Shields up

Ensuring digital duty of care for Myanmar researchers

October 2025

By DigiSec Lab

— KNOWLEDGE FOR —
K4DM
DEMOCRACY MYANMAR

MYANMAR DIGITAL RESEARCH 27

Acknowledgment

This study was conducted by DigiSec Lab, a non-profit that helps at-risk organizations in Myanmar manage digital threats, build resilience and strengthen their security practices. The team is a long-term trusted partner of The SecDev Foundation.

This paper is the last of 27 research projects coordinated by The SecDev Foundation for the Knowledge for Democracy Myanmar (K4DM) initiative, with a grant from the International Development Research Centre (IDRC). This study specifically evaluates efforts made to ensure the digital safety of the researchers engaged in the full suite of projects.

K4DM was launched in 2017 by Global Affairs Canada and IDRC. It nurtures a new generation of young actors to promote inclusion, gender equality, respect for diversity, and prosperity for all in Myanmar. Making use of online courses, fellowships and research on digital spaces, the initiative supports diverse students and researchers primarily in the Myanmar diaspora and research institutions outside the country.

Abstract

This paper examines how a digital safety framework, the Risk Assessment and Mitigation Plan (RAMP), helped protect Myanmar researchers working under threats of surveillance, censorship, and violence. Developed by DigiSec Lab, RAMP provided practical tools and training to integrate digital security into research design and practice. Between 2023 and 2025, it was applied across 27 projects coordinated by The SecDev Foundation for the Knowledge for Democracy Myanmar initiative. Drawing on survey responses, submitted RAMP plans, and five case studies, the study shows that RAMP strengthened researchers' ability to recognize risks, adopt safer communication and data storage practices, and protect participants.

Findings highlight that while most researchers avoided major security incidents, challenges remained—particularly around digital literacy, tailoring support to project contexts, and simplifying the risk assessment process. The evidence is clear: digital safety cannot be left to individual initiative. International funders who support research in conflict and authoritarian settings have a duty of care to provide structured, ongoing digital protection as part of responsible funding. The Myanmar experience shows this is both feasible and effective—and should be treated as a baseline standard, not an optional safeguard

Contents

Introduction

The February 2021 military coup in Myanmar sparked street protests, civil disobedience and an armed resistance that continues today. The coup erased years of social, political and economic progress. Amongst the many sectors of society affected: *social researchers,* who had just begun in the period after 2015 to make an impact on Myanmar's public policy process.

As a result of the coup and subsequent crackdowns, social research in Myanmar has become much more difficult, and much riskier. With increasing surveillance and the criminalization of digital activities in Myanmar, even online research poses risks to both the researchers and their research participants and other stakeholders. In this environment, Canada's International Development Research Centre (IDRC) was supporting policy researchers under a long-standing initiative called Knowledge for Democracy Myanmar (K4DM). As one part of the K4DM initiative, The SecDev Foundation, a Canadian organization focused on digital safety, was tasked with implementing a model for "safe social research" in a conflict zone, allowing Myanmar scholars to continue important policy-focused research at a time when their community and beneficiaries face a direct existential threat from the military and its supporters.

To find a way forward that respects the duty of care to avoid or minimize risk to research stakeholders, the DigiSec Lab team, composed of Myanmar digital safety experts, developed a Risk Assessment and Mitigation Plan (RAMP) as a simple, practical method for Myanmar researchers to integrate digital security concerns into their methodology designs and in the conduct of their research. Over a period stretching from mid-2023 to mid-2025, the RAMP process was carried out with 27 research teams in two rounds, reaching about 60 researchers. All the researchers were drawn from the 27 teams receiving grants from The SecDev Foundation, as part of the K4DM initiative.

This paper examines the risk assessment mitigation plan experience, drawing on a survey and discussions with over 20 researchers. The DigiSec Lab team believes the RAMP method, grounded in the 'do no harm' principle, ensures much greater safety for all involved, particularly in high-conflict areas like Myanmar. RAMP can be applied to various social projects, such as research, advocacy, events, and training—making this summary and discussion of the approach relevant for civil society groups working in a broad range of areas.

The RAMP process began as teams finalized their methodology, and before they carried out literature reviews and field work. The process started with a review of each group's initial safety plan, followed by a three-hour interactive online training session. During this training, researchers were introduced to RAMP, select digital safety tools, and the RAMP template—a type of checklist that gave each risk area a colour-coded level, with corresponding mitigations. Each team then completed and submitted their customized RAMP template, outlining research project activities, the risks these activities might encounter, and the mitigation strategies to be used for each activity. The DigiSec Lab team reviewed these submissions and provided feedback in writing or through Zoom meetings, depending on availability.

Digital security is a relatively new but essential aspect of undertaking research in Myanmar's high-risk environment. This study not only aims to provide valuable insights for improving RAMP support to researchers, but also to demonstrate to donors and other stakeholders the importance of integrating digital safety into project design *from initiation*, rather than as a second thought after project work has begun.

Methodology

This research used a triangulation approach that combined survey research, document review and case studies, to ensure the validity of findings and provide a solid basis for discussion.

For the survey collection, the research team developed a structured questionnaire with three sections, using Likert scale, multiple choice and a few open-ended questions. The first section collected the demographic information of the participants including age, gender, ethnicity, and their geographic location. In the second section, the questions focused on the clarity and effectiveness of the overall training, and the usefulness of the hands-on sharing of digital security tools. In the third section, the participants were asked specifically about the RAMP template including its ease, usefulness, and whether they experienced or mitigated any perceived or unexpected risks identified in the template. In the last section, the survey was concluded with the collection of opinions on the integration of RAMP training in future research projects and their suggestions for improvement.

Meanwhile, the document review and case study analysis were also conducted. The research team reviewed the submitted RAMP template from Batch 1 and Batch 2 researchers (as there were two rounds of research grants issued), assessing the improvement of their safety plan before and after the RAMP support. Then, six research projects were selected for case studies, representing a range of detailed and less-detailed plans, high-risk and low-risk projects, and qualitative and quantitative research groups. The research team conducted one-on-one interviews with the six selected groups to evaluate the practical implementation, relevance, and usefulness of RAMP measures, as well as any incidents that occurred in each project.

The data collection was completed during March and mid-April 2025. The survey method received 16 responses, and 5 interviews were successfully conducted (one group was unable to arrange an interview time). The interviews were conducted via Zoom without opening the camera and the participants were given the option to express their real name or remain anonymous for confidentiality. The interviewer took the notes consecutively. After the data collection, the research team undertook a descriptive analysis on the survey and case study data, based on the interview notes.

Findings

Survey analysis

As noted above, the survey received 16 responses from a diverse group of participants. According to the collected data, participants are from the 26-30 and 31-40 age groups, who can be identified as early career researchers and mid-career researchers. In terms of gender, 9 respondents identified as female, followed by 6 male respondents and 1 identifying as other (non-binary). The majority ethnic group among respondents is Burmese, with a total of 7 participants. Other represented ethnicities include Rakhine (2), Chin (1), Kayin (1), Kachin (1), and Mon Chinese (1). Geographically, all participants are currently located outside of Myanmar. These demographic distributions are illustrated below.

FIGURE 1: AGE AND GENDER OF RESPONDENTS (16)

Age of respondents	
26-30:	6/16 (37.5%)
31-40:	10/16 (62.5%)

Gender of respondents	
Women	9/16 (56.3%)
Men:	6/16 (37.5%)
Other:	1/16 (6.3%)

In section 2 of the survey, participants rated their experience with the training and their assessment of the usefulness of the digital security tools introduced during the hands-on sessions. Regarding the clarity of the training, most respondents indicated that the training clearly explained the importance of digital security, with the majority giving it a rating of 4 or 5 out of 5. Similarly, the training was widely regarded as useful in providing practical digital security tools, with most participants again rating it 4 or 5, suggesting they found it actionable and relevant. The survey also found that most participants felt confident in applying the digital security tools independently in their own projects. However, one participant rated the training at the lowest scale, highlighting an opportunity for improvement in future sessions. For details, please refer to the following figures.

FIGURE 2: HOW CLEAR WAS THE TRAINING ON THE IMPORTANCE OF DIGITAL SAFETY?

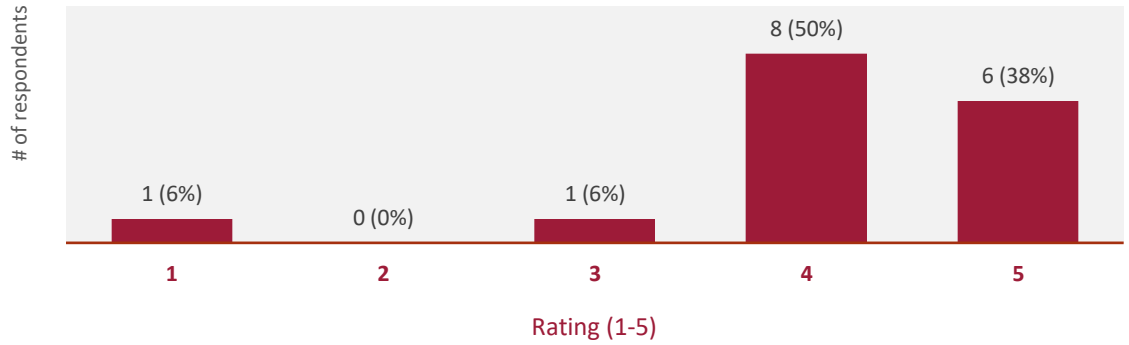


FIGURE 3: HOW USEFUL WERE THE DIGITAL SECURITY TOOLS SHARED IN THE TRAINING?

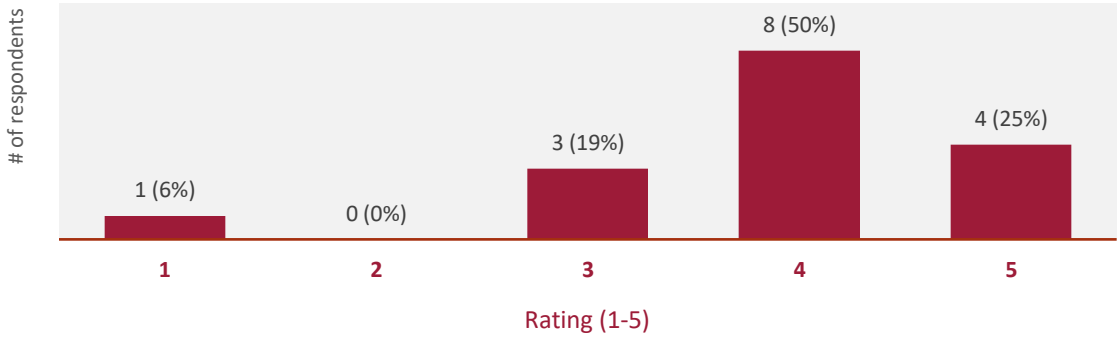
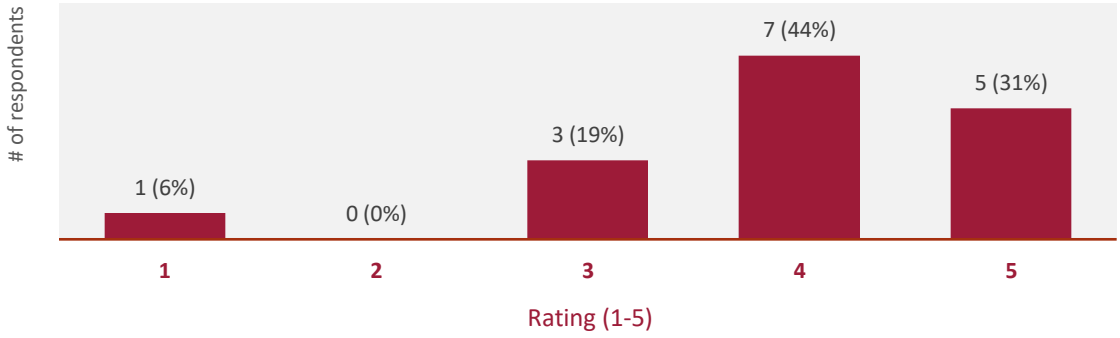
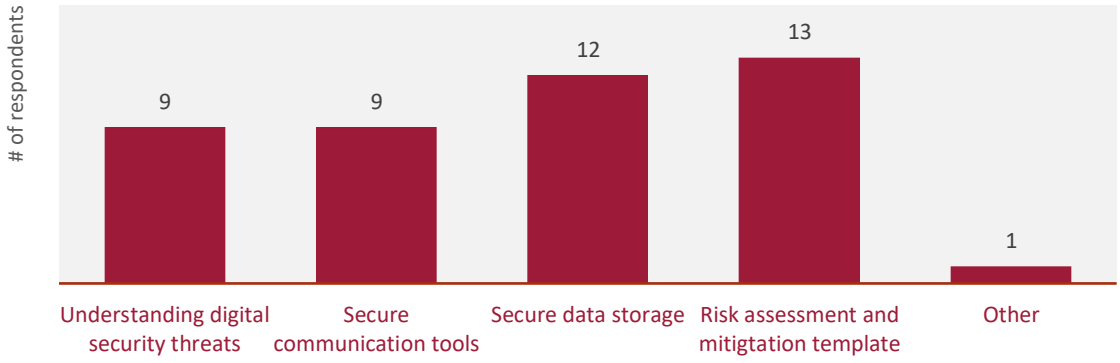


FIGURE 4: HOW CONFIDENT ARE YOU APPLYING THE TOOLS/TECHNIQUES YOU LEARNED?



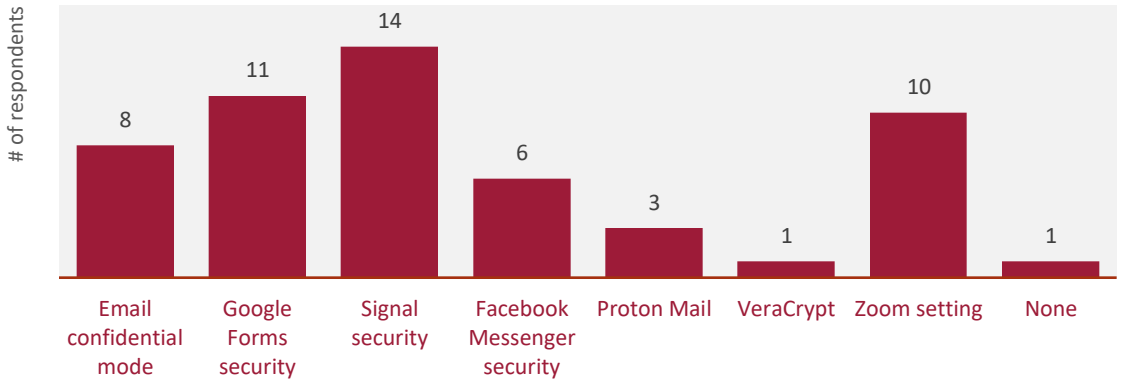
Finally, the survey dived into detailed questions on which parts of the training were beneficial to the participants and the specific tools they used in their project implementation. While the training covered four main themes, including the importance of digital security in research projects, secure communication tools, secure data storage, and how to use the RAMP template, the participants equally rated all topics as beneficial to their respective research projects (see Figure 4).

FIGURE 5: WHICH TRAINING TOPICS WERE MOST BENEFICIAL TO YOUR RESEARCH? (MULTIPLE ALLOWED)



The survey found that the hands-on training was particularly effective, as 15 out of 16 participants used the digital security tools shared during the training—ranging from using at least one to five tools or safety settings. See Figure 6 for the list of digital security tools and the number of participants who used them.

FIGURE 6: WHICH DIGITAL SECURITY TOOLS HAVE YOU CONTINUED TO USE? (MULTIPLE ALLOWED)



In Section 3 of the survey, the participants were asked about the ease and usefulness of the RAMP template for their research projects, in terms of preventing exposure to the possible risks and to mitigate the threats. Most participants found the RAMP template moderately easy to complete, with scores clustered around 3-4 out of 5. When asked how well the template helped them assess and mitigate risks, responses were positive as well, with mostly scores ranging from 3-5.

FIGURE 7: HOW EASY WAS IT TO COMPLETE THE RAMP TEMPLATE?

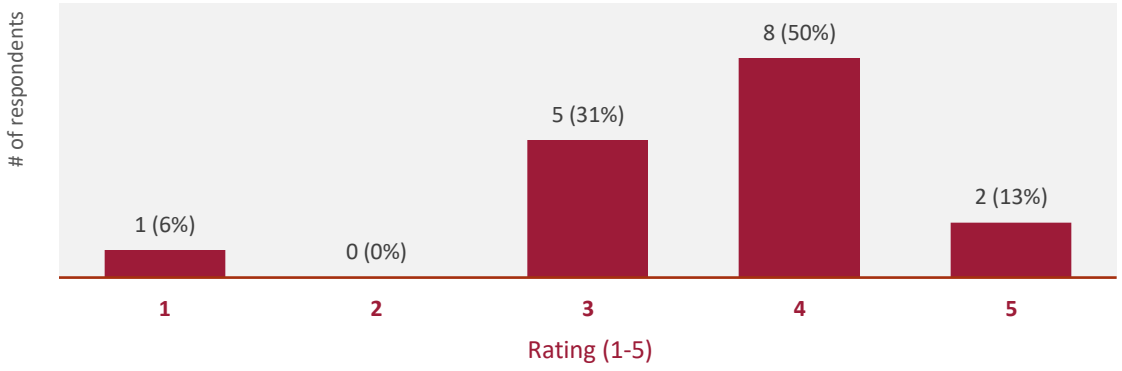
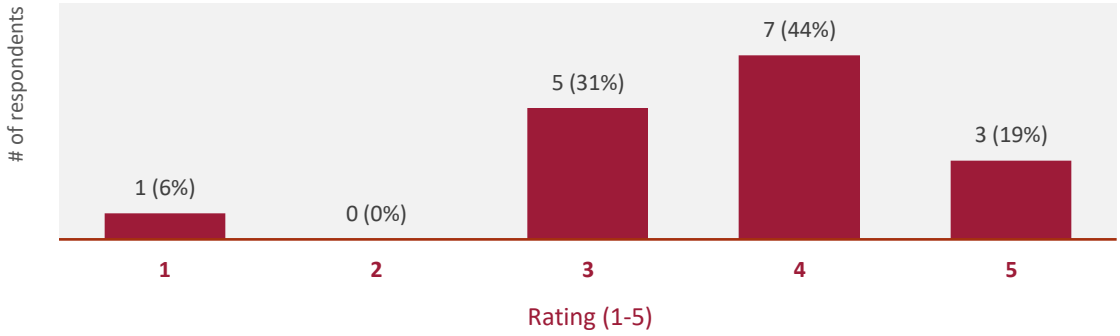
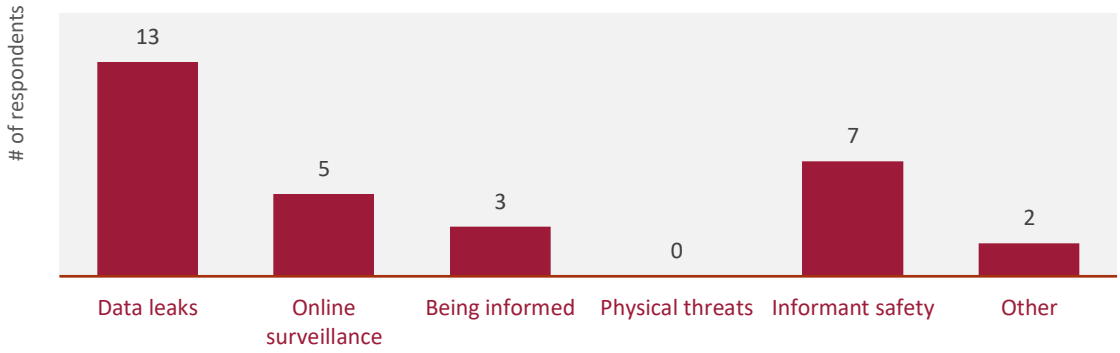


FIGURE 8: HOW WELL DID THE TEMPLATE HELP YOU ASSESS AND MITIGATE RISKS?



As part of the RAMP process, the research group was asked to fill out the RAMP template by listing the possible risks that might be encountered during the research process, and with assessing potential mitigation measures to deal with these risks. This was done before data collection began. According to the survey, the common identified risks by the research groups—regardless of methodology, research location and research participants—were data leaks, online surveillance, being informed upon, physical threats, and informant safety (see Figure 9).

FIGURE 9: WHAT WERE THE COMMON RISKS YOU IDENTIFIED? (MULTIPLE ALLOWED)



Among the researchers surveyed, only two reported security incidents during their research implementation. One said that the RAMP template helped mitigate the incident, while the other answered that it was "not supportive," and that "different research teams have varying strengths and weaknesses, so support should be tailored to their specific needs. Simply providing digital security functions will not be sufficient; a more customized approach is necessary to ensure each research team receives the support they require." This indicates that the overall training did not address the specific type of incidents, such as comprehensive informant safety risks which were identified in their RAMP, which should be taken into account when designing future training sessions. Other participants also provided suggestions and requests for future training, including topics such as data management, offline survey collection tools, and individual mentoring sessions with the team after completing the RAMP template. Overall, 15 out of 16 participants suggested that the RAMP method should be integrated into future research projects.

Case study analysis

Case study 1: Research on IDPs along the India–Myanmar Border

This case involves research on the experiences of internally displaced people (IDPs) in the India–Myanmar border region, which was conducted by a researcher residing outside of Myanmar. It demonstrates both the importance and limitations of the Risk Assessment and Mitigation Plan (RAMP) training in cross-border and non-digital research settings. Firstly, the key risk for this project was assessed as exposing the participants' personal information in the report, an understandable concern given the sensitive focus on displaced peoples. To mask interview respondents quoted in the paper, the researcher included only their age range in the final publication.

Apart from this, the researcher did not need to use many mitigations throughout the research process, due largely to their safe location in exile. However, the researcher cautioned that more rigorous risk planning would be essential if research were to take place in government-controlled areas. He acknowledged the importance of the RAMP training for local researchers by saying "I noticed that this knowledge is very useful for the local researchers, such as how to securely store information, and how to encrypt data." Accordingly, the researcher still rated the RAMP training as highly relevant for those working inside the country. The researcher completed the template and followed the recommended mitigation measures. As mentioned, most risks identified pertained to safely identifying and interacting with interview respondents. The researcher carefully chose the participants only through trusted networks and shared only required information with the participants. Here, the researcher highlighted the usefulness of the hands-on training on digital security tools. At the training, he learned that messaging platforms such as Facebook Messenger are not encrypted. He decided to use anonymous email accounts to share interview questions and related documents to the participants upon consideration of their safety. The use of Chin language in communications also was thought to help prevent surveillance and potential interception. The researchers said, "I applied some phone and online communication security practices for the participants in my research, even though there were some difficulties in applying them." However, in practical terms, the challenges were inevitable. Due to limited access to internet and electricity, some interviews had to be conducted via phone call instead of encrypted Zoom meeting according to the RAMP template.

The researcher also experienced difficulties in using certain digital security tools due to limited familiarity with digital devices. Due to his experience, he suggested including a practical session in future RAMP training, saying "It will be better if there is a practical session to test out these security tools and practices as one part of the RAMP training." He felt allowing the researchers to test and practice using different security tools for their project would help people with varying digital literacy levels. Segmenting researchers into groups based on their familiarity with IT and digital literacy would be helpful, as well as segmenting by researcher location (inside or outside Myanmar). For the RAMP template, he felt it posed no major challenges, except the difficulty of assessing participant risk, particularly related to their geographic location. Therefore, future training should explicitly differentiate risk assessment strategies for in-country versus out-of-country research participants. The researcher supported the integration of RAMP training into future research projects in Myanmar and stressed the importance of digital security skills training for researchers.

Case study 2: Research on perceptions of digital space and political activism

This case involves a research project looking at digital spaces as tools of political activism in Myanmar, which explored both public and policymaker perceptions of digital platforms in shaping Myanmar's political environment. The research used mixed methods – qualitative interviews with policymakers and a quantitative online survey with the public. Of the two methods, the research team faced greater risks with the online survey, due to the political sensitivity of the questions and the digital methods used.

The team described their effort to integrate risk management at the outset of their project, using the RAMP template: **"We identified the security risks for the research team and also the risks of the participants with the help of the RAMP team at the beginning of the research."** According to their RAMP exercise, there were no direct physical threats to the researchers, however, potential public mistrust was a key barrier (to gaining online survey participants). Many potential respondents suspected the team of being linked to the military government (SAC): **"We have encountered difficulties to collect samples based on the perception from the public participants, as they thought that we are from the SAC."** The team shared their experience with this difficulty, which shows the need to consider not only technical vulnerabilities but also perceptual and reputation risks in politically sensitive contexts.

Despite these challenges, the team highlighted that the digital security training and RAMP template was supportive to mitigate the pre-assessed risks and help them navigate through these difficulties. While the team was already familiar with some digital security practices, the training helped them adopt new and more structured protocols. According to the interview, one of the core lessons was the importance of separating personal and research communications. They said: **"We can be more secure by not using personal emails for the communication of the research."** To mitigate risk, the team created **separate research emails** and applied VPNs and pseudonymous communication strategies. Yet, some security measures were difficult to implement due to technical limitations or unfamiliarity: **"There are one or two things that we can do by ourselves among five (identified) security protocols, but we didn't know how to change the settings in Gmail to ensure our security."** This illustrates that adapting these solutions depended more on team capacity than the quality of RAMP recommendations.

The team said they were cautious in dealing with the potential risks assessed in the RAMP process, and they strictly followed the mitigation strategies. Due to the sensitivity of the research topic and the reliance on Facebook for data collection, the team adapted their data collection strategy, saying: **"We changed our target respondents who are in the areas with internet and VPN access, and we eliminated distribution of the survey through personal networks."** After changing the target audience, the researchers also worked with a low profile, conducting their research discreetly: **"We maintained a low profile as we were dependent on the public resources of Facebook posts and boosting."** For example, the team avoided using their personal profiles and networks to disseminate the survey to maintain a low profile and protect their identities. Consequently, the reliance on boosting page posts instead of personal networks required additional budget to achieve the desired sample.

Overall, the RAMP template was considered helpful and practical by the research team. The RAMP template has two core sections including assessing potential risks and brainstorming mitigation strategies, and the team had no difficulties in following the proposed mitigations, resulting in a project with no apparent risks in practice. The interviewee said: "**The RAMP framework helped us to mitigate the pre-**

assessed risks. But we encountered incidents which are not included in the pre-assessed RAMP"—in this case, the hesitance of Myanmar citizens to join online surveys given lack of trust. However, regarding solutions, the team said their experience of adapting research methodology turned out to be more complex (dealing with a lack of trust) rather than adjusting some digital safety tools or settings.

The interviewee provided recommendations for future training, such as including multiple contingency plans (Plan A and B) and addressing non-technical risks more explicitly. They also proposed changes to the format of training delivery: **"It will be better if the training is not a full day… but divided into four or five days with 2 hours per day."** This would make it easier for all team members to participate and digest the content effectively. Nonetheless, the research team strongly endorsed the inclusion of RAMP in future projects, particularly for researchers using online methods in Myanmar's restrictive digital environment. They also proposed experience-sharing sessions between alumni who engaged RAMP training to foster peer learning and get practical experience with incidents and mitigation strategies.

Case study 3: Research on cyber scams at the Myanmar–Thailand border

This case study deals with supporting a researcher looking at cyber scams targeting migrant workers along the Myanmar–Thailand border. This research was conducted by a digital security- aware researcher with experience in both online and in-person research. Due to the sensitive nature of the research, focused on 'on-the-ground' experiences, the researcher used a mixed methods approach with an online survey and in-person interviews with the forced workers in the Myanmar–Thailand border area. The project was quite challenging and vulnerable to risks in both online and offline methods, such as physical threats in conducting interviews in border areas, and information leaks by either the researcher or the interviewees. On the digital front, risks also emerged around data leakage during online survey distribution and communication with participants.

Despite prior knowledge with digital security, the researcher attended the RAMP training twice with the intention to make sure to mitigate the high levels of risk in her project. She described the training experience as both informative and applicable, saying: "**The RAMP training includes not only what I have already learned before training but also the new things such as risk metric table references."** Initially, using the RAMP template was challenging for her due to being unfamiliar with the risk matrix tool. She reported that the practice of using it repeatedly was needed, and it became easier over time. Eventually, she appreciated the usefulness of that risk metric table, saying: "I can identify risk levels by assessing and matching the likelihood and consequences. For example, if the risk level is high, I can be aware of the potential impact and plan for the mitigation of that risk." The measurement of risk level by considering the likelihood and consequences (impact of the risk) was found to be helpful for implementing the risk mitigation strategy.

In addition to that, the researcher reinforced that threat assessment stood out as particularly valuable among the components of the RAMP framework. The research noted: "**For me, threat assessment is the most useful part… it will become easier for me to plan mitigations after threat analysis.**" This was relevant to her project context given the geopolitical complexities of the Myanmar–Thailand border. In this case, the researcher was already well-equipped with security tools and faced no particular difficulty in adopting the RAMP recommended digital practices. She said: "**There were no challenges in using security tools and**

practices, such as encrypted community channels, as I am familiar with digital security." This illustrates that having prior knowledge on digital literacy serves as a good foundation for effectively using RAMP and implementing mitigation strategies.

This researcher was the recipient of two grants, one in each round of applications. The RAMP training led to significant changes in the researcher's digital practices the first time. In an earlier study on the digital economy in Rakhine State, she initially planned to contact interviewees via Facebook Messenger. However, following the RAMP training, she shifted to using encrypted messaging apps. "In the RAMP training, I've learned how to secure the online messaging conversation through secured communication channels, how to encrypt data, information, and communications to avoid the doxing and other security risks. Then, I've changed the survey channel from social media to Signal or Telegram, secured messaging apps." For in-person interviews, she reached out only through trusted networks and communicated via secure channels. In this way, the researcher shared her experience highlighting how specific lessons from the training altered her data collection methods.

As a result, despite potential physical threats and information leaks, no security incidents were reported. She emphasized: "There could be a security incident, possibly information leaks, if I did not use a secure communication channel and disappearing messages." Overall, her experience with RAMP templates was positive, and the researcher recommended more practical and accessible guidance within the RAMP training materials. Firstly, she suggested changing the format style to put the descriptions of the risk levels in a separate section, not in the comment section. Secondly, training lessons should be more comprehensive and specific to their research projects rather than general information, and she advocated for one-on-one consultation opportunities in addition to group training. Lastly, the researcher strongly supported integrating RAMP into future research efforts in Myanmar. Assessing risk is important for not only the research but also other projects underway in areas of ongoing political instability.

Case study 4: Research on masculinity narratives of armed resistance groups

This case study analyzes a research project which explored the masculinity narratives of newly emerged armed resistance groups, the People's Defense Forces (PDFs), during the 2021 Spring Revolution. The research was conducted through digital media monitoring, primarily of social media Pages of the PDFs and interviews with gender activists, experts, and PDF members in leadership roles. This case study shed a light on the critical role of the RAMP framework for a risk-aware research process in a politically sensitive, yet relatively low-risk digital environment.

The researcher shared the context of their project in which the topic was highly sensitive, so they designed the research methods to minimize risk. To probe the masculinity narratives, the media monitoring was conducted which did not involve direct interactions or fieldwork. However, challenges were still encountered because the targeted PDF Pages were only active in the beginning and later became inactive or had little engagement. It makes it difficult for the team to get enough data to validate. On the other hand, conducting interviews was manageable due to the researcher's existing relationships with many of the participants.

In this context, the researcher found the RAMP training as highly beneficial in designing the project which prioritized safety and minimized exposure to digital and physical threats. She actively joined the training

and applied the RAMP template throughout the research process to identify, evaluate, and mitigate potential risks. The researcher particularly valued learning how to assess the impact level of potential risks and found the mitigation planning component of the training practical and realistic. She emphasized "**Without a well-structured risk mitigation plan, there will be some challenges in an ever-changing world even how well we can identify the risks."** It is noticeable that having a written risk mitigation plan is crucial to mitigate the pre-assessed risks but also to adapt to new or emerging threats.

Beyond the project, she remarked that the training helped her to be more conscious of personal digital security. After the training, she avoided using public Wi-Fi and ensured secure communication channels. In applying the RAMP template, the team had no major challenges, but one difficulty was discussed. She found it challenging to identify the risk level with an exact number, assigning numerical values for likelihood and impact. In this regard, having one-on-one consultations with the RAMP team was supportive for them: **The feedback from the team gives more clarity. If there is no assistance in the process, some can be wrongly identified, and the outcomes would be different**." The researcher acknowledged that without such guidance, it would have been difficult to complete the template accurately.

Despite that, the training helped the research team adopt secure practices in both data storage and communication, such as managing how social media data was collected and how interview information was stored and shared. In this regard, the researcher requested funding support followed by technical training. Particularly, according to the training's recommendation to use paid subscription for secured data storage, she suggested that the researchers need both technical and financial support to follow the secured guidelines. Finally, the researcher emphasized the critical role of RAMP training for the research projects and recommended expanding future training for the researchers.

Case study 5: Research on counter-narratives and GBV in Myanmar

This case study looks at a research project titled "Debunking Myths: The Use of Counter Narratives to Fight Against Gender-Based Violence in Myanmar." The research used a text-based review of social media content to analyze counter-narratives to gender-based violence (GBV). As it employed only content reviewed on one social media platform, Facebook, it was considered low risk due to its digital and non-interactive context.

Still, the researcher shared her experience with the training and RAMP template, describing it as effective and relevant, despite the project's low sensitivity. Particularly, the template helped the team systematically assess internal and operational risks, even though the research did not involve fieldwork or direct interviews. It was a useful tool for them to identify hidden vulnerabilities such as secure data storage and internal communication among the team members. Before the training, they were not aware of the potential risks in these aspects.

This team primarily used the RAMP template for the internal risk assessment and had no difficulty completing the template. The researcher emphasized the importance of the RAMP template in mitigating risk by developing alternative plans, saying: "**The RAMP template is very useful for planning the alternative options of the research, especially for informal discussion and internal risk.**" Even though their team did not have to modify the methodology, she recommended other researchers to use the template to help identify risks, evaluate consequences and develop alternative methods if needed. Significantly,

the RAMP template helped them with digital content management. As their primary data is from social media content, the team experienced that comments or other content on social media is often deleted shortly after being posted. Therefore, the team needed a comprehensive data storage plan, where the RAMP training already covered most of the topics related to secure data storage and digital security. Even though there were no security incidents during the project, the researcher expressed her confidence that the RAMP training had adequately prepared them to address any potential risks. At last, the researcher strongly recommended to integrate RAMP into future research projects because normally researchers are just focused on data collection and analysis, but less careful with data storage. Therefore, the RAMP training was important to increase awareness of the digital risks among the researchers.

Conclusion

This research on RAMP effectiveness based on survey data and in-depth case study analysis provides valuable insights into the implementation of RAMP training among Myanmar researchers. The findings explicitly demonstrate that the RAMP template has become a vital framework for assessing and mitigating digital and physical risks in the current time of great political sensitivity. Yet, the training and support can be further strengthened as a better overall tool to support diverse researcher needs and evolving risk contexts.

Key insights from the survey and case studies:

1. **Acknowledgement of RAMP usefulness across different contexts:** In both survey respondents and case study interviews, most of the participants shared the common experience with RAMP as relevant and practical for their different types of research.
2. **Challenges in using RAMP template:** A few participants raised the recurring challenge of identifying the risk level using the numerical form, instead suggesting a Likert scale to make it easy and clear. Some also suggested including the description of risk level explicitly, not hidden in the comments.
3. **Request for hands-on training:** The majority of participants, especially from case study analysis, emphasized the need for more hands-on practice with digital security tools. Live demonstrations or guided simulations on setting up secure messaging apps, encryption tools, and secure data storage were highly requested, especially for researchers without prior knowledge or digital literacy.
4. **One-on-one consultation support:** The participants stressed the critical role of one-on-one consultation to get feedback and discuss further after the training. Due to the varying level of risks and sensitivity of research projects, they felt that one-on-one consultation would help them to get concrete guidance on how to refine their RAMP templates, clarify risk levels, or surmount technical barriers.
5. **Positive experience, with no major security incidents reported:** Overall, no participants reported serious security incidents throughout their research project, which we may attribute to their familiarity with digital tools and to their proactive application of risk assessing and mitigation strategies.