International Labour Organization

▶ GB.346/PFA/3

Governing Body

346th Session, Geneva, October–November 2022

Programme, Financial and Administrative Section

PFA

Programme, Financial and Administrative Segment

Date: 16 September 2022
Original: English

Third item on the agenda

Review of the ILO's cybersecurity framework

Purpose of the document

This document provides information about the findings of a cyberresilience maturity assessment and the alignment of the ILO's practices with the pillars identified in the report of the Joint Inspection Unit, *Cybersecurity in the United Nations system organizations* (see the draft decision in paragraph 13).

Relevant strategic objective: None.

Main relevant outcome: Enabling outcome C: Efficient support services and effective use of ILO resources.

Policy implications: None.

Legal implications: None.

Financial implications: None.

Follow-up action required: None.

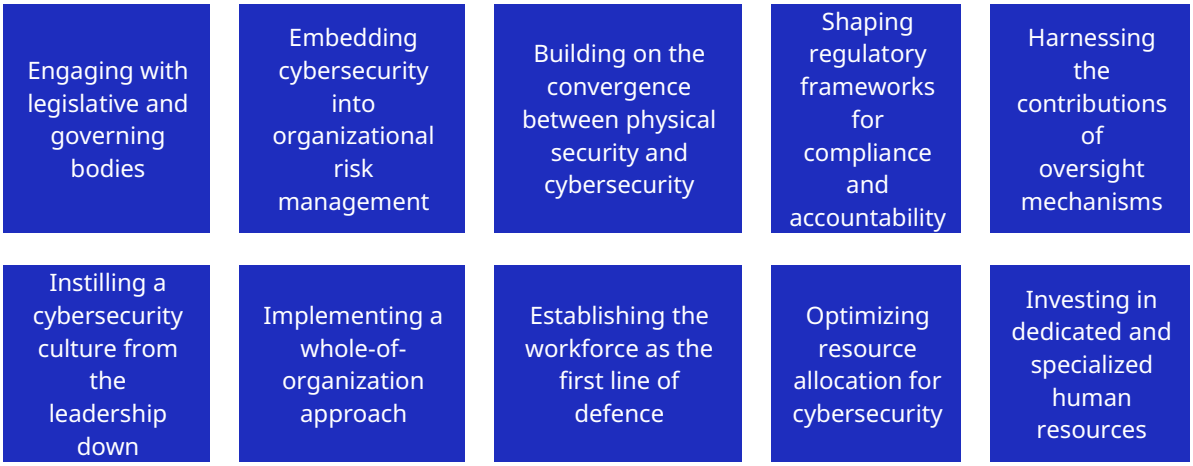
Author unit: Information and Technology Management Department (INFOTEC).

Related documents: Programme and Budget for the biennium 2022–23.

▶ Introduction

1. In 2021, the Joint Inspection Unit (JIU) delivered a report outlining common cybersecurity challenges in the United Nations (UN) system. [1] According to the report, a strong cybersecurity posture for any organization results from a multifaceted, whole-of-organization approach that cuts across several organizational domains and competences, including information and communications technology, risk management, physical safety and security, and information and knowledge management more broadly. The report also identifies ten elements, or pillars, that contribute to improving the cyberresilience of UN system organizations – in other words, their capacity to identify, prevent and detect cyberthreats, as well as to respond to and recover from incidents (figure 1).

▶ Figure 1. JIU cyberresilience pillars



2. A primary recommendation of the JIU in its report is for the executive heads of UN system organizations to review their cybersecurity frameworks and present a report on their findings to their respective governing bodies. Following established best practices, the ILO commissioned an independent organization – the UN International Computing Centre – to conduct the review and report on its findings. The present document outlines the key findings and recommendations of the review, which took the form of a cyberresilience maturity assessment.

▶ Findings and recommendations

The Office's cybersecurity maturity profile

3. The Office has a designated Information Security and Assurance Services Unit, with a team that has expanded since the initial appointment of an information technology (IT) security officer in 2007. It has established an information security management system that has been

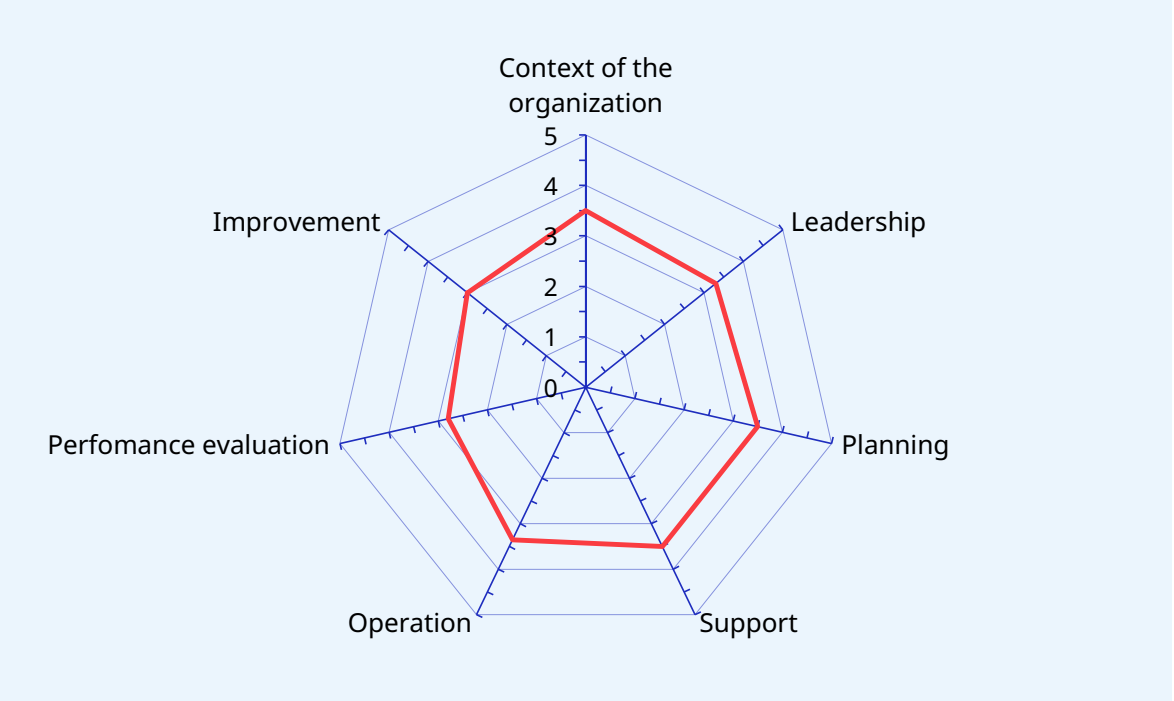
[1] United Nations, *Cybersecurity in the United Nations system organizations*, Report of the Joint Inspection Unit, JIU/REP/2021/3, 2021.

independently certified as compliant with the ISO 27001 standard for information security. Certification to this standard is recognized worldwide to indicate alignment with information security best practices.

4. The UN International Computing Centre used both the ISO 27001 standard and the JIU pillars for the purposes of the cyberresilience maturity assessment. The findings were mapped to the Capability Maturity Model. The assessment resulted in an overall cybersecurity maturity rating of 3.58 out of 5, placing the ILO's cybersecurity processes in the upper half of the model's third maturity level, which is classified as “defined”.

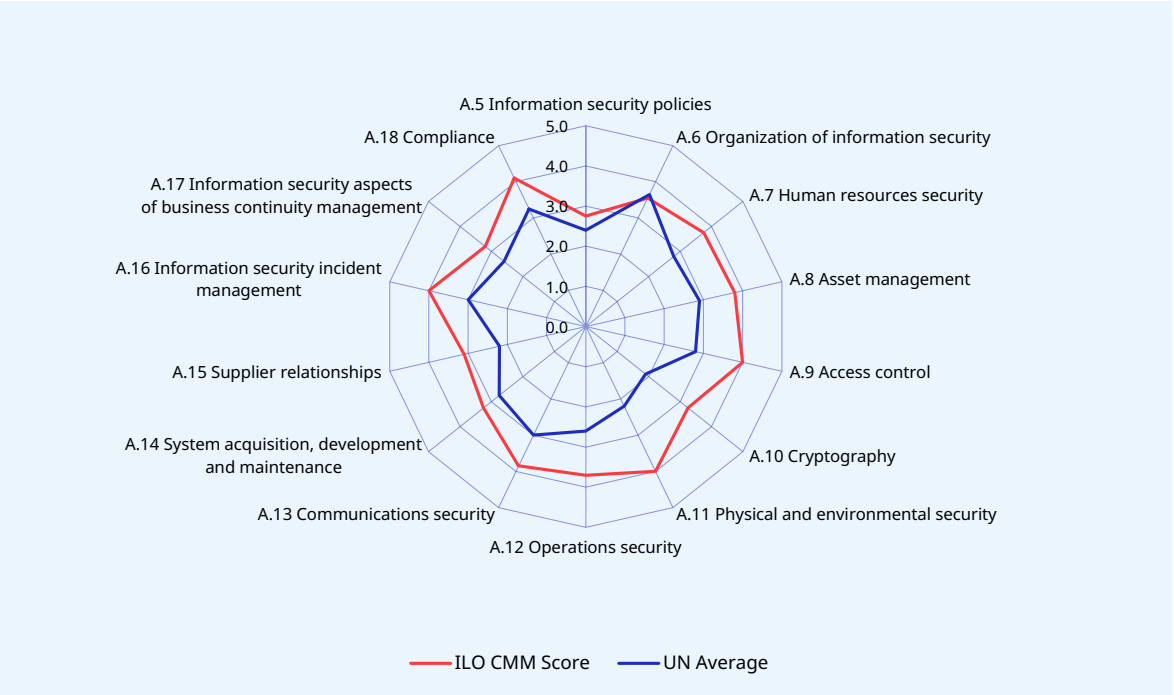
5. Figure 2 shows the maturity of key elements of the ILO's IT processes, as per the domains identified in the 2013 version of the ISO 27001 standard (the colour of the chart line is not reflective of maturity level).

▶ Figure 2. ILO cybersecurity maturity ratings as per the domains identified in the ISO 27001 standard



6. Figure 3 illustrates the findings for the ILO as per the cybersecurity control domains identified in Annex A to the 2013 version of the ISO 27001 standard. A line representing the average rating for other UN system agencies having undergone the same review is superimposed on the figure and illustrates that the ILO exceeds that average across many domains.

▶ Figure 3. ILO cybersecurity maturity ratings as per the cybersecurity control domains identified in Annex A to the ISO 27001 standard



7. The cyberresilience maturity assessment showed that multiple ISO 27001 cybersecurity controls have already been implemented and are aligned with recommendations made by the JIU in its report. The assessment also identified opportunities to further enhance cybersecurity controls.

8. The current maturity level of each cybersecurity control at the ILO is illustrated in figure 4. Cybersecurity controls that were assessed as “compliant” align with the ISO 27001 standard for industry best practice. Those that were assessed as “partially compliant” align to some extent with the ISO 27001 standard, but an issue exists that may be considered a minor non-conformity during an ISO 27001 certification audit. A mitigation plan would need to be in place to achieve and maintain certification. Cybersecurity controls that are assessed as “non-compliant” represent a major deviation from the ISO 27001 standard that would be deemed a major non-conformity during an ISO 27001 certification audit and would require priority action. None of the ILO's cybersecurity controls were found to be in the “non-compliant” category.

9. The alignment of these controls with the JIU's ten cyberresilience pillars is discussed in detail in Appendix I.

▶ Figure 4. ILO compliance with the cybersecurity controls identified in Annex A to the ISO 27001 standard

Information security policies	Organization of information security	Human resources security	Asset management	Access control	Cryptography	Physical and environmental security	Operations security	Comms. Security	System acquisition, development and maintenance	Supplier relationships	Information security incident management	Business continuity management	Compliance
A5.1 Management direction for information security	A6.1 Internal organization	A7. Prior to employment	A8.1 Responsibility for assets	A9.1 Business requirements of access control	A10.1 Cryptographic controls	A11.1 Secure areas	A12.1 Operational procedures and responsibilities	A13.1 Network security management	A14.1 Security requirements of information systems	A15.1 Information security in supplier relationships	A16.1 Management of information security incidents	A17.1 Information security continuity	A18.1 Compliance with legal and contractual requirements
	A6.2 Mobile devices and teleworking	A7.2 During employment	A8.2 Information classification	A9.2 User access management		A11.2 Equipment	A12.2 Protection from malware	A13.2 Information transfer	A14.2 Security in development and support processes	A15.2 Supplier service delivery management		A17.2 Redundancies	A18.2 Information security reviews
		A7.3 Termination and change of employment	A8.3 Media handling	A9.3 User responsibilities			A12.3 Backup		A14.3 Test data				
				A9.4 System and application access control			A12.4 Logging and monitoring						
							A12.5 Control of operational software						
							A12.6 Vulnerability management						
							A12.7 Information systems audit						

Compliant controls Partially compliant controls Non-compliant controls Controls that are not applicable

10. While the assessment provided relatively positive results, it also provided a list of recommendations that could be followed if the Office wished to further enhance its cyberresilience (Appendix II). As implementing these recommendations would imply diverting Office resources from other activities, it is proposed that attention should be focused on the recommendations that are likely to provide the best return on investment.

11. The Office proposes that its current cybersecurity communications plan should be updated to incorporate the recommendations that would contribute to a coherent road map to improve cyberresilience.

12. Each of the individual recommendations will be further examined so that they can be costed in terms of effort and potential impact. Proposals and costs will then be presented for prioritization and guidance to the IT Governance Committee, which includes senior representation from all three Office portfolios. Based on the decisions taken by the Office in the light of that guidance, it is proposed that progress reports should be incorporated into the documents providing updates on the ILO's IT strategy that are presented to the Governing Body annually.

▶ Draft decision

13. **The Governing Body took note of the information contained in document GB.346/PFA/3 and requested the Office to take into account its guidance in following up on the recommendations of the review.**

▶ Appendix I

Alignment with the JIU cyberresilience pillars

Pillar 1 – Engaging with legislative and governing bodies

JIU guidance

- Governing bodies should provide high-level strategic guidance, including through the formulation of an explicit risk appetite statement.
- Organizations should develop a reporting framework that collects and shares relevant cybersecurity metrics with legislative and governing bodies and anticipate escalation protocols to be followed in the event of attack.

Findings

In its report, the JIU observed several examples across UN system agencies where corporate enhancements to cybersecurity frameworks had originated from oversight recommendations. Engagement with legislative bodies was also identified within the Office.

- The position of IT security officer was initially created at the recommendation of the Governing Body.
- The Governing Body is informed of cybersecurity risks through multiple channels, including:
  - reports on information security audits by the Office of Internal Audit and Oversight;
  - reports by the Independent Oversight Advisory Committee (based on briefings by the Chief Information Security Officer); and
  - ad hoc cybersecurity incident reports presented to the IT Governance Committee through reports by the Chief Information Officer, which are also presented to the Governing Body where appropriate.

The Information Security and Assurance Services Unit has also defined a set of key risk indicators, although the set is not exhaustive. There is a generic reference to risk appetite in the Office's risk management framework document. Specific reference is made to the risks of cyberattacks on ILO systems (risk event 8) in the strategic risk register included in the Programme and Budget for the biennium 2022–23. Nevertheless, cybersecurity risk tolerance baselines defined to guide operational teams could be clearer.

Recommendations

- The IT Governance Committee should clarify the acceptable levels of cybersecurity risk based on input from the Governing Body.
- The IT Governance Committee should be briefed annually on common information security issues, trends, risks and opportunities, based on an analysis of industry trends, audit reports, risk registers, information security risk assessments, investigations and incident data.

Pillar 2 – Embedding cybersecurity into organizational risk management

JIU guidance

- Increase emphasis on developing effective and meaningful risk mitigation measures in conjunction with robust business continuity planning.
- Cybersecurity experts should be fully involved in the design, implementation and monitoring of internal risk management processes.

Findings

In its report, the JIU affirmed that embedding cybersecurity formally in an organization's enterprise risk management framework contributes to elevating the subject among diverse organizational priorities. The Office has established an enterprise risk management system, which is governed by the Senior Risk Officer, who reports to the Treasurer and Financial Comptroller. The system incorporates a strategic risk register that includes a risk relating to disruption from cyberattack. Information security risks are also captured at the operational level, with the Information and Technology Management Department (INFOTEC) and the Information Security and Assurance Services Unit contributing to the risk register. These risks are also often referenced in country office risk registers. There were, however, some limitations with organizational risk management.

- There is scope for further clarification within the enterprise risk management system of information security-related risks.
- The coherence of risk management operations between headquarters and some development cooperation-funded projects is limited. There is some delegation of risk management responsibilities. Information security risk management across development cooperation projects is inconsistent.

Recommendation

- The integration of information security risk management into the enterprise risk management system should be enhanced and risk management practices should be applied to information security management in order to facilitate the prioritization of resources to achieve the greatest impact.

  This recommendation is repeated under pillar 9.

Pillar 3 – Building on the convergence between physical security and cybersecurity

JIU guidance

- Integrate physical safety and security and cybersecurity management frameworks within corporate architecture.
- Upskill cybersecurity capacity inside the physical safety and security function.

Findings

In its report, the JIU observed blurred lines between physical security and cybersecurity, whereby information and communications technology systems are increasingly used to support physical security, and security incidents sometimes involve breaches across both

domains. Despite the blurring lines between them, physical and cyber domains are still generally treated as two separate domains within the Office.

- Physical security is managed by the Internal Services and Administration Department (INTSERV) in accordance with the policies of the UN security management system.
- Cybersecurity is managed by the Information Security and Assurance Services Unit in alignment with the ISO 27001 standard.

Each team has implemented multiple controls within their respective domains and INTSERV collaborates with INFOTEC to support identity and access management controls. A gap was observed, however, stemming from the converging domains and relatively low level of cybersecurity expertise within the INTSERV team, namely that the network of internet of things devices [1] supporting physical security has not been assessed for compliance with cybersecurity standards.

Recommendation

- A risk assessment and security testing of the internet of things network should be conducted.

Pillar 4 – Shaping regulatory frameworks for compliance and accountability

JIU guidance

- Create simple, non-technical and engaging language and messaging that focuses on making the consequences of risky cyberbehaviour palpable for the individual.
- Reinforce individual accountability for incidents of poor cyberhygiene. Develop nuanced means of dealing with non-compliance that are commensurate with the severity of the infraction, to encourage individuals to take responsibility for risky practices.

Findings

In its report, the JIU observed that references to cybersecurity should be included in strategic, policy, procedural and technical guidance documents. This is a practice that was observed at the ILO during the cyberresilience maturity assessment.

- The Information Security and Assurance Services Unit references the ISO 27001 standard as part of the implemented information security management system.
- The suite of documents related to the information security management system covers a range of technical control domains. However, some of the documents could be reviewed more frequently and some of the stakeholders interviewed appeared to have difficulties understanding them. There is some inconsistency concerning staff appreciation of data value and the gravity of cyberbreaches. This has resulted in the inconsistent implementation of cybersecurity controls and processes across the Organization. In addition, there were suggestions that information security assessment recommendations are not always implemented with the same rigour as audit recommendations.

[1] The operational network made up of sensors and devices that automate and manage some of the daily operations of running the ILO's property and facilities.

- Standard disciplinary procedures used by human resources in the UN system to sanction staff who breach policies and standards are applied within the ILO; however, security awareness activities have been irregular during the pandemic. Re-instating these activities on a regular basis will be necessary to reinforce understanding of individual accountabilities.
- Some system owners, including across development cooperation projects, have elected not to comply with the information security policies and standards established by the Information Security and Assurance Services Unit.
- The ILO has a number of mechanisms for managing and processing serious reports of misconduct, as well as a whistleblower protection framework; however, these mechanisms do not generally deal with reports made within the context of cybersecurity. There is also a monitoring and incident response capability; however, that is primarily focused on technology-related security incidents.

Recommendations

- An Organization-wide programme should be developed to lift the ILO's information security culture; the programme should incorporate:
  - actions that senior managers can adopt to model good cybersecurity practices;
  - targeted communications that adopt non-technical and engaging language to make the consequences of risky cyberbehaviour easily understandable for all individuals;
  - role-based information security awareness training; and
  - accountability controls establishing clear individual responsibilities for maintaining good cyberhygiene.

  The findings under pillars 6, 7 and 8 also led to this recommendation.
- Security risk-based guidelines and checklists should be developed to assist development cooperation project managers in understanding how to protect their data and systems, within the agreed risk appetite. Security checkpoints should be incorporated (and minimum security baselines formalized) within system acquisition, development and maintenance frameworks.

  The findings under pillar 7 also led to this recommendation.

Pillar 5 – Harnessing the contributions of oversight mechanisms

JIU guidance

- Develop procedures to ensure that the knowledge and experience of the cybersecurity experts within an organization can systematically inform and feed into the work of the oversight function.

Findings

The report of the JIU contains several examples of cases where enhancements to cybersecurity have originated from oversight recommendations, thus highlighting the value of such recommendations. The Office maintains oversight functions, including those described below.

- Operational oversight is delivered through the monitoring of the Information Security and Assurance Services Unit's key risk indicators, incident investigation and reporting and the risk management framework.
- Strategic oversight is delivered through management reviews performed by the IT Governance Committee, reviews by the Chief Information Officer of the Information Security and Assurance Services Unit's work plan, and Governing Body reviews of the IT strategy and audit, evaluation and oversight reports. While the Information Security and Assurance Services Unit often contributes to these strategic oversight functions, there are no documented operating procedures to ensure consistent and effective engagement with the Information Security and Assurance Services Unit during the reviews.
- Independent audits are performed by:
  - external auditors – an independent auditor is engaged to facilitate ISO 27001 certification of the information security management system; however, information security for information and communications technology systems not managed by the Information Security and Assurance Services Unit are outside the scope of the audit; and
  - internal auditors – the Office of Internal Audit and Oversight performs two or three information security audits per year. Audit domains are selected using a risk-based approach. In addition, penetration test audits are conducted jointly by the Office of Internal Audit and Oversight and external consultants. The last such audit occurred in 2019 and another one is planned for 2022.

Recommendation

- Additional key performance indicators for measuring the effectiveness of cybersecurity controls and the management of remediation activities should be developed and monitored.

Pillar 6 – Instilling a cybersecurity culture from the leadership down

JIU guidance

- Ensure that senior leadership is aware of the associated risks and implications of inaction and poor cyberhygiene.
- Instil a culture that views the occurrence of incidents as a starting point for addressing a shared problem for better protecting the organization, and not as a failure.

Findings

In its report, the JIU recognizes that executive management awareness and accountability is a starting point, and that leadership needs to encourage the acknowledgment of mistakes and vulnerabilities.

The Office's leadership team is kept informed of cybersecurity risks and issues through several reporting channels (as outlined above in connection with pillar 5). Leadership commitment is demonstrated strategically through the establishment of the Information Security and Assurance Services Unit; support for the certification of the information security management system; and the endorsement of cybersecurity policies, standards and procedures.

While the Information Security and Assurance Services Unit and supporting teams (for example, in the areas of enterprise risk management, business continuity, IT governance, and

internal audit and oversight) have been established, there are still constraints across the Office that have impacted its cybersecurity posture.

In addition, while leadership also supports non-monetary ways of influencing culture and behaviours through simulated phishing campaigns and actively participates in cybersecurity initiatives (for example, external audits), there is always scope for enhancement through visible participation in other awareness-raising programmes.

Recommendations

- A holistic review of information security resourcing and responsibilities across the Organization should be conducted with a view to enhancing compliance with existing security controls and ensuring greater coherence between information security and risk management.

  The findings under pillar 9 also led to this recommendation.

- An Organization-wide programme should be developed to lift the ILO's information security culture, as outlined in the recommendation under pillar 4.

Pillar 7 – Implementing a whole-of-organization approach

JIU guidance

- Decentralize and delegate authority to mid-level managers.
- Spell out related cyberresponsibilities for all roles and deliver role-based cybersecurity training and awareness-raising activities.

Findings

In its report, the JIU reiterates that there is a growing understanding that cybersecurity is not solely an IT responsibility. This is recognized broadly with the assignment of information security responsibilities beyond the Information Security and Assurance Services Unit and INFOTEC; however, some limitations with decentralizing responsibilities across the Office exist.

- Cybersecurity considerations are not mainstreamed into the work procedures of teams. For example:
  - the embedding of cybersecurity controls within programme and project management procedures is limited, so that security controls are inconsistently adopted by different projects and teams; and
  - cybersecurity processes are inconsistently implemented across country offices.
- Minimal role-based cybersecurity training is delivered to all staff.

Recommendations

- An Organization-wide programme should be developed to lift the ILO's information security culture, as outlined in the recommendation under pillar 4.
- Security risk-based guidelines and checklists should be developed to assist development cooperation project managers, as outlined in the recommendation under pillar 4.

Pillar 8 – Establishing the workforce as the first line of defence

JIU guidance

- Establish the basic digital literacy of each member of the workforce and empower users to play an active role in improving cyberresilience.
- Develop a training and awareness-raising programme with clear objectives defined for each category of stakeholder, in accordance with the risks they present for the organization.

Findings

There is a growing realization of the importance of the "human factor" in cybersecurity, with global recognition that individual end users are being increasingly targeted. The Office understands the need for users to be sufficiently vigilant to provide a first line of defence; therefore, induction training incorporating information security awareness is mandated for all staff. Other ad hoc communications and awareness-raising activities (for example, simulated phishing campaigns as per pillar 6, and the distribution of threat intelligence notices) contribute to enhancing user attentiveness.

There are, however, limitations that potentially compromise current levels of vigilance.

- There is a high completion rate for induction training, but this does not provide sufficient assurance of actual behavioural change.
- Regular awareness training and role-based training is not delivered to all staff (as per pillars 4 and 7).

Recommendation

- An Organization-wide programme should be developed to lift the ILO's information security culture, as outlined in the recommendation under pillar 4.

Pillar 9 – Optimizing resource allocation for cybersecurity

JIU guidance

- Identify where cybersecurity resources should be allocated to have the most meaningful impact.
- Link cybersecurity investments with business requirements and sound risk management practices to avoid overspending and underresourcing in key business areas.

Findings

In its report, the JIU recognizes that, despite increases in the resources allocated to cybersecurity, perceived resource shortages remain an obstacle to covering all aspects of cyberresilience. Discussions with senior ILO managers indicated that inadequate resourcing compromised progress on various activities contributing to cybersecurity weaknesses across multiple domains, such as asset and vulnerability management, the governance of development cooperation projects, data governance and the monitoring of some aspects of information security management.

Recommendations

- A holistic review of information security resourcing and responsibilities across the Organization should be conducted, as outlined in the recommendation under pillar 4.
- The integration of information security risk management into the enterprise risk management system should be enhanced and risk management practices should be applied to information security management in order to facilitate the prioritization of resources to achieve the greatest impact (as outlined in the recommendation under pillar 2).

Pillar 10 – Investing in dedicated and specialized human resources

JIU guidance

- Retain internal expert capacity for cybersecurity. [2]

Findings

Many UN system agencies have built specialized human resource capacity for cybersecurity in-house, and this includes the ILO.

- The Office has appointed a full-time Chief Information Security Officer, who leads the Information Security and Assurance Services Unit's team of dedicated cybersecurity experts. The team's responsibilities have evolved over time and include both security operations services and the governance of cybersecurity.
- The Information Security and Assurance Services Unit also engages external cybersecurity expertise to deliver additional information security services, such as threat intelligence services and security monitoring, incident response and penetration testing services. [3]

In its report, the JIU stresses that it is important to safeguard the opportunity for cybersecurity considerations to be voiced and heard by responsible decision-makers without restriction. This is irrespective of the organizational placement of cybersecurity, whether in the information and communications technology department or independent from it.

No restrictions are placed on the Chief Information Security Officer or the Information Security and Assurance Services Unit in terms of voicing their cybersecurity-related opinions to responsible decision-makers, although there may be opportunities for enhancing how cybersecurity considerations contribute to other corporate frameworks, such as those on enterprise risk management, information and knowledge management, physical safety and security, and oversight.

[2] Conflicts of interest should be avoided where the team providing oversight should be separate and independent from the team responsible for delivering cybersecurity services.

[3] An external company is responsible for managing the Network Operations Centre and Security Operations Centre for the Office.

▶ Appendix II

Road map to improved cyberresilience

JIU pillar	Recommendation
1	The IT Governance Committee should clarify the acceptable levels of cybersecurity risk based on input from the Governing Body.
1	The IT Governance Committee should be briefed annually on common information security issues, trends, risks and opportunities, based on an analysis of industry trends, audit reports, risk registers, information security risk assessments, investigations and incident data.
2, 9	The integration of information security risk management into the enterprise risk management system should be enhanced and risk management practices should be applied to information security management in order to facilitate the prioritization of resources to achieve the greatest impact.
3	A risk assessment and security testing of the internet of things network should be conducted.
4, 6, 7, 8	An Organization-wide programme should be developed to lift the ILO's information security culture.
4, 7	Security risk-based guidelines and checklists should be developed to assist development cooperation project managers in understanding how to protect their data and systems.
5	Additional key performance indicators for measuring the effectiveness of cybersecurity controls and the management of remediation activities should be developed and monitored.
6, 9	A holistic review of information security resourcing and responsibilities across the Organization should be conducted.