AI Project and Deployment Risk: Articulation and Legitimization

Sucheta Lahiri
Syracuse University
sulahiri@syr.edu

Jeffrey Saltz
Syracuse University
jsaltz@syr.edu

Abstract

This study explores how practitioners identify and manage AI project-related risks to reduce AI project failures. Specifically, through a qualitative research study involving 16 data science practitioners, this study presents insights into how practitioners articulate and mitigate the risk of AI project failure. A thematic analysis of this study identified six key themes (Ethical risk, BlackBox Models, Data Privacy, Data Storage, Financial Risks, and Success criteria). Further analysis explored drivers for identifying and mitigating these risks. Specifically, it was found that agency (consumer and institutional-driven) and Bourdieu's social/cultural capital (such as management hierarchy and domain knowledge) legitimized specific AI project risks and were key drivers in ensuring risks were identified and mitigated. Results from this research suggest that future research should explore different social and cultural perspectives since these perspectives can impact the articulation of risk and how these risks can be ultimately managed within an AI project context.

1. Introduction

Gartner's Data & Analytics Summit survey, conducted in 2022, highlights that only 44% of the artificial intelligence (AI) innovation leaders could see value in AI projects. In their 2021 survey, Gartner predicted that 54% of the AI projects would proceed from pilot to production environment. In other words, 46% of AI projects failed. In 2019, VentureBeat survey found that only 13% of AI projects could make it to production (Saltz & Krasteva, 2022).

In recent years, the topic of AI (and the broader field of data science) projects failure has gathered significant attention from scholars from various areas of interest. While many people use the terms data science, machine learning and AI interchangeable, there are nuanced distinctions in these terms.

Data science is a broad field focused on deriving knowledge from data, employing various analytical techniques. Machine learning, a subset of data science, specifically uses algorithms to learn from and make predictions on data. Artificial intelligence (AI) is an overarching domain that includes machine learning and aims to create systems that mimic or surpass human capabilities across various tasks (Yeturu, 2020).

There is a substantial body of literature accumulated during the past 40 years on information system (IS) failures. The IS scholarship broadly constitutes three areas of determinants contributing to IS failure: people, organization, and technology, with processes underlying across all three (Alharthi, Krotov, & Bowman, 2017).

One may hypothesize that AI (and more generally data science) project failure is driven by aforementioned IS drivers. Indeed, one key driver of preemptive failures for data science systems is a technocentric risk (Boyd, 2021), which is consistent with other IS projects in terms of being key drivers for project failures. Other key drivers not present in IS scholarship are the social and ethical risks that can cause discriminatory consequences, even in "successfully" deployed machine learning projects (Atkinson, Crawford & Ward, 2006).

A survey with 85 knowledge workers highlighted that despite the failure, the data science practitioners did not perceive failure as a hindrance to pursuing projects. In other words, the risk of failure was less important than the potential return on investment (Challen et al., 2019). In a different study, the prominent reasons for data science/AI project failure were related to unachievable expectations, ambiguous objectives, limited talent, data issues, excessive dependence on technology, inefficient deployment, and maintenance planning (Karacsony, 2022).

These reasons align with the notion that project failures can be defined with a positivist and functionalist paradigm. With this view, one can define failure with performative critical failure factors (CFF) of time, cost, and targets (Santos, Reis Neto, & Verwaal, 2018). However, what can be seen as a successful project with structured PMBoK (Project Management Body of Knowledge) criteria

URI: https://hdl.handle.net/10125/107088
978-0-9981331-7-1

may be considered a failure through the sociotechnical lens.

For example, design justice scholar and activist Constanza-Chock highlights the ‘sociotechnical reproduction of gender binary’ (Costanza-Chock, 2018) of scanning artifacts at airports that can only identify male and female identities. Constanza-Chock notes that ‘the database, models, and algorithms that assess deviance and risk are all binary and cisnormative’. Similarly, People of Color, Muslims, immigrants, and/or People with Disabilities face higher rates of social risk with the high-end machine learning-driven scanning systems (Challen et al., 2019; Costanza-Chock, 2018).

Another case study where a machine learning system was deemed 'successful' but resulted in discriminatory outcomes for people is exemplified by the Apple card incident, which exhibited gender bias against women. In this situation, David Heinemeier Hansson, a software developer, and a Danish entrepreneur, upon comparing the spending limit of his Apple Card with his spouse's, observed that even though his partner had a better credit score and other criteria in her favor, her request for a credit line increase was rejected (Vigdor, 2019).

In this situation, while the machine learning credit card algorithm for the Apple card was initially deemed a success, further analysis identified the sociotechnical issue. In short, the risks involved in Apple card case study were reputational, ethical, and social.

The above examples illustrate that despite being successful, if the sociotechnical system perpetuates social, reputational, legal, and privacy risks, it can be seen as a project failure.

This raises critical questions on how risk of AI projects is defined, and which risks are legitimized. In other words, *who identifies what risk should be considered during the execution of AI project? What risks are not considered in the AI risk management process?* Legitimization comes from the Latin word ‘legitimus’ which is related to law and consensus. Legitimization of social practices in an institutional set-up is typically performed by social actors who hold a position of authority. These social actors signify symbolic power through their technical vocabulary to meet political goals (Alharthi, Krotov & Bowman, 2017).

With this in mind, the overarching research question of this paper is:

How is the risk of failure articulated by data science practitioners during the AI project execution and deployment?

In the following section, we extend discussion on how information system scholarship defines AI risk of failure through functionalist perspective. The paper then connects the scholarship with social capital and cultural capital in the findings section to highlight the dominant themes of how data science practitioners articulate risks due to agency of different project constituents as well as based on social / cultural capital (ex. educational qualification and job role).

2. Previous Literature on AI project Risk of Failure

2.1. AI project Risk of Failure

There are existent yet scant studies in IS scholarship that identify the factors of AI project risk of failure. Some of many other primary factors of failure for AI / data science projects in IS scholarship are (1) unclear business requirements, (2) inefficient communication channels (3) compromised data quality (4) lack of relevant talent (5) rigid project plans that have no room for expansion (Lai, 2017).

For example, a Delphi study with data science experts classified the risks of data science project failure based on PMI structure: *functional scope, project management, operation management, technological, quality, resource, surrounding environment, legal, communication, organizational and others* (Joyce et al., 2021). During the content analysis of the Delphi survey, the dominant theme was the formulation of problems that started with vague and inaccurate questions. Other themes were related to poor project scope, compromised data quality, misunderstanding of the specifications, scarcity of talent, privacy breach, inefficient analysis of model, miscommunication, and transparency of model.

Another Delphi study conducted with technical data science practitioners (Chapman, 2000) confirmed similar themes in addition to themes related to absence of strategic outlook, change management and ethical issues. It is noteworthy that in this Delphi study, ethical concerns were placed towards the end of the rank order.

Other research studies identified themes focused on development risk, deadline delays, the lack of support from leadership (Martínez-Plumed et al., 2019), as well as the lack of governance policies, heterogeneity, and size of data (Boyd, 2021). Finally, the lack of an effective project management methodology was noted as one of the key reasons for the failure of AI projects (Saltz & Krasteva, 2022).

However, different narratives of risk shifting from normative definition of risk have been overlooked. Despite heightened attention to potential technical and functional deficiencies of AI projects; critical questions on how the risk of failure during project execution is articulated and interpreted by data science practitioners has not been extensively explored.

2.2. NIST AI Risk Management Framework

There have been efforts organizations, including government agencies, to help manage the risks of AI projects with risk management frameworks (RMF) (Saltz & Lahiri, 2020). For example, on January 26th, 2023, in association with public and private organizations, NIST launched a sector-agnostic Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST, 2023). Overall, the Framework is a steppingstone for the thinking process around risk management for AI projects.

In short, the AI NIST RMF defines risk with the probability and consequences of unfavorable events. Being aligned with ISO 31000:2018's definition of risk, the AI NIST Framework not only tries to minimize negative consequences of AI risk, but also explores positive events aligned with living wellbeing (NIST, 2023). The Framework recognizes three categories of risk that are directed to (1) individuals (2) institutions (3) overall living habitat. The risks span from social risk to reputational risk and climate risk. The RMF proposes test, evaluation, verification, and validation (TEVV) of the artifact across the entire (end-to-end) project life cycle. Overall, there are four core functions of NIST AI RMF: governing a culture of risk management which sets the control, depending upon the content the risk elements are mapped, measuring, or assessing the risk after identifying, and finally prioritizing and managing the risks. In addition, the framework provides generic guidelines for risk management through collective responsibilities of social actors.

However, the framework does not provide any direction on 'how' to navigate the phases from planning and design, collecting and processing data, building, validating, deploying, to monitoring and impact assessment of the model. Similarly, the 'must-have' characteristics of AI models from trustworthiness to validity, reliability, safety, security, resiliency, transparency, explainability, privacy, fairness are provided with ISO definitions. The definitions of risk are normative, and no guidance is offered on how to achieve the ideals of a 'good' AI system. In other words, a standard definition of risk from ISO is leveraged to create the RMF for AI without any consideration of social, cultural, and political context that may shift the articulation of risk on individual level.

2.3. Theoretical Foundations

2.3. 1. Bourdieu's Social Capital

Bourdieu relates social capital with power that is vested through social relationships and group affiliations. In other words, social capital originates through the networks and relationships that employees establish within their professional and business spheres. Social capital is a result of other emergent interactions among individuals within the workforce, regulatory bodies, collaborative partners, and clientele (Salajegheh & Pirmoradi, 2013). The social capital also creates *symbolic* capital with designations, work titles and social validation (Bourdieu, 2018).

In the context of AI projects, we look at the views of participants who are members of the extended project team. In the pool of participants, some hold management positions and others hold either independent contributor's position or are subject matter experts. These participants contribute to the AI project execution in some capacity and form.

2.3.2 Bourdieu's Cultural Capital

According to Bourdieu, cultural capital refers to the knowledge and intellectual abilities which offers an advantage to social elites in attaining a more elevated social status within society (Santos et al., 2018; Bourdieu, 2011). Cultural capital, highlighted as one of the most significant forms of capital, encompasses a range of cultural resources, including cultural understanding, attitudes, and artifacts that hold significance within a specific domain of data science practitioner engagement (Levy & Reiche, 2018). Cultural capital and the social hierarchy are intricately intertwined, as they function hand-in-hand to classify individuals and groups into varying positions within the social structure, determined by their respective endowments of capital resources.

With respect to this project, we interviewed subject matter experts, AI project managers, risk managers, data scientists, and strategy makers from public and private organizations to understand their perspectives on risk. These "social elites" are a part of either a hierarchical structure or alternatively, part of a flat structure where subject matter expertise supersedes work title.

3. Methodology

In this qualitative study, we were interested in understanding different perspectives and articulations of project risk and deployment from the members of the AI project team.

The participants, who all worked on AI projects, were chosen from various industries across both public and private sectors. It is noteworthy that data science practitioners were given the opportunity to categorize themselves as data scientists; there were no definitions borrowed from the literature to circumvent 'data scientist's' profile. All the participants who appeared for the semi-structured interview was termed generically as data science practitioners. Similarly, the participants were allowed to use AI, data science and machine learning concepts interchangeably despite the noted differences.

Using Bourdieu's cultural capital, the study explored how embodied cultural capital and institutional cultural capital (Levy & Reiche, 2018) solicited agencies to the AI practitioners to articulate risk and subsequently legitimize it. Social capital was used as a lens to verify how the data science practitioners are persuaded to legitimize AI project risks.

Institutionalized cultural capital was viewed to encompass both recognized qualifications such as academic degrees, as well as specialized knowledge and skills. These explicit or implicit credentials served as a foundation for validating the significance of embodied cultural capital.

The data collection for this study started with distributing posters and messages on public team collaboration tools, social media channels, and public professional networks. Due diligence was taken to make sure that only those data science practitioners were recruited who qualified the study criteria. The initial contacts selected for this study became the first node of connection who solicited the contacts of other relevant potential participants for interview. In other words, referral process or the snowball sampling was used to gather data science practitioners for this study (Parker, Scott & Geddes, 2019).

Below table provides a description of 16 AI practitioners who were selected to get interviewed.

Table 1. Education and Work Background of 16 Participants

ID	**Gender**	**Role**	**Risk Mgmt Exp (yrs)**	**Education**	**Work Background**
DS1	M	Director – AI	10	MS	Intelligence Analysis, Operational Risk Management
DS2	M	VP – Strategic Business	20	PhD	Data Science, AI
DS3	M	VP – Data & AI	17	MS	US Naval Academy, Analytics & AI
DS4	M	VP – Automation and Analytics	1	BS	Data Analytics, Business Intelligence, Data Warehouse
DS5	M	Data Scientist and Risk Manager	10	PhD	Bank regulation related to Risk Mgmt
DS6	M	Manager – Global Data Mgmt	10	MBA	Financial Industry and Professional Consulting
DS7	M	VP – Data Science	8	PhD	Finance Industry, Model Risk, Advanced Analytics
DS8	M	Deputy Director	6	BA	Risk Mgmt, Project Mgmt, IT
DS9	M	Assistant VP	6+	PhD	Data Analytics, Mgmt Consulting
DS10	M	Exec Director	12-15	MS	Credit Risk
DS11	M	Senior Risk Manager	20	BS	IT Audit, IT Risk Mgmt
DS12	M	Risk Data Analytics Architect	7	MBA,	Project Mgmt, Business Intelligence
DS13	M	Associate-Modeling	3	MS	Evaluating model risk
DS14	M	Manager-Data Science	Learning on the job	MS	Analytical solutions for sales teams
DS15	M	Manager-Manufacturing Analytics	Learning on the job	PhD	Analytics Infrastructure
DS16	M	Director-ML	7+	MBA, MS	Recommendations and personalization

As shown in table 1, no women participants could be identified for participation in the study. In addition, many of the participants were very experienced, and often part of senior management. The following section of analysis and findings highlight how the individual articulation of risk may be different from the institutional defined risk.

4. Data Analysis

Thematic analysis or TA is typically used in qualitative research to glean pertinent trends or patterns. The framework of thematic analysis consists of five phases (Castleberry & Nolen, 2018): *gathering, deconstructing, reconstructing, interpreting, and reaching a conclusion.*

In the first phase of thematic analysis, the data gathered through the semi-structured interviews were transcribed. The interviews with 16 male data science practitioners were conducted through zoom calls post IRB approval. The interview lasted from 30 minutes to 120 minutes. Before the interview, a consent form was sent to make sure that the participants were aware of the premise of the study. After gathering the data, participants were anonymized with alphanumeric digits. In the second phase of the study, we deconstructed the interview transcripts. In other words, we broke down the text data into broader components or themes. The components were gleaned independently by both the authors. Weekly calls were scheduled to discuss the matches and the mismatches of the findings. In the third phase, the deconstructed themes were reconstructed by combining smaller and similar. Brain storming calls were conducted to reconcile the differences. In the fourth and consequently the fifth phase, we interpreted the broader and subsumed under narrow themes with inductive approach and finally derived pertinent themes for this study.

5. Findings

Multiple articulations of risk of failure that arose during an AI project were shared by the participants during the interviews. In other words, the participants shared how they understood and ascribed meanings to AI project risks and deployment risk. Individual articulations were often influenced by the normative institutional and regulatory codes of risk standards and policies. However, there were other perspectives identified that had little or no point of reference attached to institutional risk.

This section provides an overview of different perspectives of the data science practitioners, in terms of how they interpreted risks of AI project execution and deployment. Table 2 below provides a snapshot of the different areas of risk focus.

Table 2. Dominant Themes of AI Project Execution and Deployment Risk

Risk Focus	Short Explanation	Organizations (ID#)
Ethical risk	Court case, reputation, model discrimination, Bias, Overfitting	DS1, DS2, DS7, DS9
BlackBox Models	Explainability, Transparency	DS1, DS7, DS9, DS16
Data Privacy	Insider Threat, PII, Data Classification	DS1, DS6, DS7, DS12
Data Storage	Data lakes, data factory, data warehouse, Data culture, Data preprocessing, Data formatting	DS4, DS5, DS8, DS16
Financial Risks	Mortgages and portfolio management, asset management, Stochastic Shocks, Monte Carlo simulations, macroeconomic indicators, daily or weekly market volatility, investment leverage	DS3, DS5
Success criteria	user experience, user recommendation,	DS3, DS8, DS16

In addition, as shown in Table 3, the analysis identified several insights with respect to how agency, and social / cultural capital impact the identification and mitigation of those risks.

Table 3. Social/Cultural Capital that Influenced AI Project Execution and Deployment Risk

Risk Focus	Impact of agency, and social/cultural capital
Ethical risk	Agency of consumers - drives proactive identification of ethical risks. Acknowledgement of ethical risk - is contingent upon the senior stakeholders who led the team
BlackBox Models	Agency of consumers - drives proactive explanation of model behavior.
Data Privacy	Agency of the government - the identification / management of risk is driven by regulations.
Data Storage	Cultural capital (i.e., domain knowledge) – drives the organization to acknowledge / manage these risks
Financial Risks	Agency of financial risk managers - drives how the financial impact of a model is evaluated. Agency of the government - the identification / management of risk is driven by regulations.
Success criteria	Agency of the client – define success criteria to reduce risk

5.1. Ethical Risk of AI projects

Ethical risk was construed as a material threat, due to model behavior, that had a potential detrimental impact on organizational reputation. For example, DS1 worked for a government defense agency and was a director for AI strategy who linked ethical risks with the legal and reputational impact to the agency.

… if we ever have to go to court, or there's a lot of people that sue us in court over personnel decisions made by the machine, what do we have to do to make sure that what we are doing is both ethical and legal? And what kind of strategic risk does that engender for the agency? So those are the kinds of federal levels of risk I have to consider when we apply projects…(Lahiri & Saltz, 2022)

Similarly, DS9, who worked as a third-party consultant for a bank, interpreted ethical risk as the bias that perpetuated with the decisions made on loan approval, that might need to be defended in a court.

…we are working on a project with [bank name]. Now they are having trouble with their customers because whenever the loan is not granted to the customers then customers may actually go to the court of law…for asking that why loan is not granted…maybe…you know some prejudice is there…

In a different example, DS2, who works as the lead ethicist and team manager at a manufacturing conglomerate, could individually define the risk and implement counter risk measures. The measures, as DS2 highlights, could be taken without the consensus of the members of the data science team, and could simply be "not doing the project". In other words, being a significant part of the power structure, DS2 could take ownership of the risk without going to management.

But the ethical risks I, I think of myself as…as the risk taker…so there…there are projects that I've simply declined. And I didn't even ask my teams, I simply said, no…this is ethically unacceptable. We're not going to do it, period…

Yet a different participant, DS7, who lead the model risk team stated that the contribution of audit occurs at the top of reporting on the model. However, in addition to the audit for model risk, it was important to have unified or centralized policies and standards to monitor the models.

… there's a lot of taking an interest in the model risk and model governance these days. There's also a lot of discussion in the industry itself, right? Like how to identify for model has been discriminating, you know, not directly but indirectly, right. So, what kind of bias matrix we should bake into the models. So, that is where I see a lot of scope and work to be done remaining, because we have very solid principles on how to…how to create a data from customer and how to store it and how to not store it. We have good policies on that. But where we are really missing the ball is having a good policy and unified standards, and the tooling aspects, for monitoring models and making sure they're not doing the wrong thing…"

The participant highlights the efficacy of having effective policies for machine learning models in place that trickles the power top-down to bring change from management to employee level.

The above narratives demonstrate that ethical risk is aligned with the reputation of the firm. There is a concern that the users in society may take legal help to hold the organization responsible for undesirable prejudice. This highlights that despite limited formal mandates with respect to model ethics, users have agencies that helps to minimize ethical risk.

Another noteworthy theme is related to the legitimization of risk through the cultural and social capital of domain experts and management practitioners. DS2 was the team manager that earned capital and the agency to enforce changes and modifications to the team's risk management processes.

In short, considering cultural capital as the signifier for power, social capital was earned with the members of AI project. The acknowledgement of ethical risk was often contingent upon the senior stakeholders who led the team. In other words, the process of acknowledging ethical risk was typically dependent upon the data science practitioners from the management team. For example, DS1 rationalized the ethical risk putting the team member's perspectives in mind, whereas for DS2, the legitimization is individualistic. This theme also generates critical enquiries on exploring the interpretations of social actors across the project, which according to Bourdieu, is the field (Levy & Reiche, 2018).

5.2 BlackBox Models

During the interviews, data science practitioners were concerned about the opacity of the data science models.

For example, DS9 articulated a risk due to the lack of model explainability. The quote below reflects the obscurity of a Blackbox model that impedes the cultural capital of the data science practitioners. In other words, the capital of technical skill and knowledge is not what it needs to be to fully explain the BlackBox, more work is required to make the model digestible to the common citizen through simple language or the use of other models. Furthermore, consumers hold the power to voice against the biases of data science models by taking legal assistance, which re-reinforces the need for explainable models. In short, the power conflict with the project is with the external forces, such as the vested consumers.

…we are working on a project with a bank…they are having trouble with their customers because whenever the loan is not granted to the customer, then customers may actually go to the court of law for asking why the loan was not granted…maybe some prejudice is there…so explaining why the loan is not granted…that's a big challenge because it's a model is like a black box…but how you explain to the customer that these are the reasons…we are unable to provide to the loan…okay, so this is the area we're still working and big challenge is there…

A different type of black box challenge was shared by participant DS1, who identified risk with the obscure and technical language that data science professionals sometimes use to communicate with stakeholders and management during the project workflow.

"…And so, as I was reading some of the language written into what we're trying to communicate to folks [management] about what they're supposed to do with their products…we are using a lot of technobabble to explain ... Yes…You sound super smart. Congratulations! But nobody can use the information because they don't understand what it means…" (Lahiri & Saltz, 2022).

5.3 Data Privacy

Many machine learning projects generate knowledge insights via the use of heterogeneous and oftentimes large amounts of data. Privacy in organizations becomes paramount in terms of safeguarding sensitive information from unauthorized access and false positives in data classification.

DS6 articulated the risk from data classification and privacy perspectives that must align with governance policies and government legislation. According to DS6, risk was generated with the misclassification of PII or when the data classification deviated from the standard data classification rule. On the context of data leakage, DS6 highlighted the hazards of not complying with GDPR mandates for data classification.

…I think the most important thing these days is really around…data privacy. So, data privacy has become a huge deal over the last three to four years now with GDPR and nuances of it, and versions of it in other regions. So, the risk of…how we keep data, how we are using other people's data…how long we are going to be using it for…and who else are we going to giving it to…are becoming very important these days…(Lahiri & Saltz, 2022).

On similar lines, DS7 who worked for a giant investment bank shared the concerns of privacy risk.

…Starting from the data privacy risk…the policies around data and the…holding the data in your warehouse and then technology risks…so there is no leakage of data because of the tooling…

Hence, with respect to data privacy risks, the dominant force for identifying and managing these data privacy risks was driven by standards and policies.

For example, DS6 shared why it was imperative that data science practitioners consider the regulations and standards while executing the project. There is a desire (or obligation) to adhere to the government established policies that ultimately directs the articulation and mitigation of this AI project risk. In other words, the identification of this risk was due to authority and standard rituals rather than intrinsic moral values.

5.4 Data Storage

Data storage risk is related to data, which is used to build predictive models, being stored in multiple, often incompatible organizational and/or technical "silos". This makes it difficult to fully leverage all the data that is available.

For example, according to DS5, risk is articulated with data inconsistencies that are not compatible with the system-based formatting systems. As a part of the issue, inconsistent data formatting was considered as an issue in risk forecasting projects.

…Well, there are certain features that are already, probably part and parcel of the risk measure, you know, daily or weekly volatility, the amount of leverage being used on an investment, and macroeconomic indicators…A lot of the work is actually loading the data. Because they don't come in the same format. Formatting is a big issue, especially around dates with dates. Dates stored are not always the same with every system…

Similarly, DS4 also highlighted that despite having the success criteria, the organization was often engaged in conflicts with cross-border teams and fragmented data repositories that created data related risks. DS8 also believed that data inconsistencies arose with siloed data repositories that had different taxonomies. Risk was interpreted with siloed processes that did not create synergy with the data.

We have…I would say…the largest bunch of disparate and improper data center that the federal government has on our side…we have eight different data centers using eight different processes, we do not have data dictionaries as a coder or anything. It's pretty much the wild wild west…

In a different part of the discussion DS8, DS8 used specific linguistic choices to legitimize risk that indicated the apparent absence of project documentation in the system. The language was intentional to rationalize risk with symbolic linguistic of cultural capital.

"…I have a backbone system that was written in COBOL that was loaded by two guys who actually knew how to fix…and they're both in their 80s. And no one…there's not a single…don't know where the codes are written down…these guys [practitioners in 80s] have the codes bolted in their head and…this has been going on for years! And so now, like I said, after four years of screaming and banging my head against the wall and drinking a lot of scotch…they [management] finally got to the idea of let's start

writing things down. I know it's not fun, but it's important…"

Further probing highlighted that the risk of working in silos is the absence of the risk culture in the organization.

… We have a lot of disparate admissions and we don't really have a risk culture. We're so risk averse, it's not even funny being federal employees terrified of the word risk…

The above narrative expresses the negative emotions towards risk; that risk, at least in this context, is considered more as a threat than an opportunity. Also, the above theme highlights that the process of legitimization of risk also entails having the culture that can inculcate the sentiment of contemplating and managing AI project risk.

5.5 Financial Risk

The concept of financial risk and risk management governance popularized from the middle of 1950s with market insurance. Further regulatory mandates with BASEL II/III accord, Sarbanes-Oxley, Solvency-II added additional layers of credit, market, liquidity, and market risks along with compliance and anti-money laundering (Winchester, Boyd, & Johnson, 2022) to finance organizations.

DS10 who worked for a large finance investment organization, managed credit risk with data analytics, process engineering and customer experience. DS10 connected data science risk with the financial risks related to mortgages and portfolio management.

…Some of the top line risk is, in terms of origination of mortgages and also the portfolio management of mortgages, so what is coming into pipeline and what is in your portfolio…

In other words, DS10 managed the financial risk management of customer portfolios that consisted of the capital revenues and credit scores details. The data was used to understand the problem or customer related capital risk and then generate a prototype for knowledge insights.

…we can sort of say high level could be understanding what is the problem, doing interviews and research interviews with client. It could be internal and external stakeholders and then doing research, to get a better understanding of your problem then proposing, your, analysis and outcomes to your stakeholders to get a buy in… and then you start doing a prototype… and then come up with a champion…

This risk management required buy-in with the stakeholders in the power structure who confirmed if the risk was a true risk. Also, being an investment organization, the risk had to adhere to specific financial regulations.

5.6 Success Criteria

The success criteria encapsulates themes such as budgetary criteria, change management, and clear business objectives that have previously been identified in IS literature (Varela & Domingues, 2022).

For example, DS2, who worked for a private manufacturing company, elucidated risk that arose with ambiguous business objectives, change management, and budgetary constraints. These themes tie well along with the IS scholarship and highlights that similar issues can occur within a data science risk context.

…There are a multitude of risks associated with data science. The most obvious one is that the project quote unquote fails…you have to figure out what the problem is and there is a risk. In fact, this occurs that more often than we'd like that. There was miscommunication and the problem is solved that never existed, and right and the problem that did existed and get solved. And a third risk is in the change management procedure that has to follow the artificial intelligence…

DS4 defined risk as the absence of the specific business objectives or the 'success criteria' in the organization. In other words, DS4 elucidated the importance of success criteria which becomes the 'ground truth' for the data science practitioners and any deviation to it is construed as risk.

…Before you calculate or even understand your risk, anyone establish any risk framework, first thing you have to do for a given project is that you have to establish what is my success criteria…what am I trying to get out of this? When do I say this project has succeeded?... And I encourage you to ask this question to many of the other participants…majority of them don't even do that…(Lahiri & Saltz, 2022)

Additionally, DS4 highlighted that despite having the success criteria, the organizations were often engaged in conflicts with cross-border teams and fragmented data repositories that created data related risks. This narrative highlighted that it was not enough for practitioners to leverage their knowledge and technical skills, they also needed to clearly understand and deliver what had been communicated via the success criteria. The potential lack of harmony (conflicts of not understanding and/or delivering "success") is a risk that could become an impediment with the successful execution of the project.

This explains why DS2 mentioned miscommunication as risk for AI projects. In a different example, according to DS6, the legitimization of risk and the risk mitigation measures were legitimized only when those risks were interpretable and effectively communicated to the practitioners.

6. Conclusion

In this qualitative study, 16 male data science practitioners were interviewed to explore how the risk of failure for an AI project was articulated on an individual level during project execution.
The cultural capital that these practitioners leveraged was created via their educational background and the number of industry years they spent with domain. The practitioners were mostly in senior leadership positions, who had their individual perspectives on risk, homogenized with institutional definitions of risk. The articulation of risk was influenced by existing finance regulations, data laws such as GDPR and the weak theme of ethical risk.

Yet, even for senior leaders of AI projects, there were attempts to articulate AI project execution and deployment risk based on the agency of others or their internal intrinsic understanding of risk.

6.1 Summary

During the content analysis of semi-structured interviews with data science practitioners, six pertinent themes - Ethical risk, BlackBox Models, Data Privacy, Data Storage, Financial Risks, Success criteria - emerged as individual articulations of AI project risk.

Cultural capital was often represented as symbolic capital to legitimize risk, and social capital was represented to gain consensus. There were also 'risk takers' encountered during the interview who did not depend upon social capital to legitimize their notion of AI project risk.

Even though the scope of this study was not related to understanding the power structure of team members, during the thematic analysis using Nicolini's zoom-in and zoom-out lens (Nicolini, 2009), there were many instances of power conflicts that legitimized and delegitimized risk.

6.2 Limitations and Future Work

This paper, to the best of our knowledge, is the first attempt to explore how risk is articulated on an individual level by the social actors who are the members of data science team.

However, the participants for this study were experts in data science domain. In this respect, one key limitation of this study was the lack of diversity of the practitioners interviewed. Hence, future work should explore participants in the data science process, who have less expertise and/or a lower position within the organization (i.e., different cultural capital than those interviewed in this study). In other words, future research should explore the AI project risk articulation from data science practitioners from different classes, genders, race, and ethnicity. For example, exploring how practitioners from offshore entities and back-office employees identify and articulate risks of AI projects. In a different example, future research should also explore if the gender of the practitioners impacts their perception and articulation of AI project risk. Another limitation of this research was the small sample size of the number of participants in the study. Hence, future research could explore these themes more broadly, via a survey of a broad range of data science practitioners.

Furthermore, Nicolini's zoom-in and zoom-out toolkit could be used to analyze social practices of data science practitioners who do not necessarily situate themselves in the power structure and mediate the risk articulation through common set of beliefs (Nicolini, 2009). Finally, this research also suggests that science and technology studies scholars, feminists, and critical scholars, analyze how AI project risks are interpreted by different races, ethnicities, and gendered practitioners.

7. References

Aho, T., Sievi-Korte, O., Kilamo, T., Yaman, S., & Mikkonen, T. (2020). Demystifying data science projects: A look on the people and process of data science today. In Product-Focused Software Process Improvement: 21st International Conference, PROFES 2020, Turin, Italy, November 25–27, 2020, Proceedings 21 (pp. 153-167). Springer International Publishing.

Alharthi, A., Krotov, V., & Bowman, M. (2017). Addressing barriers to big data. Business Horizons, 60(3), 285-292.

Arista, N., Costanza-Chock, S., Ghazavi, V., Kite, S., Klusmeier, C., Lewis, J. E., ... & Darling, K. (2021). DESIGN JUSTICE, AI, AND ESCAPE FROM THE MATRIX OF DOMINATION.

Atkinson, R., Crawford, L., & Ward, S. (2006). Fundamental uncertainties in projects and the scope of project management. International journal of project management, 24(8), 687-698.[19] Parikh, R. B., Teeple, S., & Navathe, A. S. (2019). Addressing bias in artificial intelligence in health care. Jama, 322(24), 2377-2378.

Bourdieu, P. (2011). The forms of capital.(1986). Cultural theory: An anthology, 1, 81-93.

Bourdieu, P. (2018). The forms of capital. In The sociology of economic life (pp. 78-92). Routledge.

Boyd, A. E. (2021). Intersectionality and reflexivity—decolonizing methodologies for the data science process. Patterns, 2(12), 100386.

Castleberry, A., & Nolen, A. (2018). Thematic analysis of qualitative research data: Is it as easy as it sounds?. Currents in pharmacy teaching and learning, 10(6), 807-815.

Challen, R., Denny, J., Pitt, M., Gompels, L., Edwards, T., & Tsaneva-Atanasova, K. (2019). Artificial intelligence, bias and clinical safety. BMJ Quality & Safety, 28(3), 231-237.

Challen, R., Denny, J., Pitt, M., Gompels, L., Edwards, T., & Tsaneva-Atanasova, K. (2019). Artificial intelligence, bias and clinical safety. BMJ Quality & Safety, 28(3), 231-237.

Chapman, P., Clinton, J., Kerber, R., Khabaza, T., Reinartz, T., Shearer, C., & Wirth, R. (2000). CRISP-DM 1.0: Step-by-step data mining guide. SPSS inc, 9(13), 1-73.

Collins, P. H. (1998). Fighting words: Black women and the search for justice (Vol. 7). U of Minnesota Press.

Costanza-Chock, S. (2018). Design justice, AI, and escape from the matrix of domination. Journal of Design and Science, 3(5)

Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). The KDD process for extracting useful knowledge from volumes of data. Communications of the ACM, 39(11), 27-34.

Gray, L. (2019). In a collective voice: Uncovering the Black feminist information community of activist-mothers in Chicago public housing, 1955-1970.

Gray, L. (2021). Case Study Inquiry & Black Feminist Resistance. The International Journal of Information, Diversity, & Inclusion, 5(2), 71-83.

Gustavsson, T. K., & Hallin, A. (2014). Rethinking dichotomization: A critical perspective on the use of “hard” and “soft” in project management research. International Journal of Project Management, 32(4), 568-577.

Johnson III, R. G., & Renderos, H. (2020). Invisible populations and the# MeToo movement. Public Administration Review, 80(6), 1123-1126.

Joyce, K., Smith-Doerr, L., Alegria, S., Bell, S., Cruz, T., Hoffman, S. G., ... & Shestakofsky, B. (2021). Toward a sociology of artificial intelligence: A call for research on inequalities and structural change. Socius, 7, 2378023121999581.

Kapitzke, C. (2000). Information technology as cultural capital: Shifting the boundaries of power. Education and Information Technologies, 5, 49-62.

Karacsony, P. (2022). Analysis of the Attitude of Hungarian HR Professionals to Artificial Intelligence. Naše gospodarstvo/Our economy, 68(2), 55-64.

Lahiri, S & Saltz, J. The Need for an Enhanced Process Methodology for Ethical Data Science Projects. IEEE ETHICS-2023: Ethics in the Global Innovation Helix[34] Börjesson, M. (2017). The global space of international students in 2010. Journal of Ethnic and Migration studies, 43(8), 1256-1275.

Lahiri, S., & Saltz, J. (2022, January). The Risk Management Process for Data Science: Gaps in Current Practices. In Proceedings of the 55th Hawaii International Conference on System Sciences.

Lai, S. T. (2017). An Iterative and Incremental Data Quality Improvement Procedure for Reducing the Risk of Big Data Project. J. Softw., 12(12), 945-956.

Levy, O., & Reiche, B. S. (2018). The politics of cultural capital: Social hierarchy and organizational architecture in the multinational corporation. Human Relations, 71(6), 867-894.

Martínez-Plumed, F., Contreras-Ochando, L., Ferri, C., Hernández-Orallo, J., Kull, M., Lachiche, N., ... & Flach, P. (2019). CRISP-DM twenty years later: From data mining processes to data science trajectories. IEEE Transactions on Knowledge and Data Engineering, 33(8), 3048-3061.

Modrek, S., & Chakalov, B. (2019). The# MeToo movement in the United States: text analysis of early twitter conversations. Journal of medical Internet research, 21(9), e13837.

NIST AI, (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0).

Nicolini, D. (2009). Zooming in and out: Studying practices by switching theoretical lenses and trailing connections. Organization studies, 30(12), 1391-1418.

Ozmen, E. S. (2013, March). Project Management Methodology (PMM): How can PMM serve organisations today?. In Proceedings of PMI Global Congress EMEA.

Parker, C., Scott, S., & Geddes, A. (2019). Snowball sampling. SAGE research methods foundations.

Reyes, A. (2011). Strategies of legitimization in political discourse: From words to actions. Discourse & society, 22(6), 781-807.

Salajegheh, S., & Pirmoradi, N. (2013). Social capital of the organization. Social Capital, 7(12), 40-52.

Saltz, J. S., & Krasteva, I. (2022). Current approaches for executing big data science projects—a systematic literature review. PeerJ Computer Science, 8, e862.

Saltz, J. S., & Lahiri, S. (2020). The Need for an Enterprise Risk Management Framework for Big Data Science Projects. In DATA (pp. 268-274).

Santos, A. S., Reis Neto, M. T., & Verwaal, E. (2018). Does cultural capital matter for individual job performance? A large-scale survey of the impact of cultural, social and psychological capital on individual performance in Brazil. International Journal of Productivity and Performance Management, 67(8), 1352-1370.

Varela, C., & Domingues, L. (2022). Risks of Data Science Projects-A Delphi Study. Procedia Computer Science, 196, 982-989.

Vigdor, Neil. (2019). Apple Card Investigated After Gender Discrimination Complaints. https://www.nytimes.com/2019/11/10/business/Apple-credit-card-investigation.html

Winchester, H., Boyd, A. E., & Johnson, B. (2022, May). An exploration of intersectionality in software development and use. In Proceedings of the Third Workshop on Gender Equality, Diversity, and Inclusion in Software Engineering (pp. 67-70).

Yeturu, K. (2020). Machine learning algorithms, applications, and practices in data science. In Handbook of Statistics (Vol. 43, pp. 81-206). Elsevier.