This is a peer-reviewed, accepted author manuscript of the following conference paper: Edu, J., Hooper, M., Maple, C., & Crowcroft, J. An impact and risk assessment framework for national electronic identity (eID) systems. Paper presented at International Conference on AI and the Digital Economy, Venice, Italy.

An Impact and Risk Assessment Framework for National Electronic Identity (eID) Systems

Jide Edu[1], Mark Hooper[1], Carsten Maple[1], and Jon Crowcroft[1]

[1] *The Alan Turing Institute*

Abstract

Electronic identification (eID) systems allow citizens to assert and authenticate their identities for various purposes, such as accessing government services or conducting financial transactions. These systems improve user access to rights, services, and the formal economy. As eID systems become an essential facet of national development, any failure, compromise, or misuse can be costly and damaging to the government, users, and society. Therefore, an effective risk assessment is vital for identifying emerging risks to the system and assessing their impact. However, developing a comprehensive risk assessment for these systems must extend far beyond focusing on technical security and privacy impacts and must be conducted with a contextual understanding of stakeholders and the communities these systems serve. In this study, we posit that current risk assessments do not address risk factors for all key stakeholders and explore how potential compromise could impact them each in turn. In the examination of the broader impact of risks and the potentially significant consequences for stakeholders, we propose a framework that considers a wide range of factors, including the social, economic, and political contexts in which these systems were implemented. This provides a holistic platform for a better assessment of risk to the eID system.

1 Introduction

In this age of digital interaction, the ability to prove identity digitally has become increasingly crucial and valuable. Many governments around the world are now using electronic identification (eID) systems to assert and prove residents' identities to facilitate the delivery of e-services, welfare and benefits. Such systems have become important development initiatives that enable sustainable development and have helped empower citizens by enhancing their access to rights, services, and formal economy [1]. These systems make it easier to provide a range of services that broaden financial inclusion, unlock economic value, increase access to social safety nets, and raise gender equality by offering a secure and precise method for identifying the population [2]. Furthermore, with eID systems, nations can comprehensively understand their citizens' political, educational, and economic behaviour to better plan and address their needs [3].

As eIDs are becoming an important facet of national development, any failure, compromise, or misuse of the system could be costly and damaging to the government, users, and society. There have already been reports of security and privacy incidents in media involving eID systems, such as in the case of Aadhaar, where over 200 government websites exposed Indian citizen data to the public [4]. More importantly, these systems hold massive data belonging to millions or even billions of individuals (such as India's Aadhaar system [5]), making them interesting targets for adversaries. Hackers, cybercriminals, insider threats, and nation-states all pose enormous threats to the eID system [6].

Furthermore, existing studies have demonstrated a set of unique challenges associated with these systems owing to their scale [4]. For instance, extensive data logging means that they can be used to profile registered users easily. Researchers have proposed various techniques for protecting data at scale, for example, using differential privacy techniques on the anonymised log, but it has become apparent that this is not a one-size-fits-all solution [7]. Thus, compromising such a system could provide attackers with access to valuable and sensitive information, necessitating the need to develop a robust understanding of potential risks.

An excellent starting point for securing a sociotechnical system, such as an eID system, is focusing on its risks [8]. However, focusing on risk requires considering the impact of potential threats instead of simply identifying all possible threats [9]. Despite the fast-growing research on identification system security and privacy issues, there is a lack of research on how to systematically assess the impact of successful compromise on eID systems. This study aims to fill this research gap by answering the following main research question: How can we systematically assess the impact of compromise on eID systems? There are many eID systems, all of which are contextual in their design and operation [10]. These systems are characterised by path dependency [11], their context [12], and the culture they are part of [13]. Like most complex sociotechnical systems, the impacts of risk vary across the different stakeholders [14]. Any failure of critical system goals affects stakeholders differently based on what they value.

In this paper, we present a framework for assessing the risks and impacts of a compromise on eID systems. We identify the key stakeholders in eID and discuss their values (Section 3). Based on the common decomposition of risk into impact and likelihood, we discuss possible risk impact areas for assessing the impact on the stakeholders (Section 4). We further discuss in Section 5 how these impact areas can be used to conduct an effective risk assessment of eID systems. We focus on national eID systems in particular: those designed to serve a wide range of purposes, including but not limited to population registers, unique identification numbers,

and national identification cards. These systems typically aim to pursue public policy objectives such as streamlining public administration, increasing security, managing services, or public governance. Examples include the Estonia identity system [15], which offers eID to allow its citizens to vote, submit tax claims, and check medical records, and the Aadhaar system [5] that provides unique identification to Indian citizens and lets them access government services.

This paper makes the following key contributions:

- We identify key eID stakeholders and their values that need to be protected against risk.
- We propose a multi-stakeholder impact assessment approach, allowing independent assessment of varied risk impacts on eID stakeholders.
- We implement a prioritisation technique to account for the contexts of use of the eID system and the differences in what stakeholders value.

2 Challenges

There are numerous challenges in evaluating the impact of compromise on identification systems. First, there is the problem of scarce data. Only a few governments or development partners have rigorously assessed the effects of compromise on national identity systems. Even when they do,the assumptions and figures behind the estimations are usually not publicly available [16]. Besides, governments and identity solutions providers may have incentives to downgrade the impacts [17].

In addition, it is challenging to define uniform risk impact evaluation metrics across various sectors and agencies because the design and use of identification systems are multilayered and rarely comparable across nations [18]. While cyber risk impact has usually been assessed from the three central technical aspects of information security: confidentiality, integrity and availability, the specific attributes of eID systems, as opposed to IT systems, often prevent the straightforward application of these risk impact assessment criteria. Moreover, focusing only on technical aspects is insufficient to justify investment in security [19] and provides no insight into stakeholder impacts.

Likewise, measuring risks to complex systems like identification systems is complicated. The far-reaching and diffuse nature of the effects of compromise presents greater issues for assessment. For instance, in relying private parties such as financial institutions, identity touches nearly every transaction that involves an exchange of value or trusts [2], and potential impact could be identified for almost every corner of the sector. Thus, we are limited in our ability to create a valid quantitative impact evaluation model for the identification system. Instead, this paper uses existing literature on digital identity, news articles and reports to draw some initial conclusions and proposes an analytical framework for assessing the impact of compromise on an eID system.

3 Key eID Stakeholders

In the context of eID, stakeholders are individuals and organisations involved in creating, maintaining, and using an ID system throughout the identity lifecycle. To better capture the impact of a compromise on stakeholders, we need to first understand who these stakeholders are and their roles.

The eID scheme comprises three primary stakeholders [1]. The provider of the eID scheme (the government), the individuals being identified, and the organisations relying on it for customer identification.

Government: government agencies are the primary providers of the ID systems. These include population registrars, National ID agencies, civil registrars, etc., that register people in the ID system and issue and manage credentials. In addition, they are responsible for managing and updating the identity data, resolving disputes and offering authentication and verification services at various levels of assurance [20]. Other government agencies also use these ID systems to interact with people or provide functional ID systems.

Individuals: These are the people at the centre of the Id systems. They are the system subjects whose personal data are collected. They are entitled to exercise appropriate control over their data collection, storage, and dissemination. Likewise, they are the people who use their credentials and proof of ID to access rights and services [20]. Therefore, building an ID system capable of advancing development objectives must begin with an understanding of and response to people's ID-related needs and concerns [12].

Relying private organisations: Many organisations use government ID systems to identify their customers, such as requiring government-issued credentials to open bank accounts, register SIM cards, or set up credit reporting systems. This stakeholder uses ID providers' platforms, credentials, and services to authenticate or verify the end-users identities.

Other stakeholders such as civil society, international organisations and development partners [20] also help people use eID systems, advocate for inclusion, and serve as sources of critical feedback for eID system planning and implementation.

4 Impact Assessment Factors

Assessing the impact of risk on different eID stakeholders involves considering the potential consequences of the risk event for all stakeholders affected by it. As a first step, we need to establish the key factors to consider when evaluating the impact of risk on the identity system's mission and objectives. This entails establishing a set of evaluation criteria against which the consequences of a realised risk can be assessed [21]. Besides, defining evaluation criteria is essential to security risk management as security threats must have a clearly defined impact before they can be considered system risks [22]. However, because the consequence of a single risk event to these systems can have multiple potential impacts on various stakeholders depending on their value, it is paramount to establish risk impact areas that align with these values.

We distinguish three types of impact on an eID system: "impact on the government", "impact on the end-users"; and "impact on the relying private organisations". These are further discussed below:

4.1 Impact on the government

To understand the government value attributed to implementing an eID system and which areas the risk might impact, we analyse the existing literature on public value.

The authors in [23] proposed a Public Return On Investment (PROI) framework to evaluate the value of government investments in information technology. The framework identifies two public return sources: value to the public that comes from improving the government as a whole from the point of view of the citizens and the value that comes from providing specific benefits directly to individuals, groups, or the general public. PROI defines six main government values based on the different impacts government investments in information technology can have on public stakeholders' interests. These are *financial, political, social, ideological, stewardship, and strategic values.* Another framework to value various government initiatives proposed in [24], Value Measuring Methodology (VMM), also identified five key government values: direct value to customers, social and public value, financial value to the government, operational and foundational value to the government, and strategic and political value.

Using these different value measurement dimensions, we distinguish seven key risk impact areas for the government, as shown in Table 1: *reputation, economic, social, political, operational, physical, and rights.*

Table 1: Derive government impact areas from PROI and VMM frameworks

Impact Category	**PROI**	**VMM**
Economic	Financial	Financial
Reputation	Ideological	
	Stewardship	
Social	Social	Social and public
Political	Political	Strategic and political
	Strategic	
Citizen rights		Customer direct value
Operational		Operational

Reputation Impact: The reputation impact is related to the citizen's trust in the government. It is essential that an eID system is widely adopted. One of the critical elements for wide adoption is public trust in the system [25]. Trust in the government is essential for the public acceptance of eID systems. A lack of trust will prevent citizens' participation, jeopardising the identity program, thereby widening rather than closing the humanitarian divide. Apart from harming users' trust, there could also be damage to trust relationships with other governments or non-governmental entities. Thereby undermining the eID system's usefulness by making it difficult for organisations to rely on them for secure authentication and authorisation. Thus, measuring the impact of any compromise on trust in the government and the ID system is critical.

Economic Impact: This includes all direct and indirect financial damages experienced by the ID agency. The financial implications can be assigned according to the ID agency's financial loss in terms of the *one-time financial cost* or *operating cost* of investigating and rectifying the compromise. Likewise, we could measure the economic impact in terms of *revenue loss*, as governments use the system to improve their revenue through better tax collection [1, 26]. In addition, the eID system offers government financial gains by limiting potential leaks in government benefit programs and eliminating bloated civil service wages from ghost workers [1]. A compromise could result in financial loss to the government. For example, in 2011, claims filed in the US under compromised identities resulted in fraudulent unemployment benefits payments totalling $3.3 billion [27]. The economic impact could also be in terms of economic growth and innovation, budget impact, workforce loss, diminished foreign investments, or fines and legal penalties [28].

Rights: eID systems allow governments to perform their obligations under international human rights law by giving every citizen the right to be recognised as a person and to be treated equally before the law [18]. The government leveraged identification systems to create transparency, fairness, and well governed services. These systems are carefully designed for inclusion, fairness, equity, and accessibility. This is because the government aims to ensure equal access to digital services for all citizens. Hence, these systems are implemented to facilitate access to public and private services, particularly for less-privileged parts of the population [18]. The size and quality of readily available services in a broader eGovernment ecosystem are some of the literature-identified adoptions and acceptance drivers [29]. Impact evaluations can attempt to determine the number of people/end users who have been excluded and do not have access to the identity service. The implementation of robust and inclusive identification systems also correlates with broader levels of effective governance.

Social Impact: One of the fundamental principles of identification for sustainable development is to create an interoperable platform that is responsive to the needs of various groups of users [30]. In addition to fairness, equity, and inclusiveness, measuring the effectiveness and efficiency of service delivery that utilises an identification system is also important. Like the private sector, the government can be considered a service provider for its customers— citizens. Its ultimate objectives are to improve overall social welfare and satisfy citizens' demands and needs [31]. A compromise could cause damage to or hinder a critical infrastructure sector impacting the way people live and interact in society.

Political Impact: A compromise could impact public influence and disrupt political processes, threatening national security. Countries have used eID to prevent vote rigging. For example, Nigeria uses eID to authenticate voters using biometrics, preventing approximately 4 million duplicate voters [1]. In this instance, a compromised eID system could make it more likely that election results will be disputed, increasing the risk of election violence and the associated human and financial costs.

Operational Impact: Operational impact refers to the operational damage that affects the mission capability of the government and its effectiveness. Suppose the compromise eID is used for a non-time-sensitive transaction, the impact of a limited-duration availability compromise on the government's objective and public confidence will be minimal in most cases. However, the availability of time-sensitive information is less likely to be restored before significant harm is done to the agency or public welfare. The impact of compromise on government operations can also be evaluated based on the number of teams that deal with risk events.

Physical Impact: Physical impact refers to the damage or destruction to the government's physical properties, assets or resources. This can include staff, equipment, buildings, and other infrastructure used to support an eID project.

4.2 Impact on relying private organisations

Private organisations rely on digital identity services for identification purposes. However, unlike in public organisations, the value attributed to private parties differs owing to diverse needs and requirements. In a private market, the ultimate goal of a business is profit and shareholder value maximisation [31]. Most private sector valuation methods are inextricably linked to economic value and are measured in monetary terms. However, besides financial value, there are other values, such as the operational value of increasing productivity, service quality and compliance, and the social value of improving customer satisfaction [31]. Next, we discuss how a compromise in eID systems might affect these values.

Economic Impact: Relying private organisations benefit from a robust and inclusive identification system. The ability to accurately identify customers, mitigate fraud risk, and reach new markets for trusted users and partners is essential to private organisations. A compromise could result in a regulatory fine, compensation payments, disrupted turnover, PR response costs, and reduced profits. In some cases, relying private parties may also face legal liabilities if they are found to have failed to adequately protect personal data or to have used inadequate security measures when relying on an eID system.

Operational Impact: Operational impact here refers to the extent of the breach on the business mission and objectives of the private organisations or the effect of the service interruption. Besides, private organisations that rely on eID systems are service providers for the citizens [31].

Physical Impact: The physical impact can be assessed based on damage or destruction to the organisation's physical property or resources. This includes staff, equipment, buildings, and other types of infrastructure.

Reputation Impact: A compromise can also impact the reputation of relying private parties. The reputation impact is related to the citizen's trust in the organisation. For example, if a breach occurs through relying private parties, they may experience public backlash and loss of customer trust. Reputation impact could be measured in terms of damage to public perception or the level of media scrutiny. How an organisation handles a compromise could also impact its reputation.

Social Impact: The social impact here refers to the effect of compromise on the people and communities in which the relying party operates and serves. This area could be evaluated by the impact on the organisation's activities, such as the jobs it creates and the products or services it provides. Besides, many organisations are increasingly focused on maximising their positive social impact by implementing sustainable business practices, supporting local communities, and engaging in corporate social responsibility initiatives.

4.3 Impact on End-Users

End-Users are more concerned with the identity system's transparency, usability, accessibility, availability, privacy, and security [12]. We distinguish six key risk impact areas for end-users: rights, physical, privacy, social, psychological, and economical. These are further discussed below.

Privacy Impact: One of the most valuable assets of an eID system is personal data. Therefore, compromising such a system will impact users' privacy, even though this may affect users differently depending on what they value. An important contributing factor is what has happened to the data: has it been made public, changed, or used to make decisions that affect people? If exposed, to whom and what harm could and would they cause? This will help to better measure the severity of violations. As end-users are people whose personal data are collected, they are the ones that will be directly affected by privacy violations. The fact that only individuals (end-users) can directly experience a privacy problem is especially challenging for assessing the impact.

Right: Not only does eID enable people to exercise their rights in an inclusive manner, it also holds them accountable for their obligations. For instance, eID can make it easier for citizens to access government services, especially those excluded because of the difficulty in obtaining physical documents or living in remote areas [1]. The impact of an identity breach could be evaluated by what service restriction it can cause, including those we consider fundamental human rights. Is it a breach that causes the risk of right violations that would not ordinarily be subject to enforcement efforts or those that are particularly important to enforcement programs?

Social Impact: This impact area measures how a breach affects society through the options available to end users. A compromised identity system has significant repercussions for citizens, who may be denied access to numerous services, and society at large, which is unable to develop or organise effectively [30]. In an eID system, the capability and opportunity should be equal, and the process of choosing and seeking a specific opportunity should also be fair to all end-users [10]. A compromised national identity system could impact end-users by introducing barriers to access and usage, thereby creating disparities in the availability of information and technology.

Psychological impact: There could be psychological impacts on end-users, including, but not limited to, suffering, inconvenience, and distress. This might occur due to not having access to a critical service, especially if this happens over a long period or on more than one occasion. It could also be the time the end-users spent and their efforts to seek a resolution for the breach. End-users might also suffer from anxiety, upset or stress due to compromise. For example, criminals may commit non-financial crimes in another person's name (identity theft), for which the victim is held accountable and suffers the consequences [32]. Sometimes, the psychological impact lasts much longer than the financial impact.

Physical Impact: It is crucial to assess the impact the compromise might have on people's lives, particularly if the breach could harm them. A compromise resulting in identity theft that allows criminals to falsify registration details could support child labour and human trafficking [33], which has significant implications for individuals' safety. Moreover, exclusion from life essential programs such as food security schemes can lead to starvation and death [34]. People can also be exposed to physical harm, as was the case during the Rwandan genocide when roadblocks used ethnicity written prominently on Rwandan ID cards to determine who would be murdered [35].

Economic Impact: Economic impact refers to the financial loss suffered by users in terms of the cost of services or fraud instead of loss of profit. For example, end-users can be financially impacted if an attacker uses their identity for unauthorised financial transactions [2].

5 Overview of the framework

Risk assessment is an essential part of best risk management practice. The core idea behind risk assessment is to employ analytical and structured methods to gather data, opinions, and evidence about what is at risk, the likelihood of unwanted events, and a measure of the impacts. There are many different approaches to risk assessment (we refer readers to [36] for detailed analysis). Our framework is based on these standard methodologies and aims to compute the risk for the eID system considering its specific attributes. As depicted in Figure 1, the risk assessment framework consists of the following phases, i) context establishment, ii) risk identification, iii) risk estimation, and iv) risk evaluation, which we will next discuss in detail.

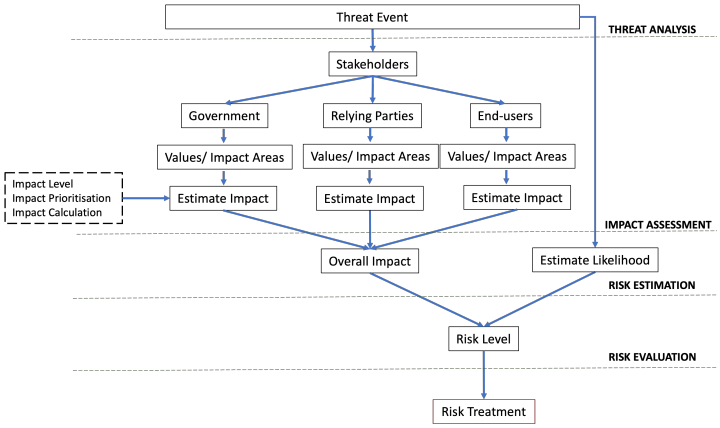

Figure 1: Workflow of the risk assessment framework

5.1 Context Establishment

In this phase, the scope and broad context of risk assessment are defined. By establishing a context for risk assessment, we can understand the external and internal factors that could affect the eID system's ability to achieve its mission, goals, and objectives. During this phase, the granularity levels of the eID system to be evaluated are defined. Basic risk measurement criteria are established as part of the context establishment process. Setting the basic criteria involves defining stakeholders' values, risk impact measurement, risk evaluation, and risk acceptance criteria. This phase sets the stage for the risk identification phase since defining the eID system objectives is a prerequisite for identifying risks.

5.2 Risk Identification

Risk identification in digital identity systems involves identifying and documenting the potential risks that may impact the identity system. This process helps to establish a clear understanding of which threats target which eID assets and what might happen if those attacks succeed [21, 37]. Several methods can be used to identify potential risks to eID systems. One popular technique is brainstorming, in which individuals with knowledge and expertise in digital identity systems generate a list of potential risks through open discussion and idea sharing [38]. Root cause analysis is another technique that involves identifying the underlying causes of potential eID risks and eliminating or mitigating these causes. This can be performed using tools such as 5-Whys [39] or fishbone diagrams [40]. Risks can also be identified through a scenario analysis by considering future events and the possible risks that may result from them. This can be conducted using tools like decision trees or Monte Carlo simulations [38].

5.3 Risk Estimation

Risk estimation in an eID system is the process of determining the impact and likelihood of a particular eID risk [8]. This consists of two fundamental processes: assessing risk impact and determining the likelihood of risk.

5.3.1 Estimate the risk impact

This process determines risk consequences. It involves three steps: identifying impact levels, prioritising impact areas, and calculating impact scores.

Impact level identification: Without a reference standard for comparison, comparing and aggregating risks across an eID system is impossible. Many frameworks [21, 37] rate impact on Likert scales, e.g. from "very low" to "very high". For example, the NIST guidelines [37] provide examples of adverse impacts, such as financial loss and harm to operations, assets, or individuals, and explain how the Likert scale should be used to determine the expected extent of each impact. The scales comprise rating levels and definitions that foster consistent interpretation and application by different users. We represent the impact areas identified in Section 4 by a three-point scale labelled "significant", "moderate", and "minor". A numeric impact value range can also be added to the scale point as follows: "Significant" – (70-100), "Moderate" – (31-69), and "Minor" – (0-30) for semi-quantitative analysis. These relative values may be amplified depending on the required granularity to visualise the risk metrics.

Risk impact areas prioritisation: In addition to evaluating the extent of an impact, there is a need to prioritise the impact areas from most important to least important based on their importance to the identity system operation and objectives. For example, an identity system developed for voter registration might prioritise citizens' rights over other impact areas. Risks that impact the citizen's rights will generate higher scores than risks with equivalent impacts and probabilities in another area. A quantitative weight can be assigned to each impact area where the most important is given the highest value, and the least is assigned the lowest value [21]. As part of context establishment, stakeholder requirements analysis can help in defining the ranking process and how the weights should be assigned.

Impact score calculation: The anticipated loss for stakeholders is estimated by the impact level of a particular risk. We define the impact of risk on any given eID system by the extent of the risk (impact value) and the impact area priority rank (quantitative weight) set by the user. This definition considers the contexts of use of the eID system and the differences in what stakeholders value. It can be mathematically expressed as follows:

$$\bar{i} = \sum_{n=1}^{n} w_n \cdot C_n \tag{1}$$

where C represents the impact value and w represents the quantitative weight of the impact area. For instance, expressing this equation using the impact areas identified in Section 4, the risk impact on relying private parties i_r can be represented with the following simple linear equation.

$$i_r = eo_r w_1 + op_r w_2 + ph_r w_3 + re_r w_4 + so_r w_5 \quad (2)$$

That is, using the impact area identified for the relying private parties, the risk impact score I_r is computed using the allocated impact value and weight for economic (eo), operational (op), physical (ph), reputation (re) and social (so) impact areas. w_1 to w_5 in the equation represents the quantitative weight value of the impact areas set by the "user".

The overall impact score I_{sum} for the risk on stakeholders can then be computed by aggregating the impact on government, relying private parties and end-users as follows.

$$I_{sum} = i_g + i_r + i_e \quad (3)$$

Where i is the computed impact value, the indices g, r, and e stand for the government, relying parties and end-users, respectively.

5.3.2 Estimate the likelihood

In this phase, the likelihood of the risk occurrence is assessed. Estimating the likelihood involves analysing the probability that a risk event will occur based on factors such as:

1. Vulnerability: How vulnerable the eID system is to the feared event based on its configuration, software, etc.
2. Threat actor capability: The expertise, knowledge about the target eID system, tools, and resources an attacker may have to exploit the vulnerability [37].
3. Motivation: The motive behind the attack, such as financial gain, political or ideological reasons, or revenge.
4. Historical data: Historical data that can provide insights into the likelihood of specific types of attacks [38].

We can rate the likelihood as "high", "medium", or "low". A "high" likelihood rating exists if the threat source is sufficiently capable and highly motivated, and the measures to guard against the vulnerability from being exploited are ineffective. If the threat source is competent and motivated and there are measures in place that could prevent the vulnerability from being exploited successfully, this is a "medium" rating. There is a "low" rating if sufficient controls are in place to prevent or at least hinder the exposure from being exploited or if the threat source lacks the capability to do so.

5.4 Risk Evaluation

Once risks have been identified and estimated, evaluating them in terms of their potential overall impact and likelihood is important. The combination of the likelihood and impact levels can be used to determine the risk level. The risk level allows us to recognise the risks that have the most significant impact on the eID system. The risk level can be rated as significant if there is a serious and urgent threat to eID systems (risk reduction remediation should be instantaneous), elevated if there is a real threat to eID systems (risk reduction remediation should be completed within a reasonable period), and low if threats are common and generally acceptable, but may still have an impact on eID systems. Additional security measures could offer greater protection against present or future unforeseeable threats. Table 2 depicts how each risk can be rated. For instance, if the risk rate score is above 50, the risk is of grave concern to the eID system. How the risk will be rated is usually based on the stakeholders' risk appetite. A high potential impact risk is often a great concern to decision makers, even if the likelihood is very low. Furthermore, frequent but low-impact risks can have long-term or cumulative consequences [38]. These types of risk require consideration, as appropriate risk treatments can differ. Nevertheless, identifying and implementing appropriate countermeasures is outside the scope of the current framework.

Table 2: Risk rating calculation

Impact (I)		**Likelihood** (L)		**Risk** ($I \times L$)	
Level	Score	Level	Score	Value Range	Description
Significant	70-100	High	1	51-100	Risk is of grave concern (significant)
Moderate	31-69	Moderate	0.5	21-50	Risk is of moderate concern (elevated)
Minor	0-30	Low	0.1	0-20	Risk is of low or no concern (low)

5.5 Use cases

To illustrate how risk impact assessment can be conducted using the aforementioned guidelines, we explore two examples.

1. Example 1: e-ID systems suffered a denial of service attack and went down for 2 minutes affecting 1% of the population. This resulted in negative social media, and about ten thousand people could not access the government services.
2. Example 2: an identity provider server configuration error results in a data breach where sensitive users' data are exposed to unauthorised parties. It violates users' privacy, causes negative social media, and causes financial loss to people and the government.

We calculated the impact of the risks and derived their risk values using the formula described above.

Impact level identification:: for the first example, the consequence indicates direct effects on the residents psychologically and socially. As illustrated in Table 3, the risk has little or no impact on the government and relying private parties, so a value of "minor" has been assigned to their impact areas. For example 2, there is a significant impact on the right, reputation, economy, society, and privacy (cf. Table 4).

Impact risk area prioritisation: considering our use cases, the impact areas have been prioritised as shown in Table 3. The stakeholders (except those relying on private parties) considered citizens' rights to be the most crucial impact area, and physical harm was the least important. These impact areas were assigned numerical weighted values between 1 and 7 for

the government, values between 1 and 6 for the end-users, and values between 1 and 5 for the relying private parties.

Impact score calculation: we compute the score for each impact area by multiplying the impact weight by the impact value assigned using the impact scales. We then compute the average impact scores I_g, I_r, and I_e, which represent the impact of risk on the government, relying on private parties, and end-users, respectively. For the first example, as shown in Table 3, we obtained the impact scores of *19* for the government, *32* for end users and 15 for the relying parties. Similarly, for Example 2 in Table 4, we have an impact score of *75* for the government, *79* for end-users, and 43 for the relying parties.

The overall impact score of the risk I_{sum} for the eID system can be computed by aggregating the risk impact scores from the government, relying parties and end-users. Using Equation 3, for Example 1 we have:

$$I_{sum} = (19 + 33 + 15)/3 = 22$$

For Example 2 we have:

$$I_{sum} = (75 + 79 + 43)/3 = 65$$

Determing the likelihood: for our examples, we assume that the likelihood of the risks occurring is high and that the threat source is sufficiently capable and highly motivated. Thus, a likelihood value of one was assigned to the risks.

Risk evaluation: As shown in Table 5, the relative impact score can be used with the risk likelihood to compute the risk rating, which can be used to prioritise the identified risks base on the stakeholders' risk appetite. For the DoS attack, we obtained a risk score of 22, representing an elevated risk level compared to the significant risk level of 65 obtained for the data breach attack that exposed the users' data.

Table 3: Impact measurement for example 1 (denial of service)

Government	**Description**	**Level**	**Value**	**Weight**	**Score**
Right	Minor impact on peoples right	Minor	25	7	175
Reputation	Limited impact on the ID agency	Minor	30	6	180
Political	Minor political impact	Minor	8	5	40
Economic	No economic loss.	Minor	10	4	40
Operational	Within their Service Level Agreement of 99.9% uptime.	Minor	10	3	30
Social	A minor impact on the society	Minor	30	2	60
Physical	No physical harm to government assets	Minor	8	1	8
			Total	**28**	**533**
			Impact Score		**19**
End-users	**Description**	**Level**	**Value**	**Weight**	**Score**
Right	Minor impact on peoples right	Minor	25	6	150
Privacy	No privacy violation	Minor	1	5	5
Psychological	Long-term inconvenience or distress	Significant	85	4	340
Economic	No economic loss	Minor	10	3	30
Social	Significant impact on the society	Significant	80	2	160
Physical	No physical harm to individuals	Minor	8	1	8
			Total	**21**	**693**
			Impact Score		**33**
Relying Parties	**Description**	**Level**	**Value**	**Weight**	**Score**
Economic	No Economic loss	Minor	10	5	50
Reputation	Limited impact on reputation	Minor	20	4	80
Operational	Minor impact on operation	Minor	10	3	30
Social	Minor impact on the society	Minor	25	2	50
Physical	Minor physical harm	Minor	8	1	8
			Total	**15**	**218**
			Impact Score		**15**

6 Discussion and Limitations

Impact focus measurement A key benefit of an impact focused risk assessment framework is that we do not need to rely on the knowledge of threats and attacks, which is necessarily incomplete. This is because the threat landscape is dynamic and it is impossible for anyone to be sure that they have complete knowledge [28]. Moreover, in an environment such as the eID system, where the threat landscape changes rapidly and novel attack patterns will continue to emerge, understanding the potential impact of the attacks on eID assets may help lessen the related uncertainty in risk management activities. .

Risk management strategies: Risk assessments alone do not necessarily reveal the appropriate mitigation strategies. Other factors such as legislation, regulations, strategy objectives, treatment options, and the likely effectiveness and side effects of various treatments also need to be considered [22]. Furthermore, identifying and managing eID risks and potential impacts require a broad set of perspectives and actors across the eID lifecycle. However, the government owns and manages the infrastructure of these systems and should be prepared to respond to risks by implementing appropriate risk-management strategies. These risk management strategies should be regularly reviewed and updated to effectively address changing threats and risks. This can involve conducting periodic risk assessments to identify new or emerging risks and reviewing and updating existing risk management strategies to ensure that they remain effective.

Varied risk perception: Lay people tend to rate higher risks related to dread (e.g., catastrophes) than domain experts, who understand the evidence regarding safety limitations and controls for such systems [41]. Moreover, people's assessment of risk is driven by their feelings and influenced by their concerns, as they naturally feel safe in their own area and are wary of danger outside of it [42]. This creates a mismatch between the perceived and actual risks, necessitating effective risk management through structured assessment methods. As the current eID system lacks a mature risk framework and practice, having a risk assessment framework could help users systematically assess eID system risks, ensuring that the limited resources can be targeted at the highest priority risks [43].

Limitations: One key limitation of this study is that it is based on elements previously described in the literature and has considered eID systems from a generic perspective. This may have resulted in significant issues being ignored or downplayed. Existing literature [44,45] recommended stakeholders' engagement to lessen the likelihood of such issues. As part of our future work, we aim to incorporate stakeholder opinions and empirically validate the framework to provide more spe-

Table 4: Impact measurement for example 2 (data breach)

Government	**Description**	**Level**	**Value**	**Weight**	**Score**
Right	Serious impact on peoples right	Significant	95	7	665
Reputation	National media attention.	Moderate	75	6	450
Political	Moderate political impact	Moderate	60	5	300
Economic	Significant economic impact	Significant	85	4	340
Operational	Moderate impact on ID agency operations.	Moderate	60	3	180
Social	Significant impact on the society	Significant	80	2	160
Physical	Minor physical harm to government assets	Minor	8	1	8
			Total	**28**	**2103**
			Impact Score		**75**
End-users	**Description**	**Level**	**Value**	**Weight**	**Score**
Right	Serious impact on peoples right	Significant	95	6	570
Privacy	Release of personal information to unauthorised parties	Significant	90	5	450
Psychological	Serious short-term discomfort, and distress	Moderate	58	4	232
Economic	Significant economic impact	Significant	82	3	246
Social	Significant impact on the society.	Significant	80	2	160
Physical	Minor physical harm to individuals	Minor	8	1	8
			Total	**21**	**1666**
			Impact Score		**79**
Relying Parties	**Description**	**Level**	**Value**	**Weight**	**Score**
Economic	Moderate economic impact	Moderate	45	5	225
Reputation	Limited impact on relying private parties' reputation.	Minor	20	4	80
Operational	Moderate impact on operations.	Moderate	65	3	195
Social	Moderate impact on the society	Moderate	71	2	142
Physical	Minor physical harm to assets	Minor	8	1	8
			Total	**15**	**650**
			Impact Score		**43**

cific insights and ensure that broader stakeholder concerns are considered. Lastly, risk assessments alone do not necessarily reveal appropriate mitigation strategies. In terms of future research, we hope to investigate how to identify and implement appropriate risk-mitigating strategies in eID systems.

7 Related Work

Research on Risk Assessments: There are many risk assessment frameworks and standards [36], with most emerging from public institutions, and government bodies [46].
The European Telecommunications Standards Institute (ETSI) [47] offers a threat, vulnerability, and risk assessment (TVRA) method to deal with security issues in the telecommunications industry. TVRA identifies threats to critical assets and how they can affect their operations. It also identifies the best way to mitigate these threats according to current capabilities and resource requirements. The work in [48] presented a framework for risk assessment within enterprise collaboration that identifies different levels of risk throughout the lifecycle of a collaborative enterprise, including pre-creation, creation, operation, and termination. The probability and impact of each risk are then determined using fuzzy linguistic terms.

Table 5: Example risk rank calculation

	Impact		**Likelihood**		**Risk**	
Example	Level	Score (I)	Level	Score (L)	Value (IxL)	Level
1	Minor	22	Moderate	1	22	Moderate
2	Moderate	65	High	1	65	Significant

The authors in [49] proposed a risk assessment framework for automotive embedded systems and demonstrated its viability in an industry-use case. The framework begins with a threat analysis to identify the assets and threats to those assets before estimating their threat level and impact. In another study, [50] presented a quantitative risk-assessment methodology for information technology outsourcing. The authors introduced four major steps for the method: (i) identifying the risks within the context of information technology outsourcing, (ii) collecting linguistic data about the likelihood and impact of risks from experts' opinions, (iii) multiplying the likelihood and impact of each risk, and (iv) making action plans to deal with it. However, despite the various existing risk assessment frameworks, the specific attributes of eID systems prevents the straightforward application of these risk assessment methods to eID systems. In addition, many of these frameworks focus primarily on general principles and guidelines, leaving users in need of more detailed implementation information [51].
Research on cyber impacts: Various attempts have been made to define the impact of cyberattacks on sociotechnical systems. For example, to understand how impact manifests within and outside of cyberspace, Agrafiotis et al. [28] proposed five different taxonomy of cyber harms, namely: i) physical or digital, ii) social and societal, iii) economic, iv) reputation and v) psychological. The authors also presented an initial set of metrics and methods to assess cyber harm in national contexts. Similarly, the authors in [52] identifies five impact areas that surround e-government projects: i) economic, ii) political, iii) security, iv) societal, and v) technical risk impact areas. In addition, the researchers in [49] identified four impact areas for risk assessment in automotive embedded systems: safety, privacy and legislative, financial, and operational. Even with the considerable research on cyber harm, no previous study has investigated the key impact areas to consider when evaluating the impact of risk on stakeholders of eID systems.

8 Conclusion

eID systems are crucial for achieving political, economic, and human development goals. They provide citizens with a means to prove their identity and gain access to services, thereby sup-

porting the reduction of societal inequality. In this study, we posit that current risk assessments do not address risk factors for all key stakeholders, we explore this and analyse how potential compromise could impact them each in turn. In examination of the broader impact of risks and the potentially significant consequences for individuals, communities, and societies our framework considers a wide range of factors. Social, economic, and political contexts in which these systems were implemented are addressed and together provide a holistic platform on which to better assess the risk to eID system.

9 Acknowledgments

This work was supported, by the Bill & Melinda Gates Foundation [INV-001309]. Under the grant conditions of the Foundation, a Creative Commons Attribution 4.0 Generic License has already been assigned to the Author Accepted Manuscript version that might arise from any submission.

References

[1] Atick, J.. 'Digital identity: the essential guide', 2018. [Online; last accessed 3-December-2022]

[2] FATF. 'Guidance on digital id', 2020. [Online; last accessed 31-May-2022]. https://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html

[3] Rodríguez, D., Busco, C., Flores, R.: 'Information technology within society's evolution', *Technology in Society*, 2015, **40**, pp.64–72. technological Futures

[4] Pratyush, R.T., Dhruv, A., Prakhar, J., Swagam, D., Preetha, D., Vineet, R., et al.. 'India's aadhaar biometric id: Structure, security, and vulnerabilities', 2022. https://fc22.ifca.ai/preproceedings/137.pdf

[5] UIDAI. 'What is aadhaar', 2019. [Online; last accessed 31-July-2022]. https://uidai.gov.in/en/

[6] ID4D. 'Assess risks', 2018. [last accessed 17-May-2023]. https://id4d.worldbank.org/guide/assess-risks

[7] Garfinkel, S. 'Implementing differential privacy for the 2020 census'. USENIX Association, 2021.

[8] Renn, O.: 'Risk governance'. 1st ed. Earthscan, 2008

[9] Horlick.Jones, T.: 'Meaning and contextualisation in risk assessment', *Reliability Engineering & System Safety*, 1998, **59**, (1), pp.79–89

[10] Marsman, H.: 'Is the capabilities approach operationalizable to analyse the impact of digital identity on human lives', *Data and Policy*, 2022, **4**, pp.e43

[11] Kubicek, H., Noack, T.: 'The path dependency of national electronic identities', *Identity in the Information Society*, 2010, **3**

[12] Brugger, J., Fraefel, M., Riedl, R. 'Raising acceptance of cross-border eid federation by value alignment'. vol. 12. ACPIL, 2014.

[13] Pappas, l., Patrick, M., Yogesh.K., D., Letizia, J., John, K., Matti, M., editors. 'Digital Transformation for a Sustainable Society in the 21st Century'. 1st ed. Springer Cham, 2019

[14] Mir, U., Kar, A., Gupta, M.: 'Ai-enabled digital identity – inputs for stakeholders and policymakers', , 2022, **13**, (3), pp.514–541

[15] OECD.: 'Digital opportunities for better agricultural policies'. OECD, 2019

[16] Mahase, E.: 'Covid-19: Government's failure to share data and face scrutiny have undermined response, say mps', *BMJ*, 2021, **372**. Available from: https://www.bmj.com/content/372/bmj.n717

[17] Guardian. 'Us government hack stole fingerprints of 5.6 million federal employees', 2015. Available from: https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints

[18] Clark, J.M. 'Public sector savings and revenue from identification systems : Opportunities and constraints', 2018.

[19] OWASP. 'Owasp risk rating', 2022. https://owasp.org/www-community/OWASP_Risk_Rating_Methodology, accessed 7 November 2022

[20] ID4D. 'Practitioner's guide: Stakeholders and roles', 2018. [Online; last accessed 17-July-2022]. https://id4d.worldbank.org/guide/stakeholders-and-roles

[21] Caralli, R., Stevens, J., Young, L., Wilson, W.. 'Introducing octave allegro: Improving the information security risk assessment process'. Pittsburgh, PA, 2007. Available from: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419

[22] Peltier, T.: 'Information Security Risk Analysis'. 1st ed. New York: Auerbach Publications, 2001

[23] Cresswell, A., Pardo, T., Burke, G., Dadayan, L. 'Advancing return on investment analysis for government information technology'. In: The Proceedings of the 8th Annual International Digital Government Research Conference, 2006. pp. 244–245

[24] Foley, K.M. 'Using the value measuring method to evaluate government initiatives', 2006.

[25] Halperin, R., Backhouse, J.: 'Risk, trust and eid: Exploring public perceptions of digital identity systems', *First Monday*, 2012, **17**

[26] Sule, M.J., Zennaro, M., Thomas, G.: 'Cybersecurity through the lens of digital identity and data protection: Issues and trends', *Technology in Society*, 2021, **67**

[27] Huffpost. 'Fraudulent unemployment benefits payments totaled $3.3 billion in 2011: Paper', 2013. Available from: https://www.huffpost.com/entry/fraudulent-unemployment-benefits_n_3175092

[28] Agrafiotis, I., Nurse, J.R.C., Goldsmith, M.e.a.: 'A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate', *Journal of Cybersecurity*, 2018, **4**, (1). Available from: https://doi.org/10.1093/cybsec/tyy006

[29] Samuel, M., Doctor, G., Christian, P., Baradi, M.: 'Drivers and barriers to e-government adoption in indian cities', *Journal of Urban Management*, 2020, **9**, (4), pp.408–417

[30] Lother, A.K.: 'Principles on identification for sustainable development– relevance and best practices in central asia', , 2022, [Online; last accessed 29-November-2021]

[31] Raus, M., Liu, J., Kipp, A.: 'Evaluating it innovations in a business-to-government context: A framework and its applications', *Government Information Quarterly*, 2010, **27**, (2), pp.122–133

[32] Harrell, E.. 'Victims of identity theft, 2016', 2016. [Online; last accessed 17-November-2022]. https://bjs.ojp.gov/content/pub/pdf/vit16.pdf

[33] Bhatia, A., Donger, E., Bhabha, J.: 'Without an aadhaar card nothing could be done', *Information Technology for Development*, 2021, **27**, (1), pp.129–149. Available from: https://doi.org/10.1080/02681102.2020.1840325

[34] Singh, R., Jackson, S.: 'Seeing like an infrastructure: Low-resolution citizens and the aadhaar identification project', , 2021, **5**, (CSCW2). Available from: https://doi.org/10.1145/3476056

[35] Fussell, J.. 'Indangamuntu 1994: Ten years ago in rwanda this identity card cost a woman her life'. Prevent Genocide International, 2016. [Online; last accessed 17-November-2022]. http://www.preventgenocide.org/edu/pastgenocides/rwanda/indangamuntu.htm

[36] ENISA. 'Risk management: Implementation principles and inventories for risk management/risk assessment methods and tools', 2006. [Online; last accessed 27-October-2022]. https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools

[37] NIST. 'National institute of standards and technology (nist): Guide for conducting risk assessments.', 2012. [Online; last accessed 17-October-2022]. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[38] ISO. 'Risk management — principles and guidelines.', 2018. [Online; last accessed 17-February-2022]. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

[39] Murugaiah, U., Benjamin, S.J., Marathamuthu, M.S., Muthaiyah, S.: 'Scrap loss reduction using the 5-whys analysis', *International Journal of Quality & Reliability Management*, 2010, **27**, (5), pp.527–540

[40] Luo, T., Wu, C., Duan, L.: 'Fishbone diagram and risk matrix analysis method and its application in safety assessment of natural gas spherical tank', *Journal of Cleaner Production*, 2018, **174**, pp.296–304

[41] Slovic, P.: 'Perception of risk', *Science*, 1987, **236**, (4799), pp.280–285. Available from: https://www.science.org/doi/abs/10.1126/science.3563507

[42] Schneier, B.: 'Beyond fear'. 2nd ed. Springer, 2006

[43] Henrie, M.: 'Cyber security risk management in the scada critical infrastructure environment', *Engineering Management Journal*, 2013, **25**, (2), pp.38–45. Available from: https://doi.org/10.1080/10429247.2013.11431973

[44] Parry.Jones, A., Hansen, J., Simeon.Dubach, D., Bjugn, R.: 'Crisis management for biobanks', *Biopreservation and Biobanking*, 2017, **15**, (3), pp.253–263

[45] Renn, O., Schweizer, P.J.: 'Inclusive risk governance: concepts and application to environmental policy making', *Environmental Policy and Governance*, 2009, **19**, (3), pp.174–185

[46] Al.Ahmad, W., Mohammad, B. 'Addressing information security risks by adopting standards'. In: International Journal of Information Security Science. vol. 2. Şeref SAĞIROĞLU, 2013. pp. 28–34

[47] ETSI. 'Cyber; methods and protocols; part 1: Method and pro forma for threat, vulnerability, risk analysis (tvra)', 2017. [Online; last accessed 27-October-2022]. https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf

[48] Wulan, M., Petrovic, D.: 'A fuzzy logic based system for risk analysis and evaluation within enterprise collaborations', *Computers in Industry*, 2012, **63**, (8), pp.739–748. special Issue on Sustainable Interoperability: The Future of Internet Based Industrial Enterprises

[49] Islam, M.M., Lautenbach, A., Sandberg, C., Olovsson, T. 'A risk assessment framework for automotive embedded systems'. In: Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security. CPSS '16. New York, NY, USA: Association for Computing Machinery, 2016. p. 3–14. Available from: https://doi.org/10.1145/2899015.2899018

[50] Samantra, C., Datta, S., Mahapatra, S.S.: 'Risk assessment in it outsourcing using fuzzy decision-making approach: An indian perspective', *Expert Systems with Applications*, 2014, **41**, (8), pp.4010–4022

[51] Sendi, A.S., Jabbarifar, M., Shajari, M., Dagenais, M. 'Femra: Fuzzy expert model for risk assessment'. In: 2010 Fifth International Conference on Internet Monitoring and Protection, 2010. pp. 48–53

[52] Evangelidis, A. 'Frames – a risk assessment framework for e-services', 2004.