be reliably operated and/or further developed	8 - medium	2	8 - medium
GEN-R4	Spying	Spying information or users that interact with the platform (e.g., using wiretapping).	12 - medium	2	9 – medium
GEN-R5	Theft or loss	Theft, or loss of devices, data carriers, software, utilities, or documents.	6 - low	3	4 – low
GEN-R6	Bad planning	The Justitia.Swiss platform is not adapting to changes regarding the requirements or regulations of the Swiss justice system because the corresponding IT service management processes (e.g., release management, change management) are missing or not functional.	16 - medium	1	16 - medium
GEN-R7	Manipulation	Manipulation of information, hardware or software	24 - high	3	20 – high
GEN-R8	System failure	Destruction, failure or malfunction of devices or systems. Includes destroying of servers, devices, storage, etc.	12 - medium	1	12 – medium

GEN-R9	Software vulnerabilities or errors	The more complex the software, the more frequently errors occur. Even with intensive testing, not all errors are discovered before the software is deployed. Software vulnerabilities can further be exploited by attackers to compromise the platform, introduce malware, read data without authorization, or manipulate the configuration of the platform. For example, a buffer overflow might be used to read/write data out of the boundaries of the buffer, in the worst case leading to remote code execution on the platform.	25 - high	6	15 – medium
GEN-R10	Violation of laws or regulations	Violation of statutory provisions or regulations	12 - medium	2	12 - medium
GEN-R11	Misuse of administrative privileges	Manual or machine access with extensive authorisations is misused to view the data transferred via the platform or to manipulate data transferred via the platform or to manipulate the data stored on the platform. The attacker may be a malicious administrator of the platform or an unknown third party who has gained access to the platform operator's environment.	18 - medium	4	15 - medium
GEN-R12	Personnel shortage or absence	Absence of personal (vacation, illness, etc.) that cannot be compensated adequately and prevents the correct operation or further development of the platform.	12 - medium	2	9 – medium
GEN-R13	Data misuse	Misuse of personal data	9 - medium	2	9 – medium
GEN-R14	Denial of service attack	Attack on the availability of the platform by using a volumetric or non-volumetric attack.	10 - medium	3	10 – medium
GEN-R15	Physical intrusion	Unauthorized intrusion into premises of the operator, software developer, or KKJPD.	8 - medium	1	8 – medium
GEN-R16	Data loss	Data is lost and irrecoverable due to one of the following reasons: - Lack of adequate backups - Hardware failure - Corruption of data - Data destruction	12 - medium	1	9 – medium

4.2 Project related (operational) risks

4.2.1 Out of scope

The operational risk analysis does not consider manipulation of data that is out-of-scope of the ISDS concept (e.g., end user or authority IT infrastructure).

4.2.2 Risks for business processes (BP)

This section describes risks related to operational use cases of the platform, including submissions, deliveries, and dossier access.

Ref	Summary	Description	Risk rating	Measures	Residual risk
BP-R1	Submissions, delivery, or dossiers are manipulated or corrupted	Files that are part of a submission, delivery, or dossier are manipulated or corrupted on the platform or in transit. Such modifications can occur in different contexts: ▪ In transit (after being submitted by the end user) ▪ At rest (while stored on the platform) ▪ In use (e.g., during processing on the platform) The course and/or outcome of judicial proceedings can be influenced by such targeted manipulation.	24 - high	2	tbd
BP-R2	Submissions or deliveries are denied by a party	A party to the proceedings denies that it has conducted a submission or delivery via the Justitia.Swiss portal (e.g., to influence ongoing proceedings).	16 – medium	1	tbd
BP-R3	Submissions or deliveries are conducted using a false identity	An attacker conducts a submission or delivery using a false identity of a party that is potentially associated to the corresponding proceedings. As a consequence, the party whose identity was misused, could be substantially disadvantaged or harmed in judicial proceedings.	20 – high	2	tbd
BP-R4	Submissions, deliveries, or dossiers are viewed by unauthorised third parties	An attacker (including unauthorized users or insiders) accesses submissions, deliveries, or dossiers without authorization.	25 – high	tbd	tbd
BP-R5	Unauthorized access to metadata of submissions, deliveries or dossiers	An attacker accesses metadata associated with submissions, deliveries, or dossiers without authorization. This also includes legitimate	25 – high	1	tbd

		Justitia.Swiss platform users who, due to access to procedural data on cases in which they are not even involved due to an error in the application or in the access control.			
BP-R6	Submissions, deliveries, or dossiers get lost	Submissions, deliveries, or dossiers are deleted, corrupted or lost before they have been stored in an electronic file or otherwise processed by the addressed judicial authority.	16 – medium	3	tbd
BP-R7	Submissions, deliveries, or dossiers containing malware damage the systems of the platform or the recipients	Malware (including ransomware) is uploaded to the platform using a submission, delivery or as part of a dossier. The malware is potentially transferred by the platform to the recipient and could damage its IT systems. The likelihood of this risk is considerable since any person with an account of the platform can upload files and create a submission.	18 – medium	4	tbd
BP-R8	Authority cannot retrace dossier access of a deputy	A deputy accesses a dossier, but this event cannot be re-traced by an authority who gave access to the dossier.	12 – medium	tbd	tbd
BP-R9	Permission changes do not get applied correctly	The permission of a user to access specific documents as part of a dossier is changed (e.g., due to a membership change) and these changes need to be applied correctly.	16 – medium	tbd	tbd
BP-R10	Incorrect configuration or misuse of permission assignment	Specific functionality supported by the platform can be assigned by the owner/administrator of an entity. This could lead to misconfiguration or intentional misuse. For example, an organisation administrator can give access to files of its organisation to any users that are registered on the platform.	16 – medium	tbd	tbd
BP-R11	Submission is conducted using an incorrect file identifier	A user mistakenly or maliciously enters an incorrect file ID when submitting a submission, whereupon the submitted files are processed in the wrong context and/or filed in the wrong electronic file. This can affect the management of the procedures involved.	12 – medium	tbd	tbd
BP-R12	Unauthorised access to the user directory	A user or third party might gain unauthorised access to the user directory, which should not be accessible by a private person.	12 – medium	tbd	tbd

BP-R13	Accumulation of permission using different contexts	A user that is part of multiple organisations might be able to accumulate permissions from different organisation-specific contexts. For example, an employee of a law firm can also act as a private person (and thus should not have access to the user directory).	12 – medium	tbd	tbd
BP-R14	Insufficient ability to provide information about existing permissions	The assignment of permissions on the Justitia.Swiss platform takes place on three levels: 1. Permissions to access dossiers or specific files are granted in the scope of a submission (and might be changed later). 2. Permissions to access functionality and data can be granted for organisations by its administrator. A user can be part of several organisations simultaneously. 3. Using delegation a user can grant permissions to any other registered users.	12 – medium	tbd	tbd

4.2.3 Risks for administrative processes (AP)

This section describes risks related to administrative use cases of the platform such as the administration of organisations, delegations, etc.

Ref	Summary	Description	Risk rating	Measures	Residual risk
AP-R1	Incorrect configuration of judicial authorities on the Justitia.Swiss platform	Incorrect data is entered for a judicial authority. This can lead to submissions being sent to the wrong address (e.g., a third party impersonating an authority). In the worst case, this could lead to an adversary giving access to fake documents in the name of an authority.	12 – medium	7	tbd
AP-R2	Registration of a user profile using a fake identity	A malicious third party registers himself using a fake identity and then uses this account to file submissions or to obtain unauthorized access to judicial files.	15 – medium	7	tbd
AP-R3	Incorrect administration of user attributes in the subscriber directory	The attributes of registered users are incorrect or inaccurate. Incorrect address data (email, postal address, etc.) could lead to notifications being sent to the wrong recipient. Incorrect authorization data (e.g., role or deputy assignments) can lead to access rights being granted unnecessarily.	15 – medium	tbd	tbd

AP-R4	Incorrect administration of group memberships	The group memberships are updated incorrectly or not updated in time. For example, in case the function or organisational affiliation of a platform user changes, this change needs to be reflected into the permissions/roles of a user profile. Examples where such membership changes occur are the following: • A law firm associate transfers from law firm A to law firm B • An employee of a legal department at company X moves to the legal department of company Y. In addition, a group administrator could also mistakenly add user to a group or miss out on removing a user.	12 – medium	tbd	tbd
AP-R5	Distinct administration domains to manage the permissions of profiles that are part of multiple organisations	Users can be part of multiple organisations with possibly distinct administration domains. Thus, overall domain exist to examine and administrate the permissions of profiles exist.	12 – medium	tbd	tbd
AP-R6	Affiliations of users to organisations are not maintained	Organizational changes (e.g., resignations or internal function changes of law firm employees) must be manually tracked by the organization administrators when managing the organizational affiliations, because the Justitia.Swiss platform does not provide for reconciliation with external systems (e.g., IAM or HR systems of judicial authorities) for the pilot phase. Previous experience from larger organizations shows that departures and internal function changes in manually administered user directories are often only tracked with a delay (or not at all). This can lead to a situation where a user who, for example, changes its affiliation from a judicial authority to a law firm can continue to use the authorizations of his old employment for a certain period of time in the context of the new employment.	20 – high	tbd	tbd
AP-R7	Delegations are not maintained	Changes to affiliations may require the adjustment of delegations	20 – high	4	tbd
AP-R8	Registration of a fake group	A malicious third party registers fake group on the platform with	16 - medium	7	tbd

		the intent of impersonation.			
AP-R9	Mass creation of profiles/groups	A malicious third party registers masses of profiles, groups, etc. to increase its attack potential (e.g., using collusion).	12 – medium	tbd	tbd
AP-R10	Compromise of a user profile	A user profile is compromised by a malicious third party. The compromised profile is then used to access and/or manipulate data transferred using this specific profile. In case the user profile is part of an authority, also data owned by this authority might be affected.	12 – medium	5	tbd

4.2.4 Risks for operation of platform (OP)

This section describes risks related to the operation of the platform.

Ref	Summary	Description	Risk rating	Measures	Residual risk
OP-R1	Compromise of the platform	Successful compromise of the Justitia.Swiss platform by a hacker. This could be possible e.g., due to a vulnerability in the code, outdated software versions, WAF rules too permissive, or misconfiguration of a platform component. The compromise is then used to access or manipulate data that is transferred via the platform.	24 – high	tbd	tbd
OP-R2	Advanced persistent threats (APTs)	Advanced persistent threat (APT) gain unauthorized access to the platform and remains undetected for an extended period. The compromise is then used to access or manipulate data that is transferred via the platform.	24 – high	tbd	tbd
OP-R3	Misuse of the signing service	The signing service gets misused by a user or third party to obtain a valid signature for a file (e.g., PDF document). This file could then be used in different contexts and appears to be issued by the platform.	12 – medium	tbd	tbd
OP-R4	Misuse of the notification service	The notification service gets misused by a user or third party to send notifications to other users of the platform. The notification appears to be issued by the platform and thus could be misused for targeted attacks on users (phishing).	12 – medium	tbd	tbd

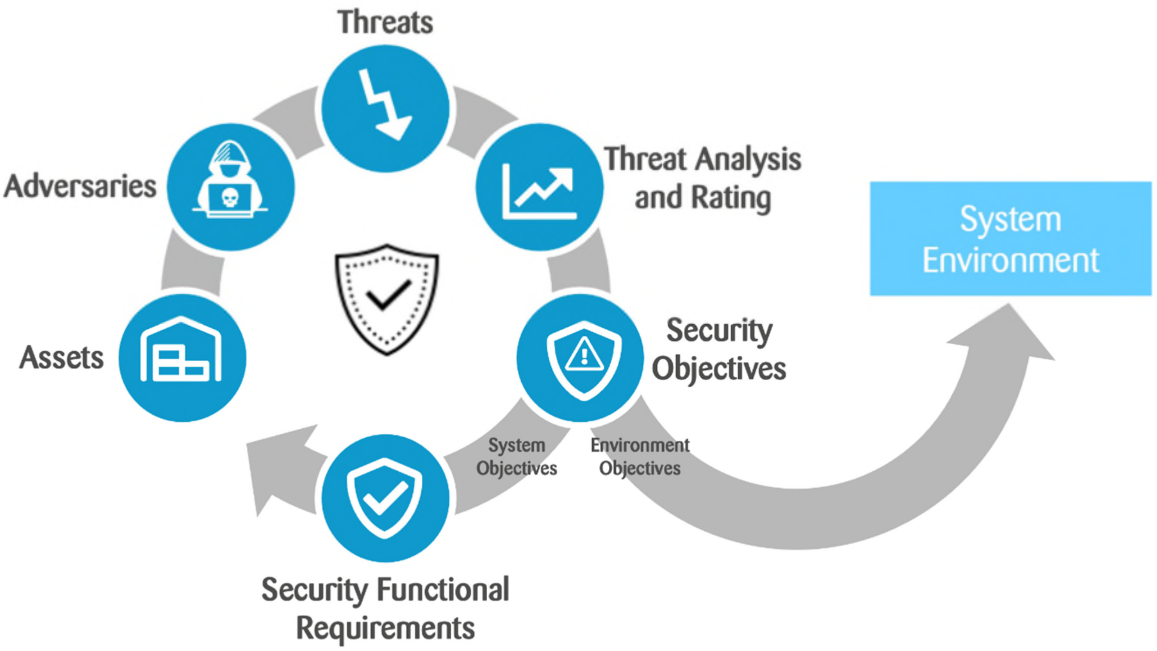
OP-R5	Malicious identity provider	An identity provider that is integrated with the justitia.swiss platform becomes maliciously. For example, this could mean that the provider claims that a user has logged in in order to get unauthorized access to the users data stored on the platform.	12 – medium	tbd	tbd
OP-R6	Supply chain attack	Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: • Manipulation of development tools / development environment • Manipulation of source code repositories (public or private) • Manipulation of source code in open-source dependencies • Manipulation of software update/distribution mechanisms • Compromised/infected system images • Replacement of legitimate software with modified versions • Sales of modified/counterfeit products to legitimate distributors • Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels. Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency. This can affect the integrity and availability of IT systems used to run the platform.	18 – high	tbd	tbd
OP-R7	DNS spoofing	Using DNS cache poisoning, the user is redirected to a spoofed, attacker-controlled website. The attacker can thus deliver arbitrary content to the user's browser and interfere in the communication from the user to the website.	12 – medium	tbd	tbd
OP-R8	Malware / Ransomware	The platform gets compromised by a malware either due to a platform compromise, a vulnerability	24 - high	tbd	tbd

		in a platform component, or a malicious administrator. This includes potential contamination of the platform by ransomware.			
OP-R9	Social engineering	The main characteristic of social engineering attacks is deception about the identity and intent of the attacker. These attacks can affect the platform in a various ways: ▪ Phishing / spearphishing: for example, an attacker sends an email to a user that appears to be sent by the platform. ▪ An attacker contacts a user and pretends to be an administrator of the platform and tries to get access to the users account ▪ An attacker calls the service desk and pretends to be a different person.	20 – high	tbd	tbd
OP-R10	Security risks are not adequately dealt with	Operational security risks are not identified correctly and thus lead to the platform being vulnerable to attacks.	12 – medium	Tbd	tbd
OP-R11	System adminstrator compromise	A system administrator account gets compromised, leading to the compromise of the Justitia platform.	24 – high	5	tbd

5 Threat modelling

5.1 Methodology

In order to run a threat modelling methodology that is both valuable (i.e., effective in identifying and mitigating threats) and complete (i.e., covering an extensive part of the system), the following illustrated approach is used:



Given the considerable complexity of the justitia.swiss platform, the threat analysis is conducted as follows:

divide the risk landscape into business-owned segments. The segmentation can be done along different dimensions: architecture components, business processes, time criticality, attackers and their capabilities, assets of the underlying business case, data flows in the systems, etc.
let segment owners conquer those segments.

5.2 STRIDE thread model overview

				Applicability			
	Threat	**Violated property**	**Threat definition**	**External entity**	**Process**	**Data flow**	**Data store**
S	**S**poofing identities	Authentication	Spoofing involves a threat actor masquerading as another user or entity to gain unauthorized access to a system.	X	X		
T	**T**ampering with data	Integrity	Tampering involves a threat actor modifying or altering data in transit or at rest, potentially leading to unauthorized access or a breach of sensitive information.		X	X	X
R	**R**epudiation	Non-repudiation	Repudiation involves a threat actor denying responsibility for an action.	X	X		X
I	**I**nformation disclosure	Confidentiality	Information disclosure involves a threat actor gaining unauthorized access to sensitive information.		X	X	X
D	**D**enial of service	Availability	Denial of service involves a threat actor disrupting or preventing normal system operations.		X	X	X
E	**E**levation of privilege	Authorization	Elevation of privilege involves a threat actor gaining unauthorized access to system resources, potentially leading to unauthorized access to sensitive information or system compromise.		X		

6 Security measures

wip = work in progress

6.1 Organisational security measures (MO)

Organisational security measures encompass a range of processes and requirements to uphold the security of the Justitia.swiss platform.

Ref.	Measure title	Status
MO1	Detailed concepts for information security	wip
MO2	ISMS of the örK certified according to ISO/IEC 27001	n/a
MO3	Security Information and Event Management (SIEM)	wip
MO4	Awareness program for all user groups	wip
MO5	No transfer of secret data via the Justitia.Swiss platform	done
MO6	Periodic review of the address directory	open
MO7	Periodic recertification of all valid deliveries	open
MO8	Quarterly recertification of all valid delegations	open
MO9	One profile per organizational affiliation	wip
MO10	Security responsibility of the software supplier as part of the contract	wip
MO11	Security responsibility of the platform operator as part of the contract	wip
MO12	Security responsibility of the judicial authorities as part of the affiliation agreement	wip
MO13	Security responsibility of the process participants as part of the terms of use	wip
MO14	Security measures also apply to judicial authorities involved in proceedings	done
MO15	Reliable caller identification by the service desk	open
MO16	Secure Software Development	wip
MO17	Right of audit of the public corporation with the platform operator	done
MO18	Penetration testing of all interfaces to the platform	wip
MO19	Vulnerability monitoring of all Internet access points	open
MO20	Source code analysis of all security modules	wip
MO21	Monitoring of cyber squatting	wip

6.2 Application security measures (MA)

Application security measures describe security requirements by the platform to safeguard sensitive data, ensure uninterrupted functionality, and mitigate the risks associated with cyberattacks and unauthorized access.

Ref.	Measure title	Status
MA1	Electronic platform seal for all inputs	wip
MA2	Possibility to enter digitally signed files in advance	wip
MA4	The platform records all legally binding events in receipts	wip
MA5	The platform can generate electronically sealed receipts of receipt and retrieval	open
MA6	2-factor authentication (2FA) of all users	wip
MA8	Mutual authentication of endpoints for all API connections	open
MA9	Quality assurance for transmitted structured data	open
MA12	Access control system for data and functions of the Justitia.Swiss platform	open
MA13	Submissions and file items are not stored outside the DossierStore	open
MA14	Files added to the system are collected online	open
MA15	Seal validation for electronic file inspection	wip
MA16	Notification of the recipient of a delivery	open
MA17	Authorization-relevant elements of a delivery are never entered manually	open
MA18	The authorization effect of a submission, service and file inspection can be checked	open
MA19	Deliveries can be cancelled on the platform Justitia.Swiss	open

MA21	Electronic seal for all file items in the central DossierStore	open
MA23	No direct write access to the central DossierStore	open
MA24	Only administrators of authorities are granted reading rights for their own DossierStore	open
MA26	Defined minimum quality level for each attribute in the address directory	open
MA27	Multi-level quality model for the attributes in the address directory	open
MA28	Defined owner for each attribute in the address directory	open
MA32	Defining the organization-independent basic authorizations	open
MA33	Provide rules for organizational assignment	open
MA34	Delegations are temporary and valid for a maximum of 12 months	open
MA35	QA system for transaction processing and data files	open
MA36	Encryption on application layer	done

6.3 Technical security measures (MT)

Technical security measures encompass a range of safeguards implemented in digital systems to protect against potential threats and vulnerabilities.

Ref.	Measure title	Status
MT1	Crypto-keys: generation and storage of unwrapped keys in HSM	wip
MT2	Encryption of the communication between user and platform	wip
MT3	Virus scan on the platform Justitia.Swiss for all transferred files	wip
MT4	Quarantine area for potentially malicious files	open
MT6	Web Application Firewall (WAF) und API-Gateway	wip
MT7	Risk-dependent access control on the Justitia.Swiss platform	open
MT8	Limited session lifetime on the Justitia.Swiss platform	done
MT9	Physical separation (anonymous area as well as non-productive and productive environments)	done
MT10	Secure administration access at the platform operator (PAM)	open
MT11	Secure remote support solution at the service desk	open
MT13	Central logging service for technical logs and the audit trail	wip
MT14	Secure configuration of all web servers of the Justitia.Swiss platform	wip
MT15	Alternate site and BCM	wip
MT16	Connection of identity providers via secure federation protocols	wip

7 Residual risks

The residual risks are calculated on an on-going basis and will be reported to the steering committees prior to the start of the MVP.