

UN OPERATIONAL RISKS

	ADMINISTRATIVE RECORDKEEPING RISKS	UN ORGANIZATIONAL RISKS				POTENTIAL RISK MITIGATION STRATEGIES
A1	Poor information management governance, resulting in reduced accountability and efficiency.	Operational risk	Financial Risk	Image risk	Physical risk	
1	An inadequate recordkeeping regime does not give ARMS the scope or authority to address and enforce records management and archival programs adequately.	X	X			Revise ST/SGB/2007/5, as recommended by the OIOS audit, to address current recordkeeping needs across the UN.
2	The ARMS low profile leaves it marginalized, unable to implement fundamental recordkeeping principles in the UN.	X		X		Raise the profile of ARMS by highlighting its critical role to support efficient, effective, and accountable recordkeeping.
3	The lack of resources for recordkeeping does not give ARMS the ability to develop and implement the tools, guidance, and governance structures necessary to protect the UN's information resources.	X	X			Increase and stabilize UN resources for recordkeeping so they are adequate to the task of providing accountable records and information management support for the UN system.
4	Recordkeeping requirements are not incorporated into organizational planning or operations, resulting in poor and inadequate recordkeeping across the UN system.	X		X		Incorporate mandatory recordkeeping requirements into all UN operations, including in requirements for project planning and execution, departmental management and reporting, and other business processes and workflows.
5	In the absence of strong and mandatory recordkeeping requirements, departments and offices across the UN develop independent records and archives functions, reducing the ability of ARMS to provide consistent and accountable IM governance across the UN system.	X		X		Strengthen the authority of ARMS to establish and enforce recordkeeping standards and make compliance with recordkeeping requirements mandatory. Consider building on the UN's existing "accountability architecture" which defines integrity, performance, and compliance and oversight as three performance pillars for accountability in UN operations.

UN OPERATIONAL RISKS

6	Accountability for departmental or project recordkeeping is not clear or mandated, there is little or no “top-down” endorsement for accountable recordkeeping, and the UN does not identify the owners of risks. The result is a lack of control over operations and over records management.	X		X		Incorporate recordkeeping responsibilities into Senior Manager Compacts, staff job descriptions, project plans, and associated staff guidance to identify clear and accountable roles and responsibilities for recordkeeping.
7	Weak or complicated business processes result in complicated and inadequate records and information systems; documenting poor business processes is more challenging and time consuming than documenting efficient operations.	X	X			Develop partnerships and liaisons with appropriate agencies across the UN to support improved business processes and to incorporate recordkeeping requirements into streamlined and efficient business processes and workflows.
A2	Inadequate change management strategies for RIM, hindering the organization’s capacity to incorporate recordkeeping requirements into changing business processes and operational activities.	Operational risk	Financial Risk	Image risk	Physical risk	
1	The UN operates in a highly independent environment, with little centralized oversight and slow change at the highest levels; offices develop their own recordkeeping and IT approaches to address immediate operational needs.	X	X			Encourage the development of a corporate approach to records and information management, in order to increase accountability, improve efficiency, maximize effectiveness, and speed up delivery of services across the UN system.
2	Staff are resistant to change and/or do not feel empowered to facilitate change themselves. People often accept poor processes rather than press for change.	X		X		Identify specific requirements for recordkeeping and train people at all levels to fulfill their assigned responsibilities, so they are empowered to act in accordance with corporate recordkeeping requirements.
3	Changes to organizational structures, staff complements, and duties and functions are common, resulting in changed priorities, ad hoc records systems, and lack of continuity.	X	X			Embed recordkeeping requirements in job descriptions, project plans, operational guidelines, and other organizational tools that outlast the tenure of individual staff members, to improve continuity of service.
4	The UN does not foster a corporate approach to information management; records management is seen as a burden, not a benefit. Since poor recordkeeping is not deemed high risk issue, staff develop ad hoc and non-compliant processes.	X	X			Increase the authority of ARMS to oversee and ensure compliance with recordkeeping requirements, to increase organizational accountability and improve efficiency across the UN system.

UN OPERATIONAL RISKS

5	Current initiatives to reduce paper and improve efficiency – such as Paper-light and SmartOffice – do not include recordkeeping requirements, despite ARMS efforts, resulting in gaps in accountability and efficiency.	X	X			Require compliance with recordkeeping requirements for all IT, IM, and efficiency initiatives that involve the creation or management of records, including an increased and formalized role for ARMS in project planning and execution.
6	Budget reductions are driving operational change – including, for example, the growth of global service centers – without the inclusion of recordkeeping requirements.	X	X			Highlight the critical value of effective recordkeeping for reducing costs and increasing success, particularly with the development of integrated or consolidated service centers or information resources.
7	In general, UN toolkits do not include implementation guidance and often do not reach the people who would most benefit from the training, resulting in poor application of training and guidance and weak recordkeeping.	X		X		Incorporate consistent recordkeeping guidance in all UN training and guidance tools and increase opportunities to provide specific guidance on implementation and “how to” create and manage records effectively, to increase compliance and encourage staff support for recordkeeping.
A3	Weak RIM emergency management measures, diminishing the organization’s ability to protect its human, financial, and information assets.	Operational risk	Financial Risk	Image risk	Physical risk	
1	The absence of clear and formalized roles and responsibilities for recordkeeping increases the risk of loss to sensitive and operational information, especially during high-risk situations such as UN peacekeeping operations and urgent “pull out” actions, where securing records is a low priority compared with transporting staff or material assets.	X			X	Identify vital and business critical records for different UN operations and develop mechanisms for securing those records – and managing other UN information resources – during emergencies or high-risk situations, so that the UN’s vital information assets are protected.
2	The significant lack of understanding of or identification of vital records across the UN places the organization’s information assets at risk. Staff do not know how to identify vital records and often over-interpret the term to mean any records they need access to at a particular time.	X			X	Train UN staff to understand the nature and scope of vital and business critical records and the need to manage records effectively in order to remove unwanted information and ensure business critical information is managed appropriately. Centralize vital records planning within ARMS to ensure the “right” records are identified and managed.

UN OPERATIONAL RISKS

3	Environmental threats and emergencies such as the threat of a flu pandemic and the experience of Super Storm Sandy in New York highlight the need for improved business continuity planning, but recordkeeping has not been included adequately in the development of business continuity plans.	X			X	Develop recordkeeping guidance to support business continuity plans and train UN staff to understand the importance of incorporating records care into business continuity processes and emergency response measures, based on a precise and formally confirmed list of vital records.
4	The significant weakness in the UN's backup and data systems was highlighted during Super Storm Sandy, but efforts to address emergency actions and business continuity processes have not incorporated adequate steps to identify and protect authentic and reliable records.	X			X	Strengthen guidance for identifying and protecting corporate records in emergency response and business continuity plans, and increase the role of ARMS in developing business continuity plans and participating in emergency response actions, in order to ensure the organization's vital and business critical records are adequately protected in an emergency.
5	Specific information systems across the UN do not include the identification of records, let along vital or business critical records, and the UN has not implemented availability requirements for access to systems and records have not been consistently developed, to ensure access to business critical information after an emergency.	X			X	Incorporate recordkeeping guidance in specific information systems control documentation, including, for example, specific guidance on identifying, securing, protecting, and accessing vital or business critical records – such as guidance about how to ensure access to business critical information one, four, or six hours after an emergency.

B	RECORDS CONTROL RISKS	UN ORGANIZATIONAL RISKS				POTENTIAL RISK MITIGATION STRATEGIES
B1	Incomplete or inadequate records classification systems, resulting in lack of control over the creation and management of official records.	Operational risk	Financial Risk	Image risk	Physical risk	
1	The absence of classification schemes and retention schedules in 50% of the UN organization results in serious risk. The creation, management, and disposition of records cannot be controlled without formal and authorized classification and retention systems in place and without the expectation that departments will and must comply with the requirements outlined in those tools.	X			X	Complete the development of all retention schedules and associated classification schemes and requirements as a high priority task. Provide ongoing support for the implementation of these schemes and requirements in departments and offices, and develop the infrastructure required to ensure compliance.

UN OPERATIONAL RISKS

2	The implementation and use of records classification systems for UN departments and offices are inadequately monitored, leading to confusion, lack of compliance, and inadequate protection of the organization's official records.	x			x	Develop and implement assessment and monitoring mechanisms for determining compliance with classification and retention requirements, including quantitative and qualitative assessments of recordkeeping operations within UN offices.
3	UN departments and offices do not effectively manage versions of records or identify and distinguish between masters, duplicates, and convenience copies of records. The poor application of records identification and classification processes results in excessive duplication and retention of unwanted records (such as multiple versions or drafts of records), along with uncontrolled destruction of records with ongoing value.	x			x	Develop or enhance and implement guidance for version control, distinguishing masters from duplicates or convenience copies, and classifying and managing records according to formal recordkeeping requirements. Develop monitoring mechanisms to ensure compliance with these requirements.
B2	Absence of or inability to enforce records retention and disposal requirements, resulting in excessive retention of unwanted records and loss of valuable evidence.	Operational risk	Financial Risk	Image risk	Physical risk	
1	As noted by OIOS, only 11 of 28 UN Secretariat departments or offices have retention schedules; another four have only partially implemented retention schedules. There is little or no systematic transfer of records to ARMS, and there is widespread unauthorized destruction of records across the agency. The result is poor and unaccountable recordkeeping, leaving gaps in the UN's institutional memory, increasing the risk to the UN's operations through inadequate information management.	x			x	Complete the development of all retention schedules and associated classification schemes and requirements as a high priority task. Provide ongoing support for the implementation of these schemes and requirements in departments and offices, and develop the infrastructure required to ensure compliance.

UN OPERATIONAL RISKS

2	The absence of formal and enforceable retention/disposal requirements for audio-visual and multimedia records, particularly UN broadcast materials (such as in the multimedia asset management system or MAMS) results in the retention of vast quantities of digital data, much of which does not have on-going value but which will be “lost” within uncontrolled digital repositories if no recordkeeping guidelines are established.	x			x	Develop and implement retention schedules and associated classification schemes and requirements for the management of audiovisual materials, including processes and guidelines for the disposal of obsolete or superseded materials. Develop monitoring mechanisms to ensure compliance with these requirements.
B3	Weaknesses in the storage and protection of physical or digital records, placing information resources at risk, especially during emergencies.	Operational risk	Financial Risk	Image risk	Physical risk	
1	The absence of rigorous and formalized security and backup processes, including the absence of adequate physical or virtual offsite storage mechanisms for paper or electronic records, leaves the UN’s information assets vulnerable to loss or damage.	x			x	Support the establishment of information security controls and backup processes for recordkeeping systems across the UN, and develop and implement necessary training, guidance, procedures, and monitoring or evaluation to ensure compliance.
2	The lack of attention to the long-term preservation of digital information – including digital preservation and migration strategies – results in serious risk to the ability of the UN to capture, use, manage, preserve, and access its electronic records now and into the future.	x			x	Continue to develop ARMS requirements for digital preservation and incorporate requirements and guidance into recordkeeping strategies, procedures, and guidance applicable across the UN system.
3	There are gaps in records management training and guidance particularly related to the care and management of non-traditional records, including: electronic records, special format records such as audiovisual or multi-media materials, records associated with GIS systems, records in or generated from databases, and records and information housed in software or tools that do not automatically create records outputs but hold authoritative information required as evidence to support actions, transactions, and decisions.	x			x	Develop training, guidance, and procedures for managing records in all media, including non-traditional records, and develop and implement mechanisms for monitoring and evaluation to ensure compliance.

UN OPERATIONAL RISKS

C	LEGAL/REGULATORY CONTROL RISKS	UN ORGANIZATIONAL RISKS				POTENTIAL RISK MITIGATION STRATEGIES
C1	Operating within inadequate or obsolete regulatory frameworks, preventing the organization from implementing accountable recordkeeping systems.	Operational risk	Financial Risk	Image risk	Physical risk	
1	There is a significant lack of control over the creation and management of electronic records across the UN. As noted by OIOS, retention policies, including the retention policy for records common to all UN offices (RCUN), do not apply to electronic records, and the UN has not addressed the need to identify and select authoritative records forms, such as electronic versus paper.	X		X		Develop criteria and requirements for selecting electronic or physical records as authoritative, as appropriate to different business functions and activities. Incorporate the criteria into retention and disposal schedules, and work with UN offices to implement these requirements and ensure compliance.
2	The UN has adopted a risk management policy (May 2011), but records and information resources have not been identified as tools for addressing or mitigating risk. The result is a critical gap in the risk management framework, because the creation, management, and protection of authoritative and reliable records have not been recognized as core components of effective risk management.	X		X		Incorporate recordkeeping requirements into risk management policies and strategies, in order to ensure the UN recognizes and adopts necessary records protections as a core component of risk management. Use the organizational and recordkeeping risk categories identified in this report as a baseline, if appropriate.
3	The UN is developing mechanisms to adopt digital signatures as authoritative, but recordkeeping and accountability requirements have not yet been taken into account adequately. There is potential for confusion between paper and electronic records, since it is not clear if and when electronic records are deemed acceptable. There is also a lack of accountability for the management of electronic records with digital signatures, if they are not protected adequately.	X			X	Develop criteria and requirements for ensuring the authenticity of digital signatures, the identification of electronic records as official, and the effective management of information systems that hold authentic digital records. Work with UN offices to implement these requirements and ensure compliance.

UN OPERATIONAL RISKS

C2	Unsatisfactory management of organizational and public requirements for access, privacy, and transparency, increasing the risk of security breaches.	Operational risk	Financial Risk	Image risk	Physical risk	
1	Trustworthiness is important to the UN, but poor records management hinders the ability of the organization and stakeholders to access information needed to support public accountability as exemplified in the Oil for Food case, where the UN strives to make records available but has not implemented the recordkeeping mechanisms necessary to ensure those records are retrievable.	X		X	X	Strengthen the authority of ARMS to establish and enforce recordkeeping standards and make compliance with recordkeeping requirements mandatory, ensuring that records remain authentic, reliable, and trustworthy.
2	Accidental unauthorized disclosure of private, sensitive, or classified information is a great risk for the organization. Security classifications are not applied consistently and the protection of privacy is not explicitly addressed in recordkeeping requirements and guidance.	X		X	X	Improve the application and enforcement of security classifications, so that procedures are robust, consistent, and controlled.
3	The UN is not bound by the kind of access and privacy requirements that govern access in national governments; consequently the declassification of records follows a traditional 20-year rule process. That declassification process is at risk because of poor and uncontrolled recordkeeping practices, resulting in excessive closure of records that should be available, along with the inadvertent premature release of records that should be closed.			X	X	Ensure declassification processes happen in a timely and consistent manner in order to ensure records become publicly available according to policy, not in an ad hoc manner. Establish, apply, and enforce retention periods to ensure records are managed appropriately and disposed of, including becoming publicly available, according to formal requirements.

UN OPERATIONAL RISKS

4	There is a move to encrypt the content held in electronic information systems, but encryption policies and procedures have not been formalized. The result is either excessive or inappropriate encryption, the loss of records because decryption processes are not known to appropriate personnel, and the inconsistent application of electronic technologies to govern digital access and restriction.			x	x	Establish formal, consistent, and accountable policies and procedures for encrypting content, including authorizing appropriate staff to carry out encryption and decryption procedures and preventing unauthorized encryption, which can result in in confusion and loss of records or information.
C3	Inadequate management of records in order to respond effectively to litigation, audits, or other accountability requirements, affecting the organization's ability to remain accountable for its actions.	Operational risk	Financial Risk	Image risk	Physical risk	
1	The culture of using information to support decision making is not strong within the UN. People do not turn to records as valuable information resources, even though those records hold critical information that would greatly inform decision making.	x		x		Incorporate mandatory recordkeeping requirements across the UN, to ensure all staff create, manage, and protect information assets for their evidential value. Based on these mandatory requirements, develop awareness raising, training, and guidance tools to communicate the value of authentic and reliable records and the critical importance of complying with recordkeeping requirements.
2	There is a general absence of recordkeeping criteria in UN audits and assessments. Poor recordkeeping is not formally recognized as a high-risk issue for the UN, and consequently the processes of records creation, management, and protection are not measured. Without formal assessments, improvements to recordkeeping cannot become a priority and the UN remains at risk because its information and records resources are not managed as accountable evidence of the organization's actions, transactions, and decisions.	x		x		Incorporate measurable recordkeeping criteria in UN audits, and develop and implement recordkeeping assessment tools across the organization, to document and measure compliance with, or lack of compliance with, essential records management actions.

UN OPERATIONAL RISKS

3	The lack of resources for recordkeeping across the UN does not give ARMS the ability to conduct risk-based inspections of records management practices or to develop and implement the tools, guidance, and governance structures necessary to protect the UN's information resources.	X		X		Increase resources for ARMS operations, particularly for the development and implementation of recordkeeping assessments, monitoring, training, and governance. Expand ARMS' responsibility for recordkeeping to support the work of departments and offices, ensure accountability for actions, and enhance the efficiency and effectiveness of operations.
---	--	---	--	---	--	--

D	TECHNOLOGY RISKS	UN ORGANIZATIONAL RISKS				POTENTIAL RISK MITIGATION STRATEGIES
D1	Weak information security through inadequate mechanisms and tools for creating, accessing, sharing, and storing records, resulting in an increased risk of security breaches.	Operational risk	Financial Risk	Image risk	Physical risk	
1	In common with other large organizations, the UN faces major threats from cyber-attacks, particularly related to inappropriate access to email accounts. The lack of control over email accounts and general lack of control over the creation, management, and disposal of electronic mail is a major threat to UN information security.			X	X	Develop and enforce recordkeeping and information security requirements for the use of email and other digital technologies, in order to ensure records are protected from inappropriate access or unauthorized destruction or change.
2	User accounts, such as those used to access email or electronic tools, are not tracked, and controls are not in place to manage passwords or access. When staff leave, their accounts are not well managed, and successors may not have access to password protected documents.			X	X	Develop, implement, and enforce mechanisms for controlling and managing user accounts for all electronic technologies and tools, in order to minimize the risk of unauthorized or inappropriate access.
3	The UN is underfunded in terms of information security, and as a result there are weaknesses in the protection, disclosure, integrity, and availability of information. Accountability is tied to integrity, both of which relate to effective protection of authentic and reliable information.			X	X	Increase resources for the creation of effective and enforceable information security mechanisms, and incorporate recordkeeping requirements into those information security processes to ensure the UN's information resources are adequately protected.

UN OPERATIONAL RISKS

4	The UN is rapidly adopting social media tools without taking into account the recordkeeping or accountability requirements for creating, managing, and disseminating official information using such tools.			x	x	Establish, implement, and enforce policies, procedures, and guidelines for the use of social media, including recordkeeping requirements, to ensure the UN's information resources are adequately protected regardless of the technologies used to create, share, manage, or store them.
D2	Uncontrolled use of information and communications technologies, increasing security risks.	Operational risk	Financial Risk	Image risk	Physical risk	
1	There is widespread and ungoverned use of commercial tools and technologies such as shared drives, SharePoint, Dropbox, Drupal, Al Fresco, Google Drive, and cloud computing. There is an extreme risk to the authenticity and security of records and information associated with this uncontrolled proliferation of information and communications technologies and absence of recordkeeping requirements.	x			x	Develop, implement, and enforce recordkeeping and information security requirements for the use of all commercial or externally managed information and communications tools and technologies, in order to ensure necessary recordkeeping protections are incorporated and maintained. Monitor the use of information and communications tools and establish mechanisms for decommissioning them, for removing and protecting authoritative records, and for destroying obsolete records when the tools are no longer in use.
2	There is widespread and uncontrolled development of internally developed information and communications systems and technologies, including SAP, Umoja, inspira, and web technologies, without adequate attention to recordkeeping requirements or information security/privacy/access controls.	x			x	Develop, implement, and enforce recordkeeping and information security requirements for the development of all internally developed information and communications tools and technologies, in order to ensure necessary recordkeeping protections are incorporated and maintained. Monitor the use of internally developed information and communications systems and technologies and establish mechanisms for decommissioning them, for removing and protecting authoritative records, and for destroying obsolete records when the systems are no longer in use.
3	There is little or no control over the use and management of email across the UN, despite the prevalence of email as a tool for creating and disseminating official communications.	x			x	Strengthen and enforce existing requirements for email management, or develop new requirements, and establish, implement, and enforce more robust guidelines for identifying and protecting official records created or received using email technologies.

UN OPERATIONAL RISKS

D3	Poor management of software applications, leading to confusion about whether systems hold reliable and authoritative records.	Operational risk	Financial Risk	Image risk	Physical risk	
1	There is widespread and ungoverned use of commercial recordkeeping software products, such as Documentum and FileNet (for Unite Docs), dtSearch, Prodagio, and other electronic correspondence logs(for the management of legal records), and other software tools for document and information creation and management. There is an extreme risk to the authenticity and security of records and information associated with this uncontrolled proliferation of software products and tools that create, capture, manipulate, or store information resources.	x			x	Develop, implement, and enforce recordkeeping and information security requirements for the use of all commercial software products, in order to ensure necessary recordkeeping protections are incorporated and maintained. Monitor the use of software tools and establish mechanisms for decommissioning them, for removing and protecting authoritative records, and for destroying obsolete records when the products are no longer in use.