International Journal on
Advanced Science
Engineering
Information Technology

Vol.10 (2020) No. 1
ISSN: 2088-5334

Risk Evaluation Using Nominal Group Technique for Cloud Computing Risk Assessment in Healthcare

Nurbaini Zainuddin[#1], Rasimah Che Mohd Yusuff [#2], Ganthan Narayana Samy[#]

[#]Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, 54100, Malaysia
E-mail: [1]nurbaini2@live.utm.my, [2]rasimah.kl@utm.my

Abstract— **Emerging of cloud computing with flexibility, improve accessing data, and cost-saving makes this technology accessible and growing fast. As a result of the emergence of cloud computing bring interest to industries to used cloud computing. Although cloud computing brings so many benefits to customers, the previous study reveals that cloud computing penetration in the Healthcare area is still low. With effective cloud risk assessment methodology will gain the confidence to cloud users in this technology. Study in cloud risk assessment methodology still infant and the complexity in identifying security risk still debating. This paper explores the risk assessment process by highlighting the method in the risk evaluation process. Risk evaluation is an essential phase in the risk assessment process. It compares the result from the risk analysis process and determines whether to accept or tolerate the risk criteria to decide on the risk analysis. In this study, the Nominal Group Technique (NGT) is introduced to compare risk analysis results in the earlier phase. Since risk evaluation based on organizational objectives, external and internal context and stakeholders' views, NGT is promising for effective results. This study not only contributing to the prioritizing list of risks and threats in a systematical manner but indirectly NGT process makes stakeholders aware of the current cloud security risk situation in the organization. Equal opportunity expressing views in this focus group discussion is hope can generate a brilliant solution in risk assessment results.**

Keywords— **cloud computing; risk assessment; nominal group technique; STRIDE-DREAD model; risk evaluation.**

I. Introduction

A survey report from Economist Intelligence Unit in 2015 reveals that cloud computing penetration in healthcare is the lowest among the industries with only 31% of pervasive presence. This is compared to retail 57%, banking 51%, manufacturing 42% and education 34% accordingly [1]. Healthcare differs from other industries as this sector is highly regulated, prune to risk, medical error and involvement internal and external party in day to day process.

Most hospital infrastructures in Malaysia are device-centric, where single workstation installed and required service or system deploy to users accordingly [2]. Although cloud computing penetration in Malaysian healthcare still low, the previous study in the area of cloud computing risk assessment for healthcare also still low. Cloud computing brings benefits to the healthcare industry. The study shows the success of cloud medical records in the literature with the outcome that the cloud removes many deficiencies in medical data, scalability, with better security and interoperability between the health system [3]. Cloud computing reduces costs by offering resources on the network. Cloud users may access services anytime and anywhere over the Internet. However, effective risk management methodology may gain the confidence to cloud users in this technology.

Cloud computing risk assessment was studied for the first time in June 2008, by Gartner in the report titled “Assessing Security Risks of Cloud Computing.” Then followed by Cloud Security Alliance (CSA) in 2009, promoting cloud computing best practice with the release of “Security Guidance for Critical Areas of Focus in Cloud Computing”[4]. Although cloud computing technology prominently getting attention to industries, research in cloud computing risk assessment still limited, and organization is facing difficulties in identifying and evaluating security risks to their operations [5].

Identifying security risk in cloud computing is a complex task [6], [7]. Even the accuracy of the evaluation also results arguably amongst the scholar [4]. The current method in the literature is not comprehensive enough [8] [9] and the use of the traditional risk assessment model is not suitable for cloud computing [10].

In recent years, many risks assessment approach has been proposed. This is to tackle the complexity of the cloud risk assessment process. Adapting current standards such as the National Institute of Standard and Technology (NIST), The International Organization for Standardization (ISO) and

Federal Information Security Management ACT (FISMA) is part of an initiative to streamline the assessment process. Another suggestion pointed by scholars is to have both quantitative and qualitative methods in assessing risk.

Somehow, the involvement of cloud service providers and cloud customers also needs to be scrutinized carefully and not all cloud models required involvement both parties in every stage of assessment [7], [11], [12]. Involvement of cloud customer significant as they the one who understands the value of the asset within their organization. Participation of cloud customer in risk treatment activity also significant since the problem occurred in the organization and the same goes to the solution of the problem [13]

In the previous study, Almorsy et al. [14] using NIST and FISMAas a basis standard, this study involved cloud customers in all risk assessment processes, which might complicate the process when the number of cloud customers increased [13]. The use of the single method in this study also may result in bias and inaccuracy.

Unlike Saripalli et al. [15], this study is using Federal Information Processing Standards (FIPS) as a conceptual basis in assessing security risks in cloud computing. However, this standard does not fit in a cloud computing environment because it is assuming that the cloud owner has full control over the security management process [14]. This study also using previous literature in the risk identification process, which shall be not accurate for the current study since threat in cloud computing is evolved whereas Albakri et al. [11] proposed a security risk assessment framework based on ISO /IEC 27005 standard for SaaS model. The framework considered the involvement of cloud consumers in the risk management process. However, cloud consumers did not participate in risk treatment and acceptance which they need to decide with their assets.

No matter what, there is no right and wrong in conducting a risk assessment as, in the end, the objective is to minimize the security risk in the cloud customer and cloud service provider. In this study, we will focus on the method on every process in cloud risk assessment as we agreed that identifying security risk in cloud computing is a complicated task. Therefore, a careful selection of methods in each process is required to minimize the complexity. Since current risk assessment tools in the market may need a bit expensive or complicated to use. This study offers simplifies version of cloud risk assessment process.

II. Materials and Method

In this section, we described the risk assessment process and how the NGT adapted in the risk evaluation process. Risk management is the systematic method in identifying, analyzing, treating, and monitoring the risks. Although many standard and framework offer steps in the risk management process, mostly the process are the same. The overall steps would be context establishment, risk identification, risk analysis, risk evaluation, risk treatment, monitoring, and communication.

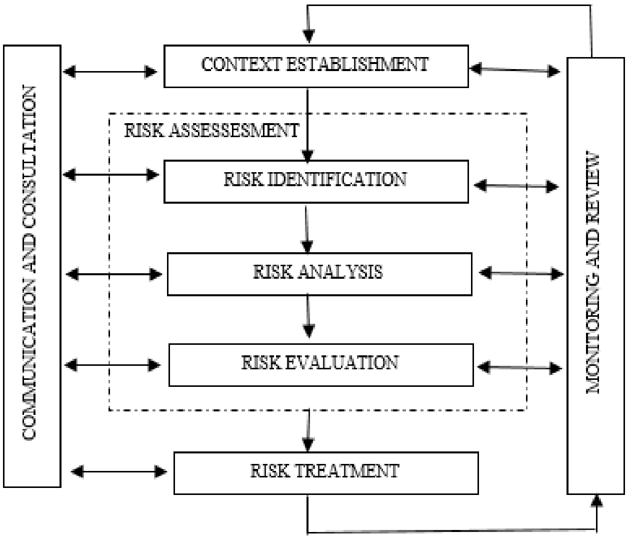

Fig. 1 Risk Management Process ISO/IEC 27005:2012 [16]

A. *Risk Assessment Process*

Risk Assessment is essential in every organization. With the implementation of risk assessment not only measure the state of security in the organization but more on the continuous process in monitoring the security of the company. Risk defines as the “combination of the probability of an event and its consequence.” Risk measured by consequences or impact and the likelihood of the event [17]. Such assessment, no matter quantitative or qualitative, requires analysis judgment, expert knowledge, and experience [18].

The risk assessment method can be defined in three categories known as rule-based, risk-based, and judgment based. The rule-based assessment method is the use of the standard collection of the system should comply. The risk-based assessment method is based on probabilities. Only empirical and statistical data from similar events are used in the assessment whereas judgment-based assessment considering unidentified threats and focus on assessing the likelihood and impact of each threat. The main factor of judgment based assessment is a subjective interpretation from the expert [19].

The risk assessment consists of three processes: risk identification, risk analysis, and risk evaluation. The general process as follow*:*

- Risk identification – It is conducted as a first process in identifying and defining a potential risk that might negatively influence the company process. The goal of risk identification is to determine what cause of potential loss, why, where and how the loss happen. Risk identification involves historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.
- Risk analysis - It is a process to comprehend the nature of risk and to determine the level of risk. The goal of risk analysis is to understand the nature of risk. In this process, the values of the likelihood and consequences of risk will be assigned accordingly. Generally, the methodology used in analyzing risk depends on vulnerabilities or incidents. The methodology includes quantitative, qualitative, or a

combination of both methods. The quantitative method relies on formula and calculation to the impact and likelihood of risk; in contrast, the qualitative method analyses risk in the events of numerical measure challenging to express [20].

- Risk evaluation -It is a process of comparing the results of risk analysis with risk criteria to determine whether the risk is acceptable or tolerable. The goal is to compare risk levels assembled in the risk analysis with risk acceptance by the company. Risk criteria usually based on organizational objectives, external and internal context, and stakeholders' views. Risk evaluation uses the understanding that risk results in a risk analysis will decide on future actions. [16]
- Risk treatment – A list prioritized in risk evaluation criteria may lead to the treatment options, whether the decision to reduce, retain, avoid, or share the risk will be selected in this process.

At the first step of this study, we determined the risk context by interviewing a few respondents from the various hospital in Klang Valley. We called up a few hospitals selected to confirmed the usage of cloud computing. Document reviews for the security control and incident report are collected during the interview. For the second step, we identify vulnerabilities and threat base on risk criteria. Risks are categorized based on the Microsoft STRIDE model. The details categorize as below:

TABLE I
CORRELATION BETWEEN STRIDE MODEL AND CLOUD ENVIRONMENT [21]

Threat Categories	**Cloud Security**
Spoofing attempting to gain access into a system using a false identity	An attacker using others username and password to access data in the cloud
Tampering Unauthorized modification of data.	Attacker modifying data on the cloud without user knowledge or permission.
Repudiation The ability of users to deny any actions or transactions performed either legitimate users or non-legitimate users.	It is an illegal operation by an authorized user in a multitenant environment due to a system lacking to trace the prohibited action.
Information Disclosure Unwanted disclosure of private data.	Accessing co-tenant workflow without authorization by a malicious insider or cloud user.
Denial of service Process of making system or service unavailable.	Controlling virtual machines or making web servers offline by an attacker or cloud user.
Elevation of privilege Occurs when authorization permissions beyond initially granted for those users to compromise or destroy the system	Accessing all system defenses project as a trusted system by cloud user or attacker

In the third step, risk evaluation-based Microsoft DREAD model to compute and prioritize risk value. The DREAD model is based on linguistic variables. Therefore, it is more meaningful for hospital respondent to perform voting and ranking during the NGT process The category is explained below [21]:

- Damage potential- extent of damage
  (How much damage is caused when a threat occurs?)
- Reproducibility- How often an effort required to reproduce attacks works.
  (How fast/easy to reproduce the data once threat exploited?)
- Exploitability- Value of effort required to exploit the threat
  (What is required to exploit this threat?)
- Affected users- Estimation of affected if exploit widely available.
  (How many users will be interrupted or affected?)
- Discoverability- Measure the level of vulnerability to be discovered.
  (How easy to discover the existence of threat in the cloud?)

Table 2 below is the value and range to be used in NGT.

TABLE II
LINGUISTIC VARIABLES AND RANGE IN DREAD [22]

	Linguistic value and range				
	1-2	3-4	5-6	7-8	9-10
Damage Potential	Negligence	Slight	Moderate	Almost	Catastrophic
Reproducibility	Probably	Likelihood	Satisfy	Critical	Vital
Exploitability	Least	Slight	Moderate	Almost	Extreme
Affected users	Noticeable	Satisfactory	Average	Disturbing	Unbearable
Discoverability	Least	Slight	Moderate	Almost	Extreme

The overall process in this study can be seen in Fig. 2 below:

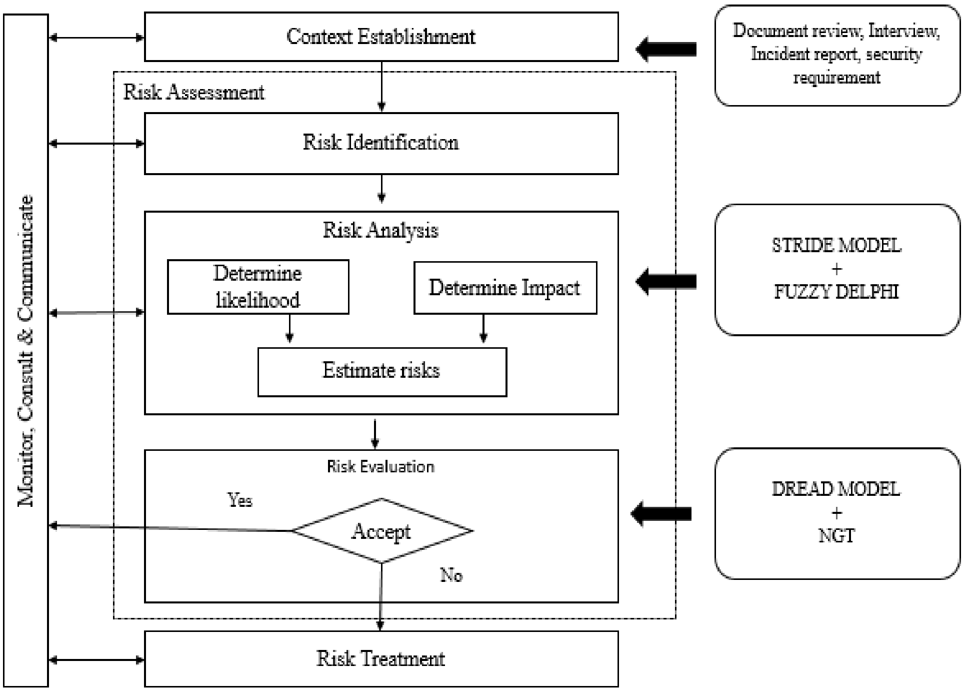

Fig. 2 Risk management process

B. Adapting NGT

NGT has been used widely in healthcare setting, especially to develop guidelines, explore opinions among health professionals and to compare views [23].NGT is an approach for decision making whereby participants having an equal opportunity to express a view and to influence decisions that are made [24]. This technique was designed by Delbecq and Van de Ven in 1975.

Commonly in NGT, includes two main stages, namely focus group discussion and voting session. NGT key features is a structured face-to-face meeting. Direct participant involvement is required and they have an equal voice and validity towards the posed questions. The generation of ideas takes place in silence, with no conferring and no seeking elucidation or explanation from the researchers. The main advantages of this technique are the equal opportunity to contribute their ideas by minimizing the domination of confident or outspoken participants, whereas commitment of time and the necessity to attend to a specific location of meeting may reduce the participant intention to take part [24].

In the risk evaluation phase, NGT process proposed in this study is adapting from Evans et al. [24], There are five phases as below:

1) *Opening statement: Introduction and explanation*

- Opening statement.
- Present risk analysis result. A list of assessed consequences, Likelihood of incident scenario, and list of risks with value level assigned.
- A copy of risk analysis result distributes to participants for the next task

2) *A silent generation of ideas*

- The participant will be given 15 minutes to read and understand the result of risk analysis.
- Issue blank paper for each participant
- To prevent advocating and influencing other participants, no discussion allows in this task.
- Participants are required to write down their feedback on the risk analysis result and the rank of risk in the result. Blank papers are to be used for any feedback that differs from the list presented.

3) *Round robin technique*

- Participants are invited to share their feedback from the previous task
- All comments and ideas are recorded during this task.

4) *Clarification of ideas*

- All participants can clarify and discuss any unclear items in this session.
- The facilitators collect all feedback written earlier by participants.

5) *Voting and ranking*

- In this task, each participant is required to vote and rank the list of risks based on earlier discussion.
- The meeting end while the final rank of each risk finalizes by participants collated.

Since NGT is the focus group discussion, proper meeting room enough to allocate participants in one time is required. Flip charts and stationery such as pen, pencil, and papers are an essential item to be used in this NGT. In the opening statement process, there are four main tasks will be performed and this is adapting from Dang et al. [25]:

- A warm welcome to all participants and explain the purposes of the focus group and the importance of every task in this session.
- Introducing the role of each participant and the importance of the participant's contribution to every task.
- Moderator presents the guidelines of NGT process and makes participant understand their role
- Explain the indication of how the output from NGT will be used

The selection of experts in the consensus method study is from the background of people who know about the topic of concern. Although NGT commonly select laypeople. In most cases, power differentiates people's contributions to this technique. Hence, participants in NGT relatively homogeneous [26].

On the optimal size of the group in NGT, by referring to the previous researcher, Harvey and Holmes [27] suggested that a group between 6 and 12 would be sufficient. This suggestion being supported by Dang [25], with six key stakeholders. Whereas Evans, [24] in her study involving 14 stakeholders in exploring risk in mental healthcare. Although many studies involved the small number of participants, Mc Millan [26] in his study analyzing 26 multiple groups ranging from two up to fourteen participants in the groups. Analyzing multiple groups are involved, and thematic analysis is needed when comparing participant's priorities across the group. In this study, three groups from three different hospitals, stakeholders, and IT workers will be employed, ranging from three to six participants in each group.

III. Results and Discussion

In this section, the researchers describe the implementation of the risk evaluation phase. The benefit of using this method and the accuracy of risk evaluation results are also discussed. There are some reasons why NGT is suitable to be used in the risk evaluation process. Firstly, involving participants from healthcare in the structured face-to-face meeting, enabled reliable and first-hand information to be obtained in real day to day healthcare operational.

Secondly, NGT is time-efficient for researchers; in the meeting, it provides an opportunity to acquire a substantial amount of information in a short time. NGT also easy to be conducted with the minimum time taken and the venue will be in the participant location area which encourages the relaxed and sharing atmosphere.

Thirdly, the equal voice of participants ensures the dominant participant did not control the whole process. Hence, creating a conducive meeting environment and initiation of changing idea.

In summary advantages and disadvantages are using NGT[25]. The advantages are as follows:

- The higher number of ideas compared to other group processes
- Generate more creative ideas compare to other group processes
- The simplicity of interpreting the results since the idea is generated, ranked and evaluated, at the session itself
- Minimal resources required
- Less time is taken

The disadvantages are as follows:

- Minimal issues covered in the session
- Limitation idea generation
- Lack of anonymity limit the participants to express their idea
- The necessity to attend a specific location may limit the participant number

Concerning the disadvantages or limitations of NGT, Huge et al. [28] commented that the success of this method depending on the goodwill of stakeholders and the more significant number of participants, the smaller the role for each participant

IV. Conclusions

Current risk assessment tools in the market may need a bit expensive or complicated to use and the scholar agreed that the cloud risk assessment process is complicated. Therefore, this study offer simplifies version of cloud risk assessment process. Since risk evaluation is based on the result of risk analysis. It is essential to compare the risk analysis result with acceptance or tolerability of risk for risk treatment purposes. Therefore, the use of NGT in this evaluation process is necessary since it involves stakeholders' views. This study contributes to prioritize the list of threats and risks in cloud risk assessment. In addition, bringing the participation of healthcare stakeholders in understanding risk assessment issues and mitigating process. Since this method is easy to adapt, it is expected that this study may give some light in minimizing the complexity issue in assessing cloud computing risks.

Acknowledgment

The authors would like to thank Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia (UTM), for the resources and support.

References

[1] Intelligence Unit, "Ascending Cloud The adoption of cloud computing in five industries," Econ., 2016.

[2] K. A. Ratnam and P. D. D. Dominic, "Adoption of cloud computing to enhance the healthcare services in Malaysia," in 2014 International Conference on Computer and Information Sciences, ICCOINS 2014 - A Conference of World Engineering, Science and Technology Congress, ESTCON 2014 - Proceedings, 2014.

[3] F. Sadoughi and L. Erfannia, "Health information system in a cloud computing context," Stud. Health Technol. Inform., vol. 236, no. 6, pp. 290–297, 2017.

[4] H. Tang, J. Yang, X. Wang, and Q. Zhou, "A Research for Cloud Computing Security Risk Assessment," Open Cybern. Syst. J., vol. 10, 2017.

[5] B. M. Dioubate, N. N. A. Molok, S. Talib, and A. O. M. Tap, "Risk assessment model for organizational information security," ARPN J. Eng. Appl. Sci., vol. 10, no. 23, pp. 17607–17613, 2015.

[6] F. M. M. Alturkistani and A. Z. Z. Emam, "A review of security risk assessment methods in cloud computing," in Advances in Intelligent Systems and Computing, 2014, vol. 1, pp. 443–453.

[7] T. K. Damenu, "Cloud Security Risk Management - A critical Review," 2015.

[8] A. Ali, D. Warren, and L. Mathiassen, “Cloud-based business services innovation: A risk management model,” Int. J. Inf. Manage., vol. 37, no. 6, pp. 639–649, 2017.

[9] S. Drissi, S. Benhadou, and H. Medromi, “A new shared and comprehensive tool of cloud computing security risk assessment,” Lect. Notes Electr. Eng., vol. 366, no. January 2016, pp. 155–167, 2016.

[10] M. Nada and B. Youssef, “Survey: Risk assessment models for cloud computing : evaluation criteria,” in Cloud Computing Technologies and Applications (CloudTech), 2017 3rd International Conference of, 2017, vol. 1, pp. 3–7.

[11] S. H. Albakri, B. Shanmugam, G. N. Samy, N. B. Idris, and A. Ahmed, “Security risk assessment framework for cloud computing environments,” Secur. Commun. Networks, 2014.

[12] R. Latif, H. Abbas, S. Assar, and Q. Ali, “Cloud computing risk assessment: A systematic literature review,” in Lecture Notes in Electrical Engineering, 2014.

[13] R. Alosaimi and M. Alnuem, “Risk Management Framework for Cloud Computing : A Critical Review,” Int. J. Comput. Sci. Inf. Technol., vol. 8, no. 4, pp. 01–11, 2016.

[14] M. Almorsy, J. Grundy, and A. S. Ibrahim, “Collaboration-based cloud computing security management framework,” Proc. - 2011 IEEE 4th Int. Conf. Cloud Comput. CLOUD 2011, pp. 364–371, 2011.

[15] P. Saripalli and B. Walters, “QUIRC: A quantitative impact and risk assessment framework for cloud security,” in Proceedings - 2010 IEEE 3rd International Conference on Cloud Computing, CLOUD 2010, 2010.

[16] MS ISO/IEC 27005:2012 Information technology -- Security techniques -- Information security risk management. 2012.

[17] K. Djemame, D. Armstrong, J. Guitart, and M. Macias, “A Risk Assessment Framework for Cloud Computing,” IEEE Trans. Cloud Comput., 2016.

[18] J. Li, Y. Bai, and N. Zaman, “A fuzzy modeling approach for risk-based access control in eHealth cloud,” Proc. - 12th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2013, pp. 17–23, 2013.

[19] G. Stergiopoulos, V. Kouktzoglou, M. Theocharidou, and D. Gritzalis, “A process-based dependency risk analysis methodology for critical infrastructures,” Int. J. Crit. Infrastructures, 2017.

[20] M. H. Drissi S. Houmani H., “Survey: Risk Assessment for Cloud Computing,” Int. J. Adv. Comput. Sci. Appl., vol. 4, no. 12, pp. 143–148, 2013.

[21] P. Anand, J. Ryoo, H. Kim, and E. Kim, “Threat assessment in the cloud environment - A quantitative approach for security pattern selection,” in ACM IMCOM 2016: Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication, 2016.

[22] A. Singhal and H. Banati, “Fuzzy Logic Approach for Threat Prioritization in Agile Security Framework using DREAD Model,” vol. 8, no. 4, pp. 182–190, 2011.

[23] S. S. McMillan, M. King, and M. P. Tully, “How to use the nominal group and Delphi techniques,” Int. J. Clin. Pharm., Feb. 2016.

[24] N. Evans et al., “Using the nominal group technique to involve young people in an evidence synthesis which explored ‘risk’ in inpatient mental healthcare,” Res. Involv. Engagem., 2017.

[25] V. H. Dang, “The Use of Nominal Group Technique: Case Study in Vietnam,” World J. Educ., vol. 5, no. 4, 2015.

[26] S. S. McMillan et al., “Using the Nominal Group Technique: how to analyse across multiple groups,” Heal. Serv. Outcomes Res. Methodol., vol. 14, no. 3, pp. 92–108, 2014.

[27] N. Harvey and C. A. Holmes, “Nominal group technique: An effective method for obtaining group consensus,” Int. J. Nurs. Pract., 2012.

[28] J. Hugé and N. Mukherjee, “The nominal group technique in ecology & conservation: Application and challenges,” Methods Ecol. Evol., vol. 9, no. 1, pp. 33–41, 2018.