OVERVIEW

The 9th Session of the Staff Security Unit (SSU) Global Retreat took place from 04 to 07 November 2018 in Makati City, Philippines.

The central theme for this year’s Global Retreat is “Managing Staff Safety and Security Through the Use of Technology”.

The programme of the Global Retreat outlined four sub-themes: the Security Environment and Technological Achievements; Operational Understanding on Data Protection and Robust Emergency Management; Technological Updates on Security Tools; and Policies, Capacity Building and Trainings. These sub-themes aim to expose IOM security professionals to the changes within the technological sphere that surrounds the UN Security Management System and understand its impact on support effective programme delivery in IOM. In addition to this, IOM security professionals were provided the opportunity to discuss the emerging safety and security trends worldwide and IOM-specific threats in the field.

The four-day Global Retreat consisted of presentations, panel discussions, group activities and simulation exercises. This year’s event gathered 52 participants: 7 from Asia and the Pacific, 5 from Middle East and North Africa, 5 from Central and West Africa, 4 from Europe and Central Asia, 5 from East Africa, 4 from Central and North America and the Caribbean/South America, 5 from Geneva, Switzerland – IOM Headquarters, 14 from IOM Manila Administrative Centre, Manila Philippines, 3 external resource speakers from Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research Institute (CENTRIC) – Sheffield Hallam University, United Kingdom.

The retreat provided the opportunity to recognize the significance of emerging technologies and to learn how these technological trends can be applied strategically in effective risk management and enhancing staff safety and security.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLOBAL RETREAT PARTICIPANTS</td>
<td>1</td>
</tr>
<tr>
<td>WELCOME REMARKS AND GLOBAL RETREAT OVERVIEW</td>
<td>2</td>
</tr>
<tr>
<td>SSU STRATEGIC PLAN: UPDATES AND WHERE WE ARE GOING</td>
<td>2</td>
</tr>
<tr>
<td>UNDSS PHYSICAL SECURITY AWARENESS (PSA) E-TOOL</td>
<td>3</td>
</tr>
<tr>
<td>REGIONAL UPDATES: FAST FACTS</td>
<td>4</td>
</tr>
<tr>
<td>CENTRAL AND WEST AFRICA</td>
<td>4</td>
</tr>
<tr>
<td>EAST AND SOUTHERN AFRICA</td>
<td>4</td>
</tr>
<tr>
<td>EUROPE AND CENTRAL ASIA</td>
<td>5</td>
</tr>
<tr>
<td>CENTRAL AND NORTH AMERICA AND THE CARIBBEAN/SOUTH AMERICA</td>
<td>5</td>
</tr>
<tr>
<td>MIDDLE EAST AND NORTH AFRICA</td>
<td>5</td>
</tr>
<tr>
<td>ASIA AND THE PACIFIC</td>
<td>6</td>
</tr>
<tr>
<td>SCAAN UPDATES AND NEW FEATURES</td>
<td>6</td>
</tr>
<tr>
<td>IOM DATA PROTECTION POLICY</td>
<td>8</td>
</tr>
<tr>
<td>ROBUST EMERGENCY/CRISIS MANAGEMENT</td>
<td>9</td>
</tr>
<tr>
<td>T.E.S.S AND TAG</td>
<td>11</td>
</tr>
<tr>
<td>ENHANCING OPERATIONAL SUPPORT TO THE MISSION THROUGH SSU OPCEN</td>
<td>12</td>
</tr>
<tr>
<td>TECHNOLOGICAL APPROACH IN STANDARDIZING SECURITY UPDATES AND REPORTING</td>
<td>13</td>
</tr>
<tr>
<td>SCAAN TRAINING OF TRAINERS</td>
<td>15</td>
</tr>
<tr>
<td>VIRTUAL REALITY TRAINING AND CROSS-TECHNOLOGY</td>
<td>16</td>
</tr>
<tr>
<td>SSU GLOBAL COORDINATION SUPPORT AT HEADQUARTERS</td>
<td>17</td>
</tr>
<tr>
<td>UPDATES ON THE UNSMS POLICIES AND IASMN</td>
<td>18</td>
</tr>
<tr>
<td>IOM MISSION SECURITY FUNDING MECHANISM</td>
<td>19</td>
</tr>
<tr>
<td>AIR SAFETY</td>
<td>20</td>
</tr>
<tr>
<td>IOM SECURITY TRAINING: UPDATES AND FUTURE OBJECTIVES</td>
<td>21</td>
</tr>
<tr>
<td>FINAL PANEL DISCUSSION</td>
<td>23</td>
</tr>
<tr>
<td>CAPACITY BUILDING EVENTS IN CONJUNCTION WITH THE GLOBAL RETREAT</td>
<td>24</td>
</tr>
<tr>
<td>UN SECURITY CERTIFICATION PROGRAMME</td>
<td>24</td>
</tr>
<tr>
<td>UN LOCAL SECURITY ASSISTANTS COURSE</td>
<td>25</td>
</tr>
<tr>
<td>WOMEN’S SECURITY AWARENESS TRAINING</td>
<td>26</td>
</tr>
</tbody>
</table>
GLOBAL RETREAT PARTICIPANTS

Participants (sitting) left to right:
Gerardine Paguibitan, Andrea Gunning (CENTRIC), Tony Day (CENTRIC), Michael Gunning (CENTRIC), Dennis Mendiola, Amy Rhoades, William Wairoa-Harrison, Maricar Purugganan, John Williamson, Steve Mayall, and Mohamed Eltemtamy.

Participants first row (standing) left to right:
Justine Paredes, Kennelyn Alagar, Retno Palupi, Mikaela Maligaya, Chona Galang, Jessica Abigail Artehce, Nescel Robles, Lalaine Mendiola, Idette Biyo, Leilani Tubon, Jairo Parra, Fernando Da Costa Chambel, Donald Osunga, and Rusmir Krka.

Participants second row (standing) left to right:
Sileshi Mekonnen, Guillame Laurent, Dominique Bollier, Osman Aksakal, Senadin Sabaniya and Muhammad Junaid Shah.

Participants last row (standing) left to right:
DAY 1 (04 November, Sunday):
The Security Environment and Technological Achievements

The general objective of this day is to set the Global Retreat’s theme and environment by providing global and regional security overview and SSU’s achievements with its Strategic Plan, which includes SCAAN (Security Communications and Analysis Network).

The first day comprised of six sessions: The Global Retreat Overview; followed by a Country Security Briefing by IOM Philippines Field Security Officer; Updates on SSU Strategic Plan and where we are heading by SSU Director; Physical Security Unit (E-tool) by UNDSS resource speaker; Regional Updates for Central and West Africa, East Africa, Europe and Central Asia, Central and North America and the Caribbean/South America, Middle East and North Africa, and Asia and the Pacific; and Updates on SCAAN’s new features by SCAAN Community Engagement Programme Manager and team.

Welcome Remarks and Global Retreat Overview

The Director of SSU, William Wairoa-Harrison opened the Global Retreat. In his opening remarks, he provided an updated on the evolving technological trends in the global security environment, and how these ever-changing technologies will play a significant role in how IOM security professionals can be more effective Security Risk Managers. Integrating technology into how security professionals and personnel can effectively support program delivery is an enabling tool that will allow security professionals to be mobile and have access to information quickly.

The participants were asked to introduce themselves and a Security Briefing from Timothy Turner, IOM Philippines Field Security Officer (FSO) followed.

SSU Strategic Plan: Updates and Where We are Heading

William Wairoa-Harrison, Director of Staff Security Unit

An overview of the SSU Strategic Plan from 2014 to 2018 was provided by the Director of SSU. With the implementation phase from 2014 to 2016, to the consolidation phase in 2016 to 2017 and review of the plan in its final year, 2018.

With the rise of global security threats and challenges in the areas where security professionals operate, it is significant to look into technological solutions that will enhance staff safety and security. The SSU Strategic Plan for 2019 to 2021 includes a focus on integrating technological systems in the Security Risk Management Process that will provide real time data and information to effectively support IOM, its programs, staff and assets. The Strategic Plan also includes a more pro-active approach in gender inclusion in staff security management system, which includes, but not limited to, strengthening staff development and capacity building.
Key takeaways:

- The use of advanced technological tools in security means sensitive data or information is easily accessible and if measures are not in place, the unauthorized use of data or information becomes a threat, hence the need for security professionals to understand in depth the significance of data protection.

- One of the major global support services of SSU is providing and delivering in-house UN-certified training programs. IOM SSU maintains a strong relationship with UNDSS Training and Development Section (TDS) and intends to continue collaborative training programs. As of date, IOM Security Trainers network is comprised of 25 UN-certified and qualified security professionals.

- One of the organizational challenges identified during the session, was changing the culture and mindset of the organization in relation to security. As security professionals, it is important to promote security as a viable aspect of program delivery, backed up with the expertise in implementing efficient and proactive security risk management decisions.

- To empower security professionals to be more effective and efficient, training opportunities are recommended to ensure that they become certified trainers and be able to assist the SSU in the delivery of training programs in relation to staff safety and security.

UNDSS Physical Security Assessments (PSA) e-Tool:
Decio Leao, UNDSS New York - Physical Security Unit (PSU)

The UNDSS PSU Blast Expert provided a session on the Physical Security Assessment Tool that is available to UN security professionals and is accessed through the UNDSS United Nations Security Managers Information Network (UNSMIN). This e-Tool is also available on mobile, currently on Android operating system. The PSU mobile application is integrated with the Security Risk Management (SRM) e-Tool and the Safety and Security Incident Recording System (SSIRS) data for improved situational awareness and analysis.

Key takeaways:

- The UNDSS PSA e-Tool has changed the way how physical security assessments is performed in the most convenient way using mobile technology yet maintaining a comprehensive report that can be generated into a downloadable document.

- Not all participants have access to UNSMIN, the use of this e-Tool is not catered to all. Requests for country access to UNSMIN must be properly coordinated with the Regional Field Security Officers (RFSOs). The RFSOs will then verify if access is relevant for the requesting security personnel. SSU Headquarters must also be informed of these access requests for accountability reasons.

- The RFSOs must assess if the UNDSS PSA e-Tool is relevant to security personnel in their region. If so, manual processes for physical security assessments can be managed efficiently into a useful document that can capture real-time data and visual images which are easily uploaded into the UNSMIN system.
Regional Updates (Fast Facts)

The regions were divided into three groups:

1. Central and West Africa, East and Southern Africa
2. Europe and Central Asia, Central and North America and the Caribbean/South America
3. Middle East and North Africa, and Asia and the Pacific

Each region was given a maximum of 20 minutes to deliver their regional updates to the participants. Participants were also grouped into three, according the regions grouping, and had to sit in each regional group presentations.

Central and West Africa
Dominique Bollier, Regional Field Security Officer and Chona Galang, Regional Security Operations and Risk Analyst

The RFSO together with the Regional Analyst presented the current security updates and challenges in the region that affect IOM’s activities. Terrorism and Armed conflict were identified to be the dominant security threats in West and Central Africa, with a high tendency to deteriorate further due to the complex security environment. The countries of Sahel region (Mali, Burkina Faso, Mauritania, Chad and Niger), and Lake Chad Basin Area (Nigeria, Niger, Cameroon and Chad) continue to witness the atrocities of the local and international terrorist groups. While, armed conflict in Central African Republic and Democratic Republic of Congo continue to progress negatively and will remain affected by the political instability. With more than 2,200 staff including 1,200 workers on hourly contracts, the duty of care is a key issue for the IOM security unit. In addition to this, the need for SSAPE training is also a crucial particularly in Nigeria and Niger, which are the two largest Missions in the region.

East and Southern Africa
John Williamson, Regional Field Security Officer and Kennelyn Alagar, Regional Security Operations and Risk Analyst

The presentation of the RFSO and the Regional Analyst covered information on IOM main operational areas and locations with SSU presence, and the comparison of prevailing general threat categories from January to June 2018 in East and Southern Africa (EaSA). Based on SSU SIOC’s daily monitoring, terrorism is observed to be the prevailing threat, followed by armed conflict and civil unrest; while, SSIRS reports received by SSU OPCEN and extracted from UNSMIN during the six-month period identified crime as the top threat category that affects IOM personnel, assets and/or operations. The following hotspots are grouped based on the prevailing threat categories: Somalia and Kenya (terrorism); South Sudan and Mozambique (armed conflict); and Ethiopia and Burundi (civil unrest). Assessment indicates that the security situation in the region is very likely to remain unpredictable in the near to medium terms, with a possibility for terrorism threat in Somalia and Kenya to continue to be elevated, and armed conflict and civil unrest related incidents to recur in the aforementioned hotspots. The assessed immediate impact on IOM in the region could still vary from indirect (for terrorism, armed conflict, and civil unrest) to direct (most especially for crime).
Europe and Central Asia
Senadin Sabanija, Field Security Officer of IOM Turkey and Justine Paredes, Regional Security Operations and Risk Analyst

The FSO of IOM Turkey and the Regional Analyst for Europe and Central Asia provided a brief overview of the number of IOM staff and offices in the region, as well as the prevailing threats across the four categories including hazards for the period of January to June 2018. The hotspots presented and the corresponding threats therein, were Turkey, Ukraine, and Greece, mainly chosen due to the large IOM footprint in these countries. The FSO of Turkey summarized the threats plaguing the country through the SRM area map, which included the conflict involving the Partiya Karkerên Kurdistanê (Kurdistan Workers’ Party – PKK), the arrest of individuals allegedly involved in the 2016 failed coup, the Idlib operations involving the Turkish army in the Syrian Arab Republic, and the rescue of migrants from the Coast. For Ukraine, the ongoing armed conflict between the army and the pro-Russian separatists were the focus. For Greece, the increase in the number of migrant camps and IOM involvement, was touched upon. The emerging trends and forecast for the entire region includes the continuation of lone-wolf attacks, the migration influx, persistence of civil unrest, Daesh presence in Tajikistan, and crimes compounding the security landscape.

The Americas and the Caribbean (AMCA)
Alister Wood, Regional Field Security Officer and Paul Weijers, Regional Analyst

The RFSO and Regional Analyst presented an overview on the Region’s coverage in terms of countries, locations, and the offices with security personnel. AMCA remains a hotbed for crime, mostly driven by drug trafficking, and politically motivated civil unrest. The post-peace agreement scenario in Colombia resulted in a record high production of cocaine, which causes an increase in local drug consumption and high crime rates throughout the region. Also in Colombia, armed conflict continues as the peace process with the National Liberation Army (ELN) guerrilla group deadlocked. Meanwhile, political civil unrest erupted in Venezuela, Nicaragua and Haiti.

Middle East and North Africa
Fernando Da Costa Chambel, Regional Field Security Officer and Gerardine Paguibitan, Regional Security Operations and Risk Analyst

The RFSO and Regional Analyst presented an overview on the Region’s coverage and the SSU MENA personnel composition. Libya, Syrian Arab Republic, Iraq and Yemen were mentioned as hotspots for the region. Armed conflict and terrorism were the prevailing threat concerns in the region. Matters with regional impact were identified, including its cross-border implications that may potentially affect IOM missions, such as the developments in the Israel-Palestinian territories, Syrian Conflict, and updates on involving radical groups were provided.
The RFSO and Regional Analyst presented an overview of staffing, office locations, security personnel, and number of SCAAN users in the region. The operational and threat landscape of IOM was described in terms of its complexity and diversity. Terrorism remains the most prevalent threat, followed by civil unrest, armed conflict, and hazards. All these affect the migration patterns in ASPAC as well. Six countries were identified as hotspots (Afghanistan, Pakistan, Bangladesh, the Philippines, Indonesia, and Papua New Guinea) attributed to the magnitude and scale of security threats affecting them. The 2019 regional security outlook will remain dynamic, given that the threat actors’ intent is high, particularly pro-Daesh groups who are continuously seeking ways to wreak havoc against multiple targets (state apparatus and soft targets). Socio-economic, cultural, and political factors will also trigger outbreaks of unrest and armed conflict within the region.

SCAAN Updates and New Features
Amy Rhoades – SCAAN Community Engagement Programme Manager and SCAAN CENTRIC team

The Security Communications and Analysis Network (SCAAN) team updated the participants with the continuous development processes that will serve the needs of staff and field security. SCAAN was initially piloted in various IOM missions in 2017 with 250 users. Institutional rollout continues with more than 3500 staff already enrolled. The system is robust and secure, and fully compliant with IOM policies on data protection and privacy.

New features to be rolled out are based on SSU’s strategic priorities and user feedback from the group discussions with the participants as facilitated by Amy Rhoades, Dennis Mendiola and CENTRIC team.

1. Dashboard & Mobile App
   a. Implementation of assigned roles and permissions structure that grants access to security officers based on their security management roles and geographic coverage within IOM
   b. Adoption of the IOM ICT password policy and two-factor authorization for dashboard users
   c. Improvement of the live dashboard overview
   d. Compilation and management of country level emergency contacts
   e. Standardization of the advisories and IFRs for more concise, contextualized information
   f. Mobile app user authentication thru IOM email verification
2. SMS fall-back
   a. SMS proxy app to route emergency signals or messages/reports using SMS [when cellular data network is not available]
   b. To explore possibility of routing SMS from non-smartphones to SMS proxy app

3. Satellite tracking and connectivity
   a. Integration of emergency signal, communications and tracking from satellite device into SCAAN.
   b. Provision of satellite connected devices for internet connectivity and routing.
   c. Cost and satellite global coverage are the major considerations for the effective use of satellite communications services.

4. Geofencing
   a. Ability to bounded geographical areas (‘no go’ zones) and push out security updates and related information to staff located within the area, notifying staff on the change in risk level.
   b. In areas with no or limited internet connectivity, SMS can be an option for issuing security updates and warnings.

5. Warden/ Headcount
   a. Warden system will send push notification requesting status update to all staff in a designated geographic area.
   b. Warden call timeframe will be capped at one hour, so that all users in the coverage area should respond within that time frame. Status of users who do not respond will be automatically set to “Not OK” and will need to be contacted.
   c. Creation of summary report on OK and Not OK status
   d. Warden system should be able to identify who are in country, including those on TDY, as well as staff outside the country.
   e. Develop the capability to define warden zones or sub regions
   f. Allow SMS messaging for staff in areas without internet connection.
   g. If the device is silent, or the app is not active, warden call notification should still be allowed to go through.

6. TRIP
   a. An updated version of the TRIP interface in the app with more UX/UI design improvements
   b. There is a need to synchronize location database with the UNDSS system
   c. To add alert or notification functionality to inform staff who are not in TRIP
   d. Explore possibility to extend SCAAN to accommodate dependents, particularly for geolocation and communications

Key takeaways:
- The SCAAN system will continue to enhance security communications and assistance with the use of its features such as geo-locating and fencing capabilities, context specific advisories and instant headcounts. Various warden headcounts were carried out throughout the year to test the efficiency of the system. Rapid response and action is essential in ensuring the safety and security of staff members working in high-risk Missions.
The SCAAN team is exploring the option of system integration with emphasis on tracking and communication using satellite communication devices. Technical evaluation and assessment of the tracking devices and satellite routers available in the market is underway.

In a general discussion after the session, one participant stated that SSU has developed SCAAN as a lifeline for emergency situations, a way for staff members to directly and instantaneously get in touch with security personnel. SCAAN allows IOM personnel to easily send alerts when they are at risk and receive lifesaving information. With a touch of a button, you will trigger an alert from your mobile device which will immediately notify the SSU Global Operations Centre and allow the team to respond rapidly and provide assistance during an emergency or crisis.

DAY 2 (05 November, Monday):
Operational Understanding on Data Protection and Robust Emergency Management
The general objective of this day is to gain operational understanding on how data protection is linked with staff security and how to plan for a robust emergency management.

The second day comprised of three sessions: IOM Data Protection Policy; Robust Emergency/Crisis Management; and a scenario exercise and debrief on the Analysis of Robust Emergency/Crisis Management,

IOM Data Protection Policy
Christina Vasala Kokkinaki, Legal Officer, Office of Legal Affairs Headquarters

The focus of the session is to provide the participants with the overall importance of data protection in the context of staff safety and security. The guest presenter outlined in her presentation the basic concepts and definitions of data protection and IOM’s Data Protection principles. The 13 IOM Data Protection principles should be incorporated into programs and projects, ensuring that these are applied systematically throughout the organization. During the session, a scenario exercise on data protection issues were given to the participants to help them understand the confidentiality of data and information received and ensure to protect data in respect to IOM personnel right to privacy.

Key takeaways:

- In situations wherein inadvertent information is disclosed, this could potentially result in harm or threat to the safety of IOM personnel. Wherein lies the need for security professionals to have a firm grasp and knowledge on the institutional safeguards for handling data and information.

- IOM security professionals are fully accountable for staff safety and security in accordance to their duty of care obligations and IOM’s data protection principles will provide guidance and support.
raise awareness amongst the participants in ensuring that appropriate efforts are made, and measures are implemented to protect IOM personnel.

- With the increased use of advanced technology in security, data theft or loss, and inappropriate use and disclosure of data is unavoidable in a certain extent. Participants are thus encouraged to learn more about IOM’s policy on data protection to efficiently handle confidential personal data throughout the organization.

- Biographical data, security incident related data, data generated from biometric security system are all considered personal data. It is worth noting that any personal data extracted from security systems should only be processed for staff security purposes. Personal data is not to be shared externally, to avoid any confidential or organizational information getting in the wrong hands. Proper clearance must also be coordinated with the Director of SSU and LEG.

Robust Emergency/Crisis Management: Presentation, Scenario Exercise, Debrief and Analysis
Anna Eliatamby, Staff Welfare Officer; William Wairoa-Harrison, Director of SSU; Alister Wood, RFSO for the Americas and the Caribbean; and Maricar Purugganan-Adkins, Global Security Coordination Support

A brief presentation on Robust Emergency Management was provided during this session, with the aim to allow the participants to apply the skills and knowledge in areas linked to effective management for emergencies, crises and disasters.

The key factors to consider in managing an emergency or crisis are: Situation Awareness, Leadership, Collaboration, Resilience and Courage, Emotional Management and Planning and Communication.

After the presentation, participants were then grouped into three to participate in a simulation exercise. Each group took on three distinct roles; as (1) Crisis Management Team (CMT) in Geneva HQ, (2) Security Management Team (SMT) and (3) Area Security Management Team (ASMT). The participants were given a complex scenario which centers on a time-sensitive evacuation that requires coordination with multiple entities. The primary objective of the exercise was for the participants to have a better understanding of themselves, particularly on how they handle stress in emergencies/crises.

At the end of the activity, group representatives were requested to provide their feedback based on how their groups were able to apply the six key qualities in the Robust Emergency Management Model.
Key takeaways:

- The first group shared that they were not prepared to take on the first scenario with the role as the SMT, due to unfamiliarity of their role for this task. This confusion resulted to the group’s inability to identify the priorities and sort critical information that they need to pass on and coordinate with the other groups. The first group shared that they learned the value of understanding the tasks of other UNSMS entities, particularly the SMT. This will allow them to identify and communicate their priorities to these other entities, particularly in an emergency or crisis. After taking notes of their key learning experiences for the first round, for the second and third rounds of the exercise, the group had a better understanding of their individual roles and had a good grasp of handling the scenarios and were able to make more structured decisions and actions.

- The second group shared that they were able to go through each scenario smoothly because they assessed the situation they were in, gathered and processed information in a timely manner. The group put into consideration the information coming from the other groups, as required in the exercise. In terms of emotional management, group members were able to manage their own individual stress and remained calm. Tasks were assigned accordingly and responsibilities were divided equally with the assurance that there was no communication gap. Teamwork was the key strength of this group. However, they encountered slight challenges in coordinating with the other actors playing the external counterparts in terms of their methods of communications. With this, the group identified the importance of enhancing their communications skills and being able to quickly adapt to the type of communication approach of their counterparts, particularly those who are outside the UN system.

- Similar to the first group, the third group, with their role as the CMT was slightly unsure and lacked the knowledge of the capacities of each department and individual roles assigned to each member. In terms of leadership, the group also recognized that the lack of structure was attributed to the group's focus on the situation. Eventually, the group understood that delegation of tasks was the key. The group engaged with each other through collaboration and was able to support one another and address the actions required of them.

- The Director of SSU as the facilitator for the CMT task, advised the participants to have a mindset of moving away from operational planning and gearing towards strategic planning. Think of long term plans that will work. He also stressed that communication is essential, when a major crisis goes down, be prepared to handle various requests and issues coming from all sides and ensure that accurate information is passed on to the right individuals.
From an SMT’s point of view, the lead facilitator noted that all three groups had challenges with task delegation. To better manage a crisis, it is critical to learn how to manage the tasks assigned and understand that collaboration is vital.

For the ASMT task, the lead facilitator noted that with this task being the last, the participants were more comfortable and had a better understanding of what was required from them. Irrespective of the type of crisis or incident, if you have a structured plan, you can effectively put together an incident response package. Another key takeaway for the participants from the facilitator was to understand the significance of communication. Consider that there are stakeholders and other individuals who will provide support as well - learn to inform and coordinate.

For the task on coordinating with government counterparts, the lead facilitator stated that the exercise was meant to test the participants limits and to learn how to adapt in a situation wherein the approach should always be calm and in a tactile manner. It is important to keep in mind the context of the local culture when approaching government officials. Participants need to understand the host government and key officials’ perception of the UN, be professional and courteous.

**DAY 3 (06 November, Tuesday):**

**Technological Updates on Security Tools**

The general objective of this day is to provide participants with the technological updates on the relevant security tools.

The third day comprised of six sessions: T.E.S.S and TAG; Enhancing Operational Support to the Mission through the SSU Global Operations Centre; Technological Approach in Standardizing Security Updates and Incident Reporting; SCAAN Training of Trainers; Presentations and demos on Virtual Reality for Security Trainings and Cross-Sector Technology.

**T.E.S.S and TAG**

John Williamson, RFSO for East and Southern Africa and Dominique Bollier, RFSO for West and Central Africa

The presenters started the session by providing participants an overview on how the Interagency Security Management Network (IASMN) has also expanded its focus on security-related technology and telecommunications, the Telecommunications Security Standards (TESS) project in collaboration with the IASMN’s Technical Advisory Group (TAG) has worked with UNSMS entities to set standards and offer guidance on security telecommunications including issues on migration from analog to digital VFH radio networks.

There was also a brief mention of the Electronic Travel Advisory (eTA), a security application, similar to SCAAN, developed by UNDSS that will be launched by January 2019. The Director of SSU provided clarification regarding the use of eTA in IOM. SCAAN is IOM’s primary and only tool. The mandatory use of SCAAN has been cleared by LEG and in accordance to existing organizational policy signed off by the Director General. It has been made clear in the IASMN Working Group that IOM cannot be mandated to use the eTA.
Key takeaways:

- In 2014, Digital Mobile Radio (DMR) was defined as the UN standard for VHF digital radios. While digital VHF networks are complex and expensive, not all of these features are being used. At present, the UN VHF networks have these two requirements; basic PTT (push to talk) feature and standard SeIV features (caller ID, alert features and capabilities for stun radios remotely).

- IOM currently makes use of analogue and digital radios, specifically MotoTrbo Professional two-way radios, they now carry digital VHF radios with geo-location and fencing features. TETRA, defined for UHF, is also commonly used in some Field Missions. However, the VHF radio remains as the fallback of the security network.

- In a general discussion following this session, it was pointed out that radio-based tracking solutions in the field will gradually be replaced by mobile phone-based vehicle positioning and tracking systems which will further reduce the need to do position reporting via VHF. One participant asked if it was possible for SCAAN to adapt the same technology as the Motorola Solutions WAVE push-to-talk group communication service that connects across different networks and devices such as a Smartphone. However, SCAAN is a system with a field-driven focus which aims to provide security personnel efficient and effective communication and increased situational awareness during a crisis. In addition to this, SCAAN facilitates rapid digital headcounts as well. SCAAN is continuously evolving with the aim of being the “go to” digital security tool not only for IOM but for other UNSMS agencies as well.

- One participant inquired if a Standard Operating Procedure (SOP) on TESS is being developed as this will surely offer practical guidance to personnel working in the field. The Director of SSU stated that this is currently included in the project deliverables of the IASMN TAG.

- With the advancement of technology in the global security environment, the importance of interoperability in security related systems and tools was highlighted in the session. Hence, the need for security personnel to be more aware of the emerging technologies that will positively impact field operations during a crisis or emergency.

**Enhancing Operational Support to your Mission through SSU Operations Centre**

Steve Mayall, Officer-in-Charge for SSU Global OPCEN; SSU OPCEN staff

The session’s objective was to provide insight to the participants on SSU Global Operations Centre’s functions, products and services. The Director of SSU briefly opened the session by affirming that although the SSU Global OPCEN (Security Information Operations Cell and 24/7 Communications Centre) is located in Manila, Philippines, it’s focus is to deliver global services to Missions worldwide; the Field Security Officer (FSO) for IOM Philippines is responsible for implementing all aspects of security management for the Manila Administrative Centre (MAC) and IOM Philippines Country Office.
During the session, the SIOC team of Regional Analysts introduced one of their newest product, the Bi-Annual IOM Security Incidents Global Snapshot which provides an overview of global safety and security incidents affecting IOM personnel. The SIOC Regional Analysts also conduct field security threat information assessments at the request of the Mission in coordination with the respective Regional Field Security Officer, OIC of SSU Global OPCEN and with the overall endorsement of the Director of SSU.

Key takeaways:

- The 24/7 Communications Centre (COMCEN) is a vital component of the SSU. The COMCEN operators function as the SCAAN Global first responders. Incident flash reports and advisories are broadcasted thru the SCAAN desktop dashboard and made available on mobile devices. With SCAAN’s ability to provide geolocation and plot movements of personnel, staff headcounts at the time of a security incident is easier to manage.
- SCAAN enhances staff safety and security by augmenting the operations of SIOC and COMCEN. The system is an effective tool in security incident management, by allowing the SSU Global OPCEN team to monitor emerging situations and respond to incidents involving IOM personnel.
- To ensure that the SSU Global Operations Centre remains the primary global hub for information and situational awareness, the need to evaluate current processes is deemed important. One way of enhancing operational support is applying technological tools that will allow timely reporting and promoting the visual content in OPCEN products that will boost engagement and improve audience retention.

Technological Approach in Standardizing Security Updates and Incident Reporting
Alister Wood, RFSO for the Americas and the Caribbean; Steve Mayall, Officer-in-Charge for SSU Global OPCEN and Paul Weijers, Regional Analyst for the Americas and the Caribbean

The session started with the RFSo AMCA, presenting an overview on the significance of Socio-Technical Systems and its application within the organization and SSU. The Socio-Technological Systems theory is “defined as any organisation, or part of it, is made up of a set of interacting sub-systems. Thus, any organisation employs people with capabilities, who work towards goals, follow processes, use technology, operate within a physical infrastructure, and share certain cultural assumptions and norms”. ²

The second part of the session is enhanced data visualization as presented by the Regional Analyst for the Americas and the Caribbean. The RA provided the participants with a glimpse of the proposed interactive format for the Monthly Security Bulletin Report produced by the Regional Analysts.

**Key takeaways:**

- Participants should understand that the Socio-Technical Systems (STS) theory is designed to optimize the social (people) and technical (technology) aspects of an organization to form a cohesive system. By applying the STS approach in the workplace, security personnel will recognize that the interdependencies between the layers in the system (psychological, technical, cultural, operational, financial and structural) will support their functions and enable them to be effective Risk Managers.

- As pointed out by the RFSO for AMCA, information systems do not exist in isolation, there is a degree of interactivity, the need of reciprocity within the system, from passing on information to receiving information. Otherwise, information becomes partial or imbalanced.

- One of the complex components of Crisis Management is not the event itself, but the amount of information required by the stakeholders and key audiences immediately after the event. This creates a massive amount of resource demand, and if systems are not in place, there is a misconception of how effective you are as a Security Risk Manager.

- Effective visuals and integrating these visual data enhancements to reports produced, without compromising the content, will increase attention, retention and engagement with the readers. The audience will process information that is easily absorbed because of the interesting way that it is presented.

- By the end of November 2018, the SSU Global Operations Centre’s SIOC will launch a new version of the daily Global Security Situation Report (GSSR) which will provide information and analysis in an interactive and engaging format.
SCAAN Training of Trainers
Amy Rhoades and SCAAN team

The presenters provided a walkthrough to participants by reviewing the current SCAAN training package, resources and other reference materials that will assist security personnel when conducting training sessions for staff in Field Missions.

A small group exercise simulated a SCAAN user training to familiarize participants in the contents and flow, and on the FAQs often encountered from new users.

Key takeaways:

- SSU regional teams discussed the status of the SCAAN deployment in regional and country offices and drafted initial plans and targets for the end of year push of the SCAAN rollout to all missions. Global target of 5000 users by 31 Dec 2018.
- The SCAAN webpage on the Intranet Portal is made available to all IOM staff which provides key resources such as the User Training Video, Installation Guides and FAQs in English, French and Spanish. In addition to this, there is a dedicated SharePoint page for SCAAN with resources specifically designed for Trainers.
- From the group discussions, one group mentioned that they would like to see specific advisories for national and international staff. Another group pointed out that they needed more technical information on SCAAN especially when used in the field. One group asked if SCAAN system work without access to the Internet, the SCAAN team stressed that currently the system and app functions with 3G and 4G networks but are looking into a fallback in the absence of internet connection.
Virtual Reality for Security Trainings and Cross-Sector Technology
Amy Rhoades and SCAAN team

This session introduced new, innovative technologies emerging in the field of security. Participants were divided into two groups and engaged in the two interactive sessions below:

1. Overview of TENSOR project using open source intelligence to identify and respond to security threats; IOM’s 360 Virtual Reality videos for security training
2. Community Policing and Cyber Threat Edu-Gaming to practice decision-making in security contexts; CENTRIC’s interactive Virtual Reality videos for experiencing security situations in an immersive environment

Key takeaways:
- The TENSOR (Retrieval and Analysis of Heterogenous Online Content for Terrorist Activity Recognition) project provides a platform for terrorism intelligence. Using open sources and online sources, this can assist in identifying, gathering and interpreting online-based terrorist-generated content with tools for searching, crawling, monitoring and gathering related sources. TENSOR offers a fast, reliable planning and prevention functionalities for early detection of terrorist activities that can potentially enhance IOM security capabilities.
- Virtual reality is a fast-developing technology that can be utilized for security trainings. Through VR, security managers and decision-makers can virtually immerse in and experience a hostile environment or scenario in which security measures can be practiced and tested.
DAY 4 (07 November, Wednesday):

Policies, Capacity Building and Trainings

The general objective of this day is to provide participants a review on relevant organizational policies and provide updates on SSU’s efforts on capacity building and training delivery.

The last day comprised of six sessions: SSU Global Coordination Support at Headquarters; Updates on UNSMS Policies from the IASMN; IOM Mission Security Funding Mechanism; Air Safety; IOM Security Training updates; and Security Training Needs.

SSU Global Coordination Support at Headquarters

William Wairoa Harrison, Director of Staff Security Unit

The Director of SSU presented an overview of Global Security Coordination Support at Headquarters. SSU is IOM’s focal point within the UNSMS, thus SSU HQ liaises with the IASMN and UNDSS Headquarters on UNSMS system-wide policies and procedures; any IOM and UNSMS security policy issues or policy related consultations are coordinated through SSU HQ. The overall management of SSU’s global administrative, procurement and finance services are under SSU HQ. Internal and inter-agency global training requirements and delivery coordination also falls under SSU HQ’s purview. The SCAAN project is the brainchild of SSU Headquarters, with this the Technical Coordinator directly reports to the Director of SSU.

Key takeaways:

- Regional Field Security Officers play a key role in providing technical advise to Field Missions during the procurement process. To ensure that IOM’s procurement processes are carried out systematically, there should be coordination between requesting Mission and the RFSO, the SSU Procurement Focal point and the Global Procurement and Supply Unit (GPSU).
- SSU stays true to its mandate of providing specialized safety and security trainings, with 25 certified UN trainers in the IOM Security Trainers network. Qualified security professionals are nominated to attend UNDSS certified courses, with the expectation to pass on the gained experience and knowledge to the field.
- Participants were also reminded that all staff nominations to safety and security related trainings must be properly coordinated with RFSOs and approved by SSU Headquarters.
- To ensure aviation safety within the organization, the Director of SSU as the Air Travel Focal Point (ATFP), and the RFSO for East and Southern Africa as the Alternate Air Travel Focal Point (AATFP), provide advise and guidance to IOM personnel on any issues related to aviation safety. Endorsements and approvals on the use of commercial airlines must be coordinated with the Director of SSU and the AATFP.
Updates on the UNSMS Policies and IASMN
William Wairoa Harrison, Director of Staff Security Unit

The Director of SSU updated the participants on the current UNSMS policies being reviewed during the last IASMN session in June 2018:

- The Field Security Handbook (FSH) transition to the Security Policy Manual,
- The review of the Air Travel Policy,
- Minimum Operating Security Standards (MOSS) has been replaced to Security Risk Management Measures (SRMM).
- The Safety Risk Management Working Group is working on a draft policy, identify safety hazards, the inclusion of safety incidents, and crisis related planning. Occupational Health and Safety (OSH) initiatives in crisis management was also discussed.

Key takeaways:

- In response to a participant’s query on what is SSU’s role is when OSH comes into play, the Director of SSU emphasized that in the first 48 hours of a major hazard or disaster, we will be the first responders, until it is confirmed that IOM staff are no longer at risk.
- One participant sought clarification and guidance on where SSU sits with regards to Business Continuity Planning (BCP). The Director of SSU, stressed that even though Security is a vital component of the BCP, the BCP does not belong to Staff Security alone. There are other core departments such as Human Resources (HR), Administrative Services, Finance, Procurement, Information Technology (IT) and Occupational Health Unit (OCU) with critical support functions. The Chief of Mission is responsible for ensuring that all core departments’ business processes and services continue in the event of a disaster. Security can coordinate and assist with the development of a Mission BCP but maintaining the BCP lies with the Chief of Mission. The IOM BCP Guidelines is currently being revised and updated, and a standard BCP template will be made available.
- During the session, the Director of SSU provided an update on the Third Party Contractor (TPC) IOM guidelines. The Guidelines outline that the TPC is responsible for its employees under all circumstances, IOM has a moral duty of care in for TPCs on safety and security. SSU is a member of the TPC Advisory Group.
SSU, in coordination with the Advisory Group and the Mission Field Security Officer (FSO), is also involved in providing the minimum-security requirements to be included in the TPC Service Agreement, including recommendations on the necessary equipment to be provided to the TPC employees in relation to safety and security (e.g. radios and PPEs – helmets and body armor).

- One participant raised that Staff Security needs to be involved at the beginning of program development. Guidelines must be updated yearly so we have a common understanding. The Chief of Mission and Project Manager’s allocation for security is not triggered in the first phase of the proposal writing. In a project, only five to 10 percent is allocated to security especially for projects in high-risk Missions.

**IOM Mission Security Funding Mechanism**

William Wairoa Harrison, Director of Staff Security Unit and Lalaine Mendiola, SSU Finance Assistant

The SSU Finance Assistant briefly presented the SSU Funding Mechanism based on Council Resolution 1111, and reminded the participants that Missions are responsible for including safety and security costs in their programmes and Mission budget plans. In addition to this all safety and security related requirements directly associated with project implementation should be included in the project’s budget.

**Key takeaways:**

- The Chiefs of Mission (CoMs) should understand that Member States have given the mandate to the Director General that all safety and security costs must be projectized in the Missions’ budget plan. SSU will assist the Mission to fill the financial gaps in the absence of funds to cover security needs and requirements, provided that the request is justifiable. However, if a Mission cannot provide a proper justification for SSU to cover these costs, then there is a perception that the Mission does not require these funds.

- All Mission Safety/Security Funding requests must be supported by a written endorsement from the Mission’s Regional Field Security Officer (RFSO) prior to submission to the SSU Finance Assistant.
The session on Air Safety by Alternate Air Travel Focal Point (ATTFP) provided guidance to the participants by understanding that there is an authorizing structure in place, and that the use of air operators is rated into three categories.

In applying for restricted/conditional airline use, the ATFP and AATFP have developed a template for requesting blanket approvals. SSU is in the position to revoke a blanket approval if reports are received that there is a downgrade in the carrier’s safety and security record. The decision to fly with the restricted airline is solely on staff member’s discretion and they are not compelled to use a restricted airline. Aside from approval process, the presenter also discussed the classification of civilian aircrafts.

Key takeaways:

- As emphasized by the AAFTP, aviation is statistically safe. He added that the main risks of aviation are not always related to mechanical error, the primary cause in aviation accidents are caused by pilot error.
- At the end of the session, participants were well informed on how to identify civil aircrafts, through the aircraft’s registration mark, appropriate nationality marks, common and underside markings. These markings serve as a guide when the AATFP conducts a risk assessment; making sure that the aircraft being used or will be used is up to standards.
- IOM personnel, as members of the UNSMS should comply to the safety requirements in air travel and by understanding the air operator categorizations, staff safety and security is enhanced.
- One participant inquired if there was a way to filter the Registered Air Operators Booking List by country rather than alphabetically arranged by Airline. This needs to be assessed if feasible since the booking list is also derived from the Aviation Risk Management Office (ARMO) UNDSS.
IOM Security Training: Updates and Future Objectives

Security Training Needs and Development of a Regional Delivery Plan
William Wairoa Harrison, Director of Staff Security Unit

A panel discussion on security training needs followed, with the list of trainings identified by the participants:

- Training on basic security guidelines on de-escalation and negotiation techniques in a situation wherein a beneficiary is angry or hostile
- UN standardized Training for Drivers on Road Safety strategies
- Middle Management Training for Security Officers and Field Security Coordination Officers
- ToT on First Aid – Cardio Pulmonary Resuscitation (CPR) and Automated External Defibrillator (AED) Training
- Hostage Incident Management (HIM) General course for Field Security Officers (FSOs) provided by RFSOs
- BCP Training
- Crisis Management Training
- Fire Safety Training
- Virtual Reality integrated into Security Trainings (IOM Field Scenarios e.g. convoy, active shooter, hostage incidents, crisis management)

Key takeaways:

- To ensure the quality of IOM-delivered security trainings, IOM Security Trainers must deliver or co-deliver at least one training every six months to retain certification. Security Trainers who are unable to facilitate trainings must consult with their respective RFSOs and seek guidance.
- The criteria to be an IOM Security Trainer is to successfully complete the TOT, after which should have organized and co-delivered relevant trainings with a certified trainer.
- Training plans must be shared to SSU HQ for inclusion in the official IOM Global Security Training Calendar (yearly and quarterly).
- To nominate or be nominated in Certification Courses, IOM staff member/requesting Mission must seek endorsement from the RFSO, the RFSO will then request approval from the Director of SSU, finally SSU Headquarters will coordinate the nomination to UNDSS TDS.
- The Director of SSU is the overall Security Training Focal Point and Manager for IOM trainings. All IOM-led security training certificates must be coordinated with the SSU Global Admin and Finance team and signed by the Director of SSU. Data and list of participants must also be shared to the SSU Global Admin and Finance team for record-keeping.
The guidelines and principles in these security training packages remain the same regardless of the Country. However, training modules must be developed to tailor-fit the needs of the Mission, and according to the duty station’s socio-cultural and environmental context.

The RFSO for WCA proposed a mentoring program for colleagues nominated to attend UNDSS SCP and LSA Courses. The Director of SSU was in total agreement and assigned the RFSOs as the Focal Point for these pre-course mentoring program.

On HIMCO courses, the RFSO for AMCA said that there is an absolute need to have FSOs trained in the same criteria as that of the RFSOs in response to general HIM awareness, the FSOs will then be able to provide support to the RFSOs in the event of a HIM incident. The Director of SSU will discuss with the UNDSS Under Secretary General (USG) for UNDSS TDS to provide UN-certified HIMCO courses for IOM.

The RFSO for WCA stressed that the SSAFE training is important in Democratic Republic of Congo (DRC), and proposed to have at least four to six dedicated UNDSS TDS-certified trainers (from the current two trainers that they have in the region).

The OIC for SSU Global OPCEN iterated the importance of health and safety, proposing First Aid trainings relevant to drivers. UNDSS and IOM does not provide certified First Aid training. While the Director of SSU, agrees that there is no concrete training programme for this, his concern is who in SSU are qualified to deliver these trainings.
Final Panel Discussion
William Wairoa Harrison, Director of Staff Security Unit
To conclude the Global Retreat, the Director of SSU said that with the shrinking humanitarian space, and where IOM personnel are working in insecure and unstable areas, the demand for ensuring staff safety and security has become challenging. Yet it is with due diligence that security professionals must continue to guarantee that we fulfill our obligations to adopt the principle of maintaining operations in a safe and secure manner by accepting responsibility and accountability for security management.

Next generation technology increases efficiency and productivity in relation to humanitarian efforts, the Director of SSU encouraged the participants to adapt to this changing landscape and to take on an approach of finding innovative ways in enhancing staff safety and security.

One participant suggested that Global SSU Retreats should be held in other regions aside from Manila, Philippines. The Director of SSU considered the idea of a Regional SSU Retreat in the various Regional Offices. This is something that needs to be sufficiently planned and put in place in due course. Another participant highlighted that it was important that Security Analysts to visit other Field offices to enable them to gain updated perspectives on the situation in the field. Networking across regions is beneficial in allowing them to obtain relevant safety and security information from the ground and build a network of diverse relationships.
Capacity Building Events in Conjunction with the SSU Global Retreat

In conjunction with the Global Retreat, SSU also delivered five (5) UN certified security trainings: UN Security Certification Programme (SCP); Local Security Assistants Course (LSA); and three (3) sessions of Women Security Awareness Training (WSAT). The delivery of these trainings is part of SSU’s wider commitment in partnering with UNDSS Training and Development Section (TDS) and the IAMSMN in sharing training resources to meet the growing needs of UNSMS agencies and organizations. Within the UN system, IOM has now become one of the leading agencies in security training delivery.

The capacity building programme of SSU in Manila in October-November, as part of the SSU Global Retreat, trained a total of 95 IOM and UNSMS personnel.

UN Security Certification Programme (SCP)

Course Director: Jacques Legros, UNDSS TDS
Co-Facilitators: Dominique Bollier (IOM) and Senadin Sabanija (IOM), James Abraham (UNDSS)
Resource Specialist Facilitators: Anna Eliatamby (IOM), Maricar Purugganan-Adkins (IOM)
Training Host: IOM

The SCP Course is a 10-day programme that certifies security personnel as a UN Security Management System (UNSMS) Security Professionals. This pass-or-fail course is mandatory for UN security personnel who would like to pursue a career as an international Security Adviser/Officer in the UNSMS. Without successfully completing this course, the progress within the UNSMS is limited. All international Field Security Officers are required to pass this course.

Delivery of the SCP course requires a UNDSS TDS to be the Course Director and co-facilitation could be done by UN-certified trainers. In IOM, we have 7 in-house trainers that are certified to co-facilitate the UN SCP course.

In this IOM-hosted SCP course, there were 22 participants, which includes 15 IOM personnel. At the end of the course, 19 participants were successfully certified as Security Professionals within the UNSMS. Course Director, Jaques Legros, also commended the impressive organizational skills and resources of IOM. The SCP course was held in Makati Diamond Hotel on 22 October to 02 November 2018.
UN Local Security Assistants Course (LSA)
Course Director: William Wairoa-Harrison (IOM)
Co-Facilitator: Senadin Sabanija
Resource Specialist Facilitators: Anna Eliatamby (IOM), Maricar Purugganan-Adkins (IOM)
Training Host: IOM

The LSA Course is designed to provide Local Security Assistants worldwide the tools required to work efficiently within the UN Security Management System (UNSMS) in accordance with UN Framework of Accountability for Safety and Security, ensuring standardization of processes and procedures. It also enables the participants to enhance their capabilities with the aim to improve the knowledge, behavior and skills in fulfilling their roles and responsibilities.

The course is delivered in 5 days. The LSA Course is a mandatory requirement for the SCP course.

In IOM, there are a total of 13 trainers who are certified to deliver the LSA course. In this IOM-hosted LSA course, 19 participants completed the course, including 9 IOM staff. The LSA course was held in Makati Diamond Hotel on 29 October to 02 November 2018.
Women’s Security Awareness Training (WSAT)
Lead Facilitator in WSATs Manila: Maricar Purugganan-Adkins (IOM)
Lead Facilitator in WSAT Cotabato: Thitiwan Vijitsopha (IOM)
Resource Specialist Facilitator: Anna Eliatamby (IOM)
Training Host: IOM

The WSAT is a significant part of IOM SSU’s training strategic plan and implementation of the UNSMS policy on Gender Inclusion in the Security Management System. In IOM, we have 2 certified UN WSAT trainers and 2 trainers pending for certification.

The overall objective of the WSAT is to raise awareness on the safety and security risks and issues experienced by women working in the UN. In addition, the training aims to address these risks and issues by sharing best practices, providing practical tools to prevent and mitigate these security risks, and enabling women to work with confidence in an ever-changing security environment. WSAT is a 2-day programme that consists of 8 core modules.

SSU delivered 2 sessions of WSAT on 06-07 and 08-09 November at the Makati Diamond Hotel and IOM office at Tower 6789 Alpha Land respectively. A WSAT session was also delivered by Thitiwan Vijitsopha in Cotabato City on 08-09 November. In the WSAT sessions in Makati City, there were a total of 28 participants from MAC and IOM Philippines Country Office. In the WSAT in Cotabato City, a total of 26 female staff members, including IOM Philippines Chief of Mission, participated in the training.