Trust in Practice: Evaluating Third-Party Software in Large Organisational Procurement

Hannah Lear[1], Majdouline Hamdi[1], Kim van Leussen[1], Aminul Didar Islam[1,2], and Slinger Jansen[1,2]

[1] Utrecht University, Heidelberglaan 8, 3584 CS Utrecht, The Netherlands
[2] LUT University, Yliopistonkatu 34, 53850 Lappeenranta, Finland

Abstract. As large organisations increasingly rely on third-party software to support core operations, trust has emerged as a critical factor. This study reports how trust-related considerations influence the procurement and evaluation of third-party software in large enterprises. Drawing from the literature and nine semi-structured interviews, this study identified specific trust factors, such as certifications, regulatory obligations, and vendor transparency. The findings offer practical insights for improving procurement and evaluation strategies, contribute novel understanding of the trust dimensions specific to software procurement and risk assessment, and provide software vendors with insights on how to make their software more trustworthy.

Keywords: Trust · Third-party software · Procurement · Compliance management · Organisational cybersecurity.

1 Introduction

Software procurement is the structured process through which organizations select, evaluate, acquire, and maintain third-party software tools and services that support their operations. It has become a strategic activity in modern software ecosystems, where interdependencies between vendors, platforms, and users shape both economic and security outcomes [14]. Procurement decisions increasingly determine not only cost efficiency but also the resilience, compliance, and long-term viability of digital infrastructures.

In practice, software procurement combines formal procedures and informal decision-making. While structured frameworks and tender processes are well documented in procurement research [15, 22], studies consistently show that organizations often adapt or even bypass formal models to align with internal culture, urgency, and perceived risks [2, 3]. This tension between prescriptive procurement models and situated practices highlights a persistent gap between how organizations are advised to procure and how they actually make software decisions.

The growing complexity of software and business ecosystems amplifies the stakes of these choices. Interconnected systems, multi-layered dependencies, and cloud-based architectures mean that a single compromised vendor may trigger cascading failures across an organization. High-profile supply chain incidents such as SolarWinds have demonstrated how vulnerabilities in trusted suppliers can escalate into systemic risks [8, 23]. Moreover, compliance with regulatory frameworks such as the GDPR and the NIS2 Directive now forms a central determinant in vendor selection, alongside concerns about data sovereignty and geopolitical exposure [5, 20].

In this landscape, trust becomes a central decision determinant. Trust in software procurement refers to the willingness of organizational actors to accept risk based on confidence in a vendor's reliability, competence, and integrity [12]. However, empirical evidence about how such trust is evaluated and maintained across the procurement lifecycle remains limited. While multiple trust models exist in the broader software ecosystem literature [11, 16], little is known about how large organizations operationalize these models when assessing third-party software suppliers or how they re-evaluate trust after procurement.

This study focuses on trust in third-party software procurement across product software, SaaS, and infrastructure contexts. It examines which trust mechanisms organizations apply, how these interact with formal procurement procedures, and how trust evolves over time. While prior studies on outsourcing and supplier relationship management provide valuable insights [6, 9], software procurement differs by its technical opacity, frequent updates, and layered dependencies. Addressing this gap, we explore how procurement teams integrate trust factors such as certifications, compliance audits, and transparency into their decision-making, leading to the following research question: *"What is the process of identifying and evaluating trust factors in procurement processes for third-party software products within large organizations?"*

The paper contributes by (1) mapping how trust considerations are embedded in real-world procurement processes, (2) proposing a conceptual model of trust mechanisms across procurement phases, and (3) extending theoretical understanding of trust beyond outsourcing to the domain of digital software acquisition. The remainder of this paper is structured as follows. Section 2 provides background on trust in software ecosystems and procurement, highlighting the limitations of existing frameworks and introducing the concept of trust factors, such as certifications, performance, and transparency. Section 3 describes the research method, including the selection criteria for participants, the interview protocol, and the thematic coding approach used to analyse the data. Section 4 presents the results of the study, organised into key dimensions of procurement practice: the structure and flexibility of procurement processes, the roles and interactions of stakeholders, the trust mechanisms used across procurement phases, and the evaluation of risk categories. This section also includes a model that synthesizes how trust is operationalised in procurement organizations (see Figure 2). Section 5 discusses the implications of these findings, comparing them to existing procurement models, and reflecting on challenges such as shadow IT and procurement under legal uncertainty. It also offers practical recommendations for improving procurement strategies. Section 6 concludes by summarising the main findings on trust in software procurement.

2 Background

Procurement research traditionally conceptualizes software acquisition as a multistage decision process involving need identification, vendor evaluation, negotiation, and post-contract management [15, 22]. In public and private sectors alike, structured approaches such as the six-stage ERP model [22] provide governance and accountability but are frequently adapted to accommodate contextual pressures such as innovation speed or departmental autonomy [3]. Recent studies have emphasized hybrid or agile procurement strategies that balance compliance with flexibility [5, 20].

Within this process, trust serves as a mechanism to mitigate uncertainty about vendor reliability, data protection, and long-term performance. Trust factors include technical indicators (e.g., security certifications), institutional assurances (e.g., regulatory compliance), and relational dimensions such as transparency and prior collaboration. In complex software ecosystems, these factors collectively shape procurement outcomes by influencing perceived vendor credibility and risk tolerance [6, 11].

Security and compliance certifications, such as ISO/IEC 27001 or SOC 2, often function as baseline trust signals, ensuring that vendors meet minimum legal and technical standards [13]. However, scholars caution against equating certification with genuine trustworthiness, since certificates reflect only a momentary compliance status [12]. Empirical work shows that high-reliability organizations complement formal audits with continuous monitoring, reputation assessments, and transparent reporting mechanisms [19].

From a relational perspective, procurement success depends on interpersonal and organizational trust. Factors such as responsiveness, prior experience, and openness in communication help sustain trust beyond the initial contract [6]. Moreover, evidence from outsourcing and supplier management literature suggests that trust and control coexist rather than substitute each other, jointly shaping risk perception and collaboration quality [18].

Despite the existence of mature procurement models, there remains limited empirical understanding of how large organizations operationalize trust in the acquisition of third-party software. Most existing studies focus on either technical evaluation or contractual governance, while the integration of trust as an evolving construct across the procurement lifecycle remains underexplored. This study addresses that gap by examining how organizations combine formal mechanisms (certifications, contracts, SLAs) and relational mechanisms (transparency, reputation, responsiveness) to manage risk and sustain trust over time.

3 Research Method

A qualitative research method was applied in this study to enable an in-depth investigation of organisational perspectives on software procurement and trust. Third-party software tools are often embedded within complex IT environments, requiring procurement teams to carefully evaluate trust-related factors. To explore these practices, multiple interviews were conducted with members of such teams to gain practical insights into how trust is assessed and managed. Participants were recruited through desk research, using publicly available contact information, and through outreach on platforms such as LinkedIn. To ensure consistency across respondents, the researchers applied the following selection criteria:

1. The company needs to be large and have a minimum of 250 employees[3].
2. The company has to make use of one or multiple third-party software.
3. The company needs to have both procurement departments and internal risk assessment teams.

After approaching 47 large organizations, nine participants were gathered. To achieve diversity, the roles included professions such as IT managers, risk assessors, and professors. With the nine participants, semi-structured interviews were conducted that lasted between 30 and 60 minutes, with the option of either in person or online, based on the participant's preference. To minimise interviewer bias, two researchers were present during these interviews. Beforehand, permission was requested to record the interview so that all relevant information could be analysed afterwards. The questions that were asked during the interviews were predetermined and put in an interview guide so that consistency among the different researchers was ensured, of which a preview is given in Table 1.

Table 1: A sample of the questions asked during the interviews. The full interview protocol is posted here: Interview Protocol.

Theme	**Key Question**
Trust Requirements	What trust-related requirements are typically checked before approving a third-party software vendor (e.g., certifications, audit results, reputation)?
Regulatory Compliance	Are there standard compliance checks or regulatory obligations that third-party vendors must meet (e.g., GDPR, ISO, etc.)?
Ongoing Evaluation	Do you re-evaluate the trustworthiness of third-party vendors periodically? If yes, how often and through which mechanisms?
Risk vs. Functionality	How do you balance risk and functionality when a tool is highly useful but has questionable trust signals?

The interview guide was divided into three sections: opening questions, which addressed the participants' role and involvement in procurement; main questions, which focused on trust-related evaluation practices; and concluding prompts, which invited participants to share any additional insights. The main section

[3] A threshold of 250 employees is commonly used in the literature to classify an organisation as *large* [7].

drew on themes identified in the literature review, including certifications, compliance, and risk assessment, to ensure alignment between theoretical frameworks and real-world practices. Primarily, the study of Hou et al. [11] was used to deductively inspire the interview protocol.

Data Analysis Process. To analyse the interview data, the researchers first transcribed the recordings. The coding process followed a pragmatic, theory-informed approach. Trust-related guidelines identified in prior literature [11] served as a deductive framework for initial code construction, ensuring conceptual alignment with existing models of trust in software ecosystems. During analysis, semi-open coding was applied to capture additional factors that emerged inductively from the interviews, following the adaptive logic of thematic analysis [4]. This combination of deductive and inductive coding reflects a pragmatic stance toward qualitative inquiry [17], ensuring that both established and context-specific trust mechanisms were systematically represented in the findings. Additional codes were included if they were mentioned by more than three respondents. Two examples of the coding process are provided in Table 2.

Table 2: Examples of the semi-open coding process.

Guideline	**Nvivo code**	**Interview segment**
Security & compliance certifications	Certification	Respondent 5: *"Um, right now I think we work with, um, ISO 27001, ISO 27001, and also, um, another one, which I don't know from my head, but um, we work with two certificates, if that helps"*
Performance & reliability	Past performance	Respondent 9: *"And the CISO knows when some suppliers don't have a good reputation about the security if there have been security incidents in the past. She will know that. And then she will say such as, okay, this is not not just an application we have to go for"*

To ensure coding consistency and intercoder reliability, the researchers reviewed each other's work. Moreover, the program, NVivo, was used as it easily views the overall coverage of the nodes that were set up. In the end, this resulted in multiple codes surrounding trust factors mentioned by different participants and their perspective towards the selection process and the associated requirements. By analysing these codes, the following themes were found: 1) Software procurement process, 2) Trust mechanisms, 3) Monitoring trust, and 4) Risk perception and evaluation. This enabled conclusions about the role of trust factors during the procurement of third-party software products.

Reliability, Validity, and Limitations. Participant selection may vary across different researchers due to the availability of respondents. However, this limitation was reduced by applying clear selection criteria, which helped maintain consistency if another researcher were to replicate the study. To ensure internal validity, the study used a consistent interview protocol[4] and conducted thematic coding using NVivo software. While the trust factors found in the literature were used as a guideline, other factors could also emerge. To address this, the study applied a semi-open coding process to capture additional relevant factors identified by participants, enhancing the validity of the findings. It is, however, acknowledged that the results may not be generalisable to countries with different legal frameworks, market conditions, or cultural attitudes toward risk, thereby limiting external validity.

Ethical issues were carefully considered throughout both the data collection and analysis processes. Participants were explicitly asked for permission to record their interviews, with clear assurances that their responses would remain anonymised and used only for educational purposes related to Utrecht University. Recordings were permanently deleted after the analysis phase, ensuring that participants' privacy was fully protected.

Finally, this study is limited in scope and generalisability. All participants were based in Dutch organisations, which may not fully represent procurement practices elsewhere. While organisations from multiple sectors were included, their internal processes vary. Moreover, three interviews originated from a single organisation, albeit from individuals holding different roles.

4 Results: Software Procurement Process Dimensions

This section presents the findings from nine semi-structured interviews, structured around three key dimensions of procurement practice observed across the participating organisations. First, it examines the varying configurations of procurement processes, including differences in procedural structure, decision-making logic, and stakeholder engagement. Second, it analyses the trust-related requirements embedded within procurement activities, encompassing regulatory compliance, technical standards, and institutional risk classifications. Third, it investigates the mechanisms through which trust is monitored and reassessed over time, with attention to performance tracking, contractual enforcement, and supplier accountability, each of which contributes to sustaining reliable vendor relationships.

Software Procurement Process: Formal and Flexible. A formal procurement process was common among our respondents. Typically, the companies initially had a request for a particular software or identified a need for software. They would then hold a structured tender or structured intake, followed by the risk and privacy checks, before signing a contract or tender agreement. This layout is visualised in Table 3.

R.9 described the process beginning with an "*assignment to attract a new kind of software*", typically due to dissatisfaction with the existing solution (Stage 1 of Table 3). This initiates the formation of a multidisciplinary team (Stage 2),

[4] A link to the protocol is found here: https://zenodo.org/records/17338732

composed of representatives from various departments depending on the software needs. The team proceeds to define specific requirements and formulate a request for proposal (RFP), incorporating legal, functional, and security-related questions (Stages 3 and 4). Vendors responding to the RFP are evaluated based on multiple criteria such as security, privacy, architecture, corporate social responsibility (CSR), and references (Stage 5). Shortlisted vendors are invited to a demonstration session (Stage 7), in which they will also be scored based on their performance, after which, the final selection would be made and a contract signed (Stages 8–9).

Table 3: Stages in the Procurement Process Observed in Practice. Please note that the rows in which formal trust dominates are blue, whereas the rows in which relational trust dominates are light green. These colors are similar to the ones in Fig. 1, as are the four phases.

No.	**Stage**	**Description**
Pre-contracting phase		
1	Need Identified	Triggered by user demand, dissatisfaction, or contract expiration
2	Team Formed	Multidisciplinary team including procurement, IT, privacy, and business users
3	Define Requirements	Legal (GDPR), security (ISO), data hosting, and data processing agreements
4	Send RFP	Use of templates with audit rights, certification checks, and functional needs
5	Vendor Response & Scoring	Evaluation of answers, certifications, documentation, and references
6	Shortlist Vendors	Selection of top candidates based on predefined scoring criteria
7	Demo & Deep Dive	Vendor presentations and detailed Q&A with domain experts and CISOs
8	Final Evaluation	Risk, legal, trust, and compliance assessment before approval
Contracting phase		
9	Contract Signed	Contractual agreement including (Data Processing Agreement) DPA, (Service-level Agreement) SLA, and legal clauses
Monitoring phase		
10	Implementation	Technical deployment and internal onboarding
11	Monitoring	Periodic review of certifications, SLAs, and performance incidents
Evaluation phase		
12	Re-evaluation or Renewal	Triggered at contract end or due to performance/risk concerns

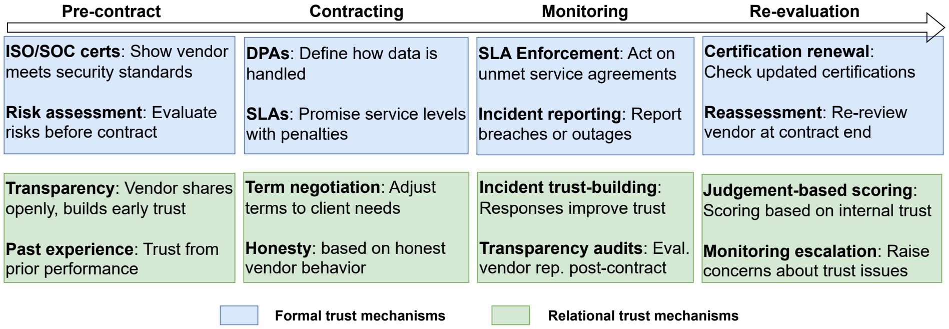
Some organisations applied a more flexible procurement approach depending on the scope of product use. *R.5*, for example, noted that if a tool was intended for a single department, the process was relatively simple. In contrast, broader or more costly requests involving multiple departments trigger a more formal procedure: "*If it's a big request for something that is for more [departments]* *and more users, and maybe also a bit expensive, then I will discuss it [with a procurement officer]... and we will see several things - technical specifics, procurement measures."*

Similarly, there were variations in the procurement process based on the sensitivity of the software and the data it would process. For example, *R.3* explained that "*if the classification [of risk] is very high, [they] need to take a lot of measures, and the supplier needs to take a lot of measures*," and *R.6* mentioned, "*if they don't [have ISO], we make [sic] a risk assessment if it's necessary, and we can still do business with them."* This necessity to continue business was a common theme among respondents, with many noting that a lack of alternatives often meant they had to compromise on certain aspects of their procurement checklist (see Appendix B for more). A preference often mentioned was that servers should be European Union-based, but due to the lack of alternatives, many companies had to continue working with large companies such as Microsoft or Google, whose servers are located in the United States. Had an alternative solution with EU-based servers and the necessary security measures been available, it would have been the preferred option, particularly given that several respondents cited increasing political uncertainty as a concern.

Key Stakeholders and Roles. Software procurement involves multiple stakeholders with varying roles and interpretations, often leading to coordination challenges. *R.9* described aligning strategic and maintenance IT, contract managers, and business users, with the strategic IT department advising the board when needed: *"Maybe we should reconsider this supplier..."*. While no major conflicts between procurement and risk teams were reported, differences in language, templates, and structural setups were common. For instance, *R.7* noted departmental variation in interpreting risk documentation.

Across all organisations, the Chief Information Security Officer (CISO) played a central role in defining trust policies, reviewing certifications, and escalating risks. Procurement teams tracked vendor performance and enforced contract terms; legal departments ensured compliance through managing DPAs and SLAs; and IT teams handled technical assessments such as encryption and access control. Procurement structures varied: some followed decentralised but coordinated models, others maintained central oversight with distributed execution. Overall, trust maintenance was a shared responsibility, shaped by institutional structure and the clarity of interdepartmental collaboration.

Trust Mechanisms in Procurement. Organisations use a layered trust strategy, combining formal mechanisms (classification model based on confidentiality, integrity, and availability (CIA) model, certifications, legal documents) and relational mechanisms (for example past experience, transparency, risk dialogue). These mechanisms are applied at different stages of the procurement lifecycle. Figure 1 shows a timeline in which it is seen how trust mechanisms evolve during a vendor relationship. This timeline demonstrates that while formal mechanisms dominate early stages, relational and experience-based mechanisms also play a role during ongoing collaboration and contract renewal. The following section will dive deeper into each of these mechanisms.



Pre-contract	Contracting	Monitoring	Re-evaluation
ISO/SOC certs: Show vendor meets security standards **Risk assessment**: Evaluate risks before contract	**DPAs**: Define how data is handled **SLAs**: Promise service levels with penalties	**SLA Enforcement**: Act on unmet service agreements **Incident reporting**: Report breaches or outages	**Certification renewal**: Check updated certifications **Reassessment**: Re-review vendor at contract end
Transparency: Vendor shares openly, builds early trust **Past experience**: Trust from prior performance	**Term negotiation**: Adjust terms to client needs **Honesty**: based on honest vendor behavior	**Incident trust-building**: Responses improve trust **Transparency audits**: Eval. vendor rep. post-contract	**Judgement-based scoring**: Scoring based on internal trust **Monitoring escalation**: Raise concerns about trust issues

Fig. 1: Trust mechanisms across procurement phases.

Formal Mechanisms. Most respondents, including *R.6*, explained that ISO 27001 certification is required for vendors whose services touch the organisation's IT infrastructure. Other organisations also mentioned ISO 27002 certification and SOC 2 & 3. If a vendor does not have this certification, often the case with small, innovative startups, a risk assessment is performed to decide whether collaboration is still possible. All respondents required GDPR compliance, supplemented by sector-specific frameworks such as SURF agreements in academia, BIO for government, and NEN 7510 for healthcare; sub-processors were explicitly checked for compliance and data residency.

Few organizations check whether the certification is in fact valid. As *R.3* noted: *"You still need to look into it to see, 'Okay, what did you test? When was the certification? Because if it's ten years old, 'yeah, thanks', but we need something that's a little bit newer."* Some organisations implemented internal frameworks that go beyond certification requirements, highlighting recognition that formal trust mechanisms alone do not guarantee reliability. In such cases, certifications function more as entry criteria than full assessments. Respondents also highlighted the need for formal legal instruments such as DPAs, especially when personal data is involved and SLAs that hold post-contract obligations such as incident reporting.

Relational mechanisms. A recurring theme was transparency; vendors who fail to clearly explain their processes or avoid answering detailed questions raise red flags early in the procurement process. *R.3* explained: *"If they're not transparent about how they work... more questions pop up."* Trust was also shaped by transparency about past performance, with *R.8* even increasing trust in a vendor after a ransomware attack, interpreting their improved protocols as a sign of maturity. *R.9* implemented a quantified trust score, based on responses to structured questionnaires, while *R.8* rejected such models in favour of case-by-case judgment. This variation illustrates the coexistence of formalised and subjective approaches, depending on the organisation's culture and capacity. Table 5 summarises all the different trust mechanisms.

Table 4: Expanded list of trust mechanisms across procurement phases.

	Mechanism	**Phase**	**Notes**
Formal	ISO / SOC certifications	Pre-contract	Baseline security qualification
	Risk assessment reports	Pre-contract	Alternative for small/startup vendors
	Data Processing Agreement	Contracting	When handling personal data
	SLA clauses	Contracting	Includes penalties and service levels
	SLA enforcement	Monitoring	Used when SLA breaches occur
	Incident reporting	Monitoring	Obligatory in case of breaches
	Certification renewal check	Re-evaluation	Ensures certifications stay current
	Formal reassessment	Re-evaluation	Periodic review before contract renewal
Relational	Transparency in communication	All phases	Lack of openness is a red flag
	Past experience with vendor	All phases	Especially relevant for renewals
	Term negotiation flexibility	Contracting	Adjusting terms to organisational needs
	Honesty / trust signals	Pre-contract	First impressions
	Incident trust-building	Monitoring	Vendor response builds trust
	Transparency audits	Monitoring	Reviewing vendor openness
	Judgement-based trust scoring	Selection	Subjective scoring in absence of metrics
	Monitoring escalation	Re-evaluation	Internal escalation when trust drops

Monitoring trust. Organisations do not rely on a single, static assessment of trust but instead monitor it throughout the vendor relationship. Most respondents mentioned a periodic re-evaluation of industry certifications, especially when certificates expire and need to be renewed. *R.6* explained that certifications are reassessed as part of a broader technical and legal verification process. In other cases, such as with *R.3*, vendors who initially lacked the required certifications were allowed to proceed under the condition that improvements would be made within a set time frame.

R.7 described monitoring through contractual obligations, including SLAs and incident reporting duties. Vendors were required to share system logs and relevant information when incidents occurred, so the organisation could inform authorities and evaluate the impact. If expectations were not met or incidents were poorly handled, the issue escalated internally. *R.2* acknowledged that communication was sometimes lacking because IT and procurement were not always informed about software acquisitions. As they admitted, *"I have no idea what everyone is purchasing"*, and often only learnt about tools after the fact.

Risk Perception and Evaluation. The interviews revealed several categories of trust-related risks in third-party software procurement, which can be broadly grouped into technical, relational, and legal/compliance concerns. While these categories often overlap, distinguishing them provides a clearer view of how organisations assess and respond to risk.

Technical trust concerns. The most frequently mentioned technical risk was the threat of data breaches. *R.9* identified hacking as the most concerning issue due to its potential to compromise sensitive client information. Although most respondents had not personally experienced breaches, *R.8* described a case where a third-party vendor failed to delete data after the contract end date. The data remained on an outdated server, which was later hacked, leading to the theft of alumni information. This experience led the respondent to place greater emphasis on secure data deletion.

Relational and operational concerns. Several respondents described trust issues stemming from supplier behaviour and internal organisational limitations. *R.7* reported that some vendors impose unusual conditions, such as requiring non-disclosure agreements (NDAs) to access essential security documentation such as SOC 2 reports. *R.2* noted instances where suppliers promised one thing but delivered another, though they clarified that these discrepancies had not yet led to concrete security issues. These tensions highlight the challenge of maintaining clear expectations and oversight in supplier relationships.

Trust issues also arose from internal decentralisation. *R.2* explained that individual departments sometimes procured software without involving IT or procurement, which meant the organisation lacked visibility and contractual control over these tools. To address this, they advocated for centralising procurement oversight. Similarly, *R.7* stated that due to the organisation's size, it was difficult to conduct risk assessments for every supplier, which sometimes led to ambiguity about when a certification or formal evaluation was necessary.

Legal and compliance concerns. A third major category of risk is related to compliance and jurisdictional uncertainty, especially around U.S.-based cloud providers. All educational institutions interviewed expressed concern over reliance on dominant suppliers such as Microsoft and Google due to the implications of the U.S. CLOUD Act[5]. *Respondents 4* and *6* stressed the importance of knowing where data is stored and whether customers retain control. While these vendors were sometimes approved, the process involved penetration testing and a case-by-case risk evaluation.

R.8 described the legal complexities of cross-border data transfers, stating: *"We ask the supplier who will be transporting the data for us to the third country to tell us how the legal protection mechanism in that other country is organised. Yeah, that is very complicated."* As the GDPR does not apply outside the EU, working with U.S. suppliers increases legal uncertainty. *R.4* echoed this concern, stating: *"The US has been proven to be not such a reliable partner as it used to be. So there is [a] big uncertainty, but we are very much depending on you know, stuff such as Microsoft, Google, Amazon, and they store their data wherever they want to."* These accounts reflect how legal and political factors can limit procurement choices, even when risks are well understood.

Managing risk through evaluation and monitoring. Given the range of risks, respondents emphasised the importance of ongoing evaluation and monitoring. *R.3* described a tiered approach where high-risk vendors were reviewed more frequently-monthly, quarterly, or annually, depending on risk level. In contrast, *respondents 3 and 8* said that some suppliers were only re-evaluated at

[5] The CLOUD Act amends the 1986 Stored Communications Act (SCA) to allow U.S. federal law enforcement to compel U.S.-based technology companies, via warrant or subpoena, to provide data, even if it is stored on servers outside the United States [1]

contract renewal, typically every three to four years. Other organisations reported more regular reviews, often every three months, to assess performance. In addition to supplier dialogue, *R.2* used customer satisfaction surveys as part of their monitoring strategy. These findings suggest that organisations must tailor their trust assessments based on the type of risk involved. Technical, relational, and legal risks each require distinct mitigation strategies, and often necessitate layered governance and monitoring mechanisms.

Conceptual Procurement Trust Model. We present our findings in the form of a conceptual procurement trust model, with entities and transitions between those entities. The conceptual model of trust in third-party software procurement begins with **Trust Factors**, such as certifications, transparency, and prior performance data. These factors are *used by* various **Procurement Actors**, including procurement teams, risk officers, CISOs, and vendors, who *conduct* key **Procurement Processes** such as evaluation, contracting, and monitoring. These processes *produce* measurable **Outputs**, such as procurement decisions, trust scores, and risk mitigation plans. The outcomes of these outputs *inform* future activities and, through a feedback Loop, can *shape* policies and trigger reassessments of trustworthiness over time. This means that what happens after the contract, such as new risks or incidents, can lead to changes in how trust is measured or how future decisions are made. For example, the organisation might update its policies or reassess how much it trusts a vendor.

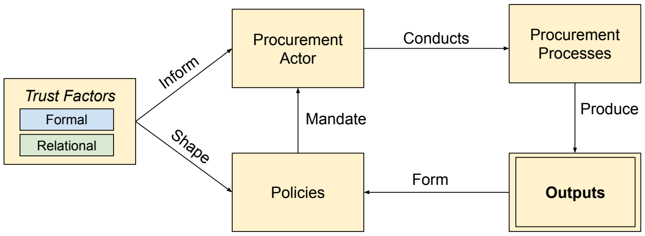


Fig. 2: The conceptual models shows how trust factors shape procurement decisions and actions through an extensive feedback loop.

The conceptual model echos the interviews: trust is not just something that happens at the start, but something that can change over time based on what the vendor does and how the situation develops. The model also shows that trust is built using both formal steps, such as certificates and contracts, and informal factors, such as transparency and past experience. These elements often work together during different stages of procurement.

5 Discussion

The procurement process observed in this study builds on the six-stage model [22], but extends it with a more iterative structure. In addition to standard phases, organisations include steps such as team formation, vendor demonstrations, trust scoring, ongoing monitoring, and reassessment. This reflects the practical complexity of managing procurement risks and trust factors over time, and demonstrates that procurement should be understood as a cyclical process rather than a linear one.

Shadow IT and Bypassing Formal Processes. The interviews revealed cases of shadow IT, where employees acquire software without involving central procurement or IT. This typically happens when formal processes are too slow or rigid. While sometimes justified by urgency, such practices introduce risks related to compliance, integration, and security. A more flexible procurement track for low-risk cases may help organisations maintain oversight while avoiding bottlenecks [21].

Proposed Improvements to Procurement Practices. The interviews suggest several actionable improvements. Flexible tracks for low-risk software could coexist with stricter controls for high-risk tools. Trust scoring mechanisms, vendor demos, and deep-dive sessions support clearer comparisons. Strengthening monitoring routines, especially around certification expiry and incident response, can help maintain trust over time. Internal consistency could be improved with shared templates and training, and vendor transparency should be incentivised by requiring disclosure of sub-processors, hosting locations, and prior incidents.

Consequences for Software Vendors. Vendors entering formal procurement need to demonstrate that their products are mature or strategically important enough to warrant evaluation. They must meet baseline requirements, including certifications and legal documentation, or present a clear and credible rationale for missing elements. In the latter case, trust may still be established through transparency, performance history, or risk assessments.

Future Research. Certification alone is rarely sufficient. Instead, organisations adapt evaluation practices based on internal risk tolerances and operational realities. To support this, publishing trust-relevant documents such as certifications in centralised procurement dashboards could improve oversight [10].

Legal and geopolitical concerns are becoming more prominent. Organisations expressed unease about U.S.-based cloud services due to data sovereignty issues. Trust frameworks must adapt to address extraterritorial data access and jurisdictional complexity.

For researchers, the findings call for new models that reflect trust as a dynamic, ongoing process. Future studies could explore trust trajectories over time, differences across sectors, and the integration of automated trust scoring tools. There is also room to investigate how cross-border procurement alliances shape trust and market balance. Finally, analysing real-world procurement documents may yield deeper insights into how trust, risk, and compliance are formalised in practice.

6 Conclusion

This study examined how large organisations assess and maintain trust throughout the lifecycle of third-party software procurement. Rather than relying solely on static indicators like certifications or compliance checklists, organisations apply a layered approach that evolves with shifting risks, vendor performance, and institutional priorities. Trust emerges not at a single decision point but through ongoing processes: structured evaluations, lived experiences, and negotiated compromises. It is shaped as much by legal frameworks and security standards as by transparency, responsiveness, and organisational context.

By mapping formal and relational trust mechanisms to procurement stages, this study clarifies how trust is operationalised in practice and how it is monitored over time. The findings challenge simplistic models of procurement and highlight the need for more flexible, risk-aware strategies; especially as legal uncertainty and supply chain complexity grow.

Statement of AI Usage. AI was used during the writing process to improve the English clarity and conciseness. None of the content was generated, however, without the author reviewing and editing. AI was also used to translate documents from Dutch to English; however, the translations were checked before being included.

References

1. Alston and Bird LLP: The cloud act and its impact on cross-border access to contents of communications, `https://www.alstonprivacy.com/cloud-act-impact-cross-border-access-contents-communications/`, accessed 2024-06-10
2. Ayala, C., Hauge, Ø., Conradi, R., Franch, X., Li, J.: Selection of third party software in off-the-shelf-based software development—an interview study with industrial practitioners. Journal of Systems and Software **84**(4), 620–637 (2011)
3. Bjarnason, E., Åberg, P., Ali, N.B.: Software selection in large-scale software engineering: A model and criteria based on interactive rapid reviews. Empirical Software Engineering **28**, 51 (2023)
4. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative Research in Psychology **3**(2), 77–101 (2006)
5. Bromberg, D., Manoharan, A.: E-procurement implementation in the united states: Understanding progress in local government. Public Administration Quarterly **39**(3), 360–392 (2015)
6. Cheng, X., Fu, S., de Vreede, G.J.: Determinants of trust in computer-mediated offshore software-outsourcing collaboration. International Journal of Information Management **57**, 102301 (2021)
7. Crowther, D., Aras, G.: Corporate social responsibility in medium to large enterprises. In: Aras, G., Crowther, D., Vettori, S. (eds.) Corporate Social Responsibility in SMEs. Social Responsibility Research Network (2009)
8. DeFranco, J.F., Kshetri, N.: Software supply chains. Computer **55**(10), 16–17 (2022)

9. Grover, V., Cheon, M.J., Teng, J.T.C.: The effect of service quality and partnership on the outsourcing of information systems functions. Journal of Management Information Systems **12**(4), 89–116 (1996)
10. Hou, F., Farshidi, S., Jansen, S.: TrustSECO: A distributed infrastructure for providing trust in the software ecosystem. In: International Conference on Advanced Information Systems Engineering. pp. 121–133. Springer (2021)
11. Hou, F., Jansen, S.: A systematic literature review on trust in the software ecosystem. Empirical Software Engineering **28** (2022)
12. Hou, F., Jansen, S.: A survey of the state-of-the-art approaches for evaluating trust in software ecosystems. Journal of Software: Evolution and Process **36** (2024)
13. Ilori, O., Nwosu, N., Naiho, H.: Third-party vendor risks in it security: A comprehensive audit review and mitigation strategies. World Journal of Advanced Research and Reviews **22**(3), 213–224 (2024)
14. Jansen, S., Cusumano, M.A., Brinkkemper, S.: Software Ecosystems: Analyzing and Managing Business Networks in the Software Industry. EE Publishing (2013)
15. Lonsdale, C.: The effect of the market on is/it outsourcing decisions: A review of the literature and a research agenda. Journal of Strategic Information Systems **10**(3), 241–268 (2001)
16. McKnight, D.H., Choudhury, V., Kacmar, C.: Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research **13**(3), 334–359 (2002)
17. Morgan, D.L.: Pragmatism as a paradigm for social research. Qualitative Inquiry **20**(8), 1045–1053 (2014)
18. Poppo, L., Zenger, T.: Do formal contracts and relational governance function as substitutes or complements? Strategic Management Journal **23**(8), 707–725 (2002)
19. Siddiqui, S., Thapa, C., Holland, R., Shao, W., Camtepe, S.A.: Elevating software trust: Unveiling and quantifying the risk landscape. arXiv preprint arXiv:2408.02876 (2024)
20. Vaidya, K., Sajeev, A.S.M., Callender, G.: Critical factors that influence e-procurement implementation success in the public sector. Journal of Public Procurement **6**(1/2), 70–99 (2006)
21. Van Acken, J.P., Jansen, F., Jansen, S., Labunets, K.: Who is the it department anyway: An evaluative case study of shadow it mindsets among corporate employees. In: 20th Symp. on Usable Priv. and Sec. (SOUPS 2024). pp. 527–545 (2024)
22. Verville, J., Halingten, A.: A six-stage model of the buying process for erp software. Industrial Marketing Management **32**(7), 585–594 (2003)
23. Williams, L., Benedetti, G., Hamer, S., Paramitha, R., Rahman, I., Tamanna, M., Tystahl, G., Zahan, N., Morrison, P., Acar, Y., Cukier, M., Kästner, C., Kapravelos, A., Wermke, D., Enck, W.: Research directions in software supply chain security. ACM Transactions on Software Engineering and Methodology **34**(5) (2025)