Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2017/081

Audit of management of websites and social media at United Nations Headquarters

Website management needed to be improved by utilizing the standard project management framework, decommissioning obsolete websites, performing network vulnerability assessments on a regular basis, and improving disaster recovery plans

14 August 2017
Assignment No. AT2016/580/01

Audit of management of websites and social media at United Nations Headquarters

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of management of websites and social media at United Nations Headquarters. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over the management of websites and social media at United Nations Headquarters. The audit covered the period from January 2016 to February 2017 and included a review of: project governance (including policies, data classification, data storage and retention, network security and design, access controls and disaster recovery); and information and communications technology (ICT) support system (including vulnerability assessments, site content controls and monitoring, data storage and preservation, and incident management).

The Department of Public Information (DPI) and the Office of Information and Communications Technology (OICT) had implemented some good practices for the management of social media and websites. Controls over data classification, social media content monitoring, and incident management were generally adequate. However, DPI needed to comply with the United Nations' project management methodology for website development projects and decommission obsolete websites. OICT needed to include regularly scheduled vulnerability assessments for website security and improve disaster recovery planning to include test plans, testing methodology and the frequency of testing.

OIOS made four recommendations. To address issues identified in the audit:

DPI, in collaboration with OICT, needed to establish a mechanism to ensure compliance with the requirements of the Organization's ICT project management framework for website development projects.

OICT needed to: (i) in collaboration with DPI, establish a monitoring process to identify obsolete websites and links, and a procedure and timeframe to decommission obsolete websites; (ii) establish regularly scheduled vulnerability assessments of websites and web-based applications, control access to the use of internal vulnerability scanning tools and monitor their use; and (iii) finalize the Headquarters disaster recovery plan document, including a detailed plan of activities to be executed for failover and failback and a standard procedure for annual testing of the disaster recovery plan for the Headquarters Webfarm.

DPI and OICT accepted the recommendations and have initiated action to implement them.

CONTENTS

Audit of management of websites and social media at United Nations Headquarters

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of management of websites and social media at United Nations Headquarters.

2. Internet publishing at United Nations Headquarters is regulated by the provisions of ST/AI/2001/5 which established the framework, criteria and procedures for the creation of internet sites. These normative instruments defined internet publishing as the provision of any textual, tabular, graphic or audio-visual material to the public through the internet by or on behalf of the United Nations.

3. Within the Secretariat, the use of internet, intranet and extranet support the dissemination and sharing of information, aspects of which are partly carried out by the Department of Public Information (DPI) and the Office of Information and Communications Technology (OICT) of the Department of Management (DM) in accordance with their respective mandates.

4. In recent years, there has been a proliferation of websites and social media channels created by the various departments and offices of the United Nations Secretariat. There were approximately 191 different websites and/or web presences (not including social media) of the Secretariat, with some sites hosted by OICT, DPI and the United Nations Global Service Centre in Brindisi, while others were hosted externally by third party providers. There has also been an increase in the use of social media (which included Facebook, Flickr, YouTube, LinkedIn and Twitter) by many departments and offices.

5. OICT is responsible for providing ICT support at United Nations Headquarters and, in cooperation with the Department of Peacekeeping Operations (DPKO) as appropriate, for lease lines and satellite communications to overseas duty stations. OICT also provides infrastructure support for enterprise-wide applications, consulting and advisory services to all offices of the Secretariat. These included measuring progress on an ongoing basis to ensure strategic alignment, quality control, and compliance with Secretariat-wide policies.

6. DPI was established to promote global awareness and understanding of the work of the United Nations. DPI did this through radio, television, print, the internet, video-conferencing and other media tools. The Department's mandate is to help fulfil the substantive purposes of the United Nations by strategic communication of the activities and concerns of the Organization to achieve the greatest public impact. While the concerned departments and offices of the Secretariat generated the information content, DPI, working in close cooperation with the media, Member States and civil society partners, was responsible for coordination and refinement of the content as well as its presentation and distribution.

7. The Strategic Communication Division (SCS) of DPI is responsible for broadening understanding of and support for the work of the United Nations based on the priorities given by Member States. SCS formulates communications strategies on priority issues and carries out communications campaigns to support the substantive goals of the Organization. It also manages a network of 63 United Nations information centres and offices around the world. Based on DPI's priorities for the year, SCS reached out to a global target audience through information products (websites, posters and publications), outreach activities carried out by information centres, and through the international media. The integration of social media platforms, including social networking tools such as Facebook, Twitter, Tumblr, Flickr and YouTube, was an increasingly important component of DPI's communication strategy.

8. Comments provided by DPI and DM are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

9. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over the management of websites and social media at United Nations Headquarters.

10. This audit was included in the 2016 risk-based work plan of OIOS due to risks associated with the management of websites and social media by the Organization.

11. OIOS conducted this audit from December 2016 to March 2017. The audit covered the period from January 2016 to February 2017. Based on an activity-level risk assessment, the audit covered higher and medium risk areas in the network and data security, which included: project governance (including policies, data classification, data storage and retention, network security and design, access controls and disaster recovery); and ICT support system (including vulnerability assessments, site content controls and monitoring, data storage and preservation, and incident management).

12. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; (c) review of network design and security; (d) sample testing which included a selection of websites hosted by DPI, OICT, and third party providers; and (e) identifying websites and pages/channels created on public social media and mitigation of the related risks. OIOS also tested a sample of web applications that were migrated from a legacy platform and the associated project management and data migration controls.

13. The audit included only public-facing websites created by the offices/departments of the Secretariat in New York. It did not include the Secretariat's intranet (i.e. iSeek) and websites created by Offices away from Headquarters, field missions, and regional commissions.

III. AUDIT RESULTS

A. Project governance

Need to comply with the project management methodology for web development projects

14. All ICT projects in the Secretariat are required to be managed in accordance with the ICT project management framework established by OICT. This framework is based on PRINCE2 (Projects in Controlled Environments) methodology, tailored to the Organization’s environment, and has clearly defined processes, steps and templates to control each ICT project.

15. OIOS reviewed a sample of website projects in both DPI and OICT and noted that projects to develop publicly accessible websites generally tended to be short-term and low cost (less than $200,000) which, according to the framework, did not require a business case. However, low cost projects were not exempt from following the ICT project management framework and handbook. OIOS review of specific website projects showed that on occasion, there was non-compliance with the requirements of the ICT project management framework. Specifically, the review showed that:

(i) The project to redesign and migrate the CTIFF (Counter-Terrorism Implementation Taskforce) website to Drupal (a free and open source content-management framework) contained a project initiation document, design requirements, end user documentation, and

consultant evaluation. However, it did not include other required elements such as project brief, formal project plans, status reports, formal testing documentation, and project closure.

(ii) The United Nations News Centre migration to Drupal project (currently in progress and in the testing phase) was not utilizing the ICT project management framework methodology or templates, and project documentation was not easily identifiable. DPI utilized JIRA (a project-management software application) and Agile software development methodology (an interactive methodology under which requirements and solutions evolve through the collaborative effort of cross-functional teams). However, this did not allow for the inclusion of principles of the ICT project management framework and therefore created a condition whereby essential steps could be excluded.

16. Non-compliance with the ICT project management framework could lead to inadequate project oversight and non-completion of projects in a timely manner, which may in turn affect the achievement of project goals.

(1) DPI, in collaboration with OICT, should establish a mechanism to ensure compliance with the requirements of the Organization's ICT project management framework for website development projects.

DPI accepted recommendation 1 and stated that it will work with OICT to establish a mechanism to ensure compliance with the requirements of the Organization's ICT project management framework for website development projects. The mechanism will define the conditions under which website initiatives should be considered ICT projects requiring the use of the PRINCE2 framework or can be treated as a Request for Service and be recorded and tracked accordingly. Recommendation 1 remains open pending receipt of evidence that a mechanism has been established to ensure compliance with the Organization's ICT project management framework for website development projects.

ICT policies relating to social media were being developed

17. The professional standards defined in the Control Objectives for Information and Related Technology (COBIT) framework recommend that an Organization should implement ICT controls for social media. Due to the nature of social media, preventive controls are limited and reliance must therefore be placed on policies, training, enforcement of policies, and monitoring of social media websites to guard against potentially harmful activities. In addition, legal review of social media policies should be included to ensure that they comply with liability and regulatory requirements.

18. OIOS reviewed DPI and OICT policies for websites and social media and noted the following:

(i) There were no formalized official United Nations policies on social media. There were two guideline documents for social media (the DPI Social Media Guidelines for DPI staff, interns, consultants, and volunteers, and United Nations Guidelines on the use of Internal Social Media), and the Secretary-General's bulletin regarding staff's personal use of social media. A draft official policy on the use of social media for the United Nations Secretariat was currently in progress.

(ii) DPI utilized a third-party service to provide reports to assist in monitoring the content of social media. However, there was no specific policy regarding monitoring requirements, reviews, follow-ups, or the related actions to be taken.

(iii) DPI had not yet implemented a recommendation from a previous OIOS audit of 2010 ("Audit of Internet publishing and use of social media at the United Nations Secretariat" – Assignment No. AT2010/520/01) which had recommended that user departments and offices consult with the Office of Legal Affairs (OLA) before entering into contractual agreements with external providers of social media services.

19. The absence of adequate social media policies and procedures for the use of social media exposed the Organization to reputational, legal and operational risks.

20. DPI was in the process of addressing the above weaknesses based on a recommendation made in an OIOS audit of the management of strategic communications activities in DPI (Report 2016/140) to finalize corporate social media policies and develop procedures for the governance and control over the creation and content management of social media accounts. Since this recommendation was being implemented, OIOS did not make an additional recommendation in the present report.

B. ICT support system

Data classification controls were generally adequate

21. The Secretary-General's bulletin ST/SGB/2007/6 on information sensitivity, classification and handling provides guidance on classification and handling of sensitive information. The COBIT framework for website development recommends the establishment of a data classification scheme based on criticality and sensitivity of enterprise data. For publicly accessible websites, this should include details about data ownership, appropriate security levels and protection control, and all websites should be registered and approved.

22. OIOS reviewed data classification controls for websites (there were approximately 191 websites across multiple departments, such as DPI, DM, the Department of Economic and Social Affairs, the Department of Safety and Security, and others). The review showed that: (a) websites developed and hosted by OICT and DPI were required to be registered and approved prior to their deployment or publication; (b) DPI and OICT maintained a content-based registry of websites; (c) security requirements including sensitivity of data and exposure were maintained in an application inventory; and (d) all websites and social media sites were required to have security requirements defined with security levels (unclassified, confidential, or strictly confidential) depending on the risk level.

23. Based on the review, OIOS concluded that data classification controls were generally adequate.

Social media content monitoring controls were generally adequate

24. The COBIT framework recommends that an organization should establish technical processes to adequately address the risk of unauthorized or fraudulent use of its brand on social media sites or other disparaging postings that could have a negative impact on the organization.

25. OIOS reviewed social media monitoring controls and noted that improvements had been made since the previous audit of the management of strategic communications activities in DPI as follows: (a) DPI took a proactive role in monitoring the main social media accounts (e.g. Facebook, Twitter, and Instagram); (b) an online risk management service was utilized to monitor and flag audience activity on social media accounts and alert DPI when suspicious words were used in posts; (c) DPI utilized the online risk management service to assist in filtering out abusive, offensive or inappropriate comments on the Facebook account; and (d) DPI enlisted three interns who monitored comments on all social media

platforms and reported and responded to comments approved by DPI when necessary. OIOS therefore concluded that the controls for monitoring the social media were generally adequate.

Need for timely review of obsolete or abandoned websites

26. An organization's public-facing websites reflect its professionalism and have a bearing on its reputation. Out of the 191 public-facing websites hosted by OICT and DPI, OIOS noted the following:

(i) Six websites appeared to be outdated or abandoned (i.e., referred to obsolete or no longer relevant);

(ii) Four websites had links that gave error messages (i.e., "service unavailable"); and

(iii) Two websites had been identified by DPI as apparently abandoned but they were not shut down because no response was received from the site owners.

27. This was due to the lack of a monitoring process to identify obsolete websites and links, and lack of a procedure to ensure the timely decommissioning of obsolete websites. The presence of abandoned or obsolete websites in the un.org domain could have a negative impact on the Organization's image.

(2) OICT, in collaboration with DPI, should establish: (i) a monitoring process to identify obsolete websites and links; and (ii) a procedure and timeframe to decommission obsolete websites.

OICT accepted recommendation 2 and stated that its Website Rationalization and Standardization Programme aims to standardize and consolidate the United Nations website portfolio and ensure compliance with prevailing controls and standards in cooperation with DPI. Following the first phase of public website review and remediation, OICT is proposing to undertake a second phase of this work in coordination with DPI to methodically address and remediate United Nations websites in cooperation with departmental website owners. Departments will additionally be requested to appoint a focal point familiar with their public websites in order to retroactively review their existing websites and record them in the registry and to undertake required remediation including deletion of obsolete websites and links where necessary. Recommendation 2 remains open pending receipt of evidence that OICT has established: (i) a monitoring process to identify obsolete websites and links; and (ii) a procedure and timeframe to decommission obsolete websites.

Network security vulnerability assessments needed to be conducted regularly

28. The United Nations ICT Enterprise Architecture Roadmap established in 2014 governs ICT infrastructure and application architecture. It encompasses the Organization's network requirements, contains standard industry best practices and recommends adoption and maturing of IS0 27001 (best practices for information technology security). ISO 27001 recommends that networks should be designed in a manner to protect information in systems and applications, and network services should be managed in accordance with security mechanisms and service level requirements, whether these services are provided in-house or outsourced. In addition, periodic vulnerability assessments and penetration tests of ICT systems should be performed regularly to prevent and reduce the negative impact of the potential exploitation of network vulnerabilities.

29. OIOS reviewed the network architecture and security for websites. The architecture followed proper network management requirements in accordance with the ICT Enterprise Architecture Roadmap, including adherence to enterprise zoning architecture, enterprise standards and security policies. The

network security was built and implemented in a multi-tier architecture. OICT websites were hosted in accordance with standard industry best practices. OIOS also noted that:

(i) OICT had adequate policies in place related to network security; and

(ii) There was an Intrusion Detection Service (IDS) in place to help support the timely identification of potential security incidents.

30. There were 10 websites hosted by DPI that utilized cloud technology not currently offered by OICT. These websites were hosted by third-party cloud computing providers covered by adequate service level agreements (SLAs) that complied with the ICT enterprise policies. The websites had gone through an ICT security compliance process in accordance with website security policies. DPI monitored the service performance to ensure that vendors were in compliance with the SLAs. Collectively, the existing tools and services provided daily, weekly and monthly reports and email alerts that included content violations. Furthermore, there had been no major incidents with the cloud computing services since the inception of the SLAs.

31. OIOS review of network vulnerability assessment practices showed that OICT had implemented some good practices in this area. OICT required a vulnerability assessment for all new web-based applications prior to release into production to verify the effectiveness of the security controls required based on the security level. Following release, each web application was subject to security re-testing if any changes were made to the code of the existing modules. In addition, the IDS in place assisted in identifying potential security threats and incidents.

32. However, OIOS also noted the following:

(i) Vulnerability assessments were performed prior to website deployment but were not performed on a regular basis for web-based applications; and

(ii) There was no monitoring of activities of persons with access to vulnerability scanning tools and their associated privileges to ensure that no unauthorized or malicious internal activity was performed by using these tools.

33. Periodic vulnerability assessments are required to provide the Organization with test results and recommendations to mitigate the identified risks. OICT was in the process of preparing a request for proposals in order to introduce additional capacity to perform periodic vulnerability assessments of web-based applications. However, the lack of periodic ICT vulnerability testing and the lack of controls over the use of vulnerability scanning tools could lead to security breach, potential loss of information assets and unavailability of ICT systems and applications.

(3) OICT should: (i) establish regularly scheduled vulnerability assessments of websites and web-based applications; and (ii) control access to the use of internal vulnerability scanning tools and monitor their use.

OICT accepted recommendation 3 and stated that it is in the process of establishing a protocol to ensure vulnerability assessments of websites and web-based applications are performed on a regular basis, based on the established methodology which defines different security levels and associated controls based on the characteristics of the website or application. This protocol will include the access control to and monitoring of the use of internal vulnerability scanning tools. Recommendation 3 remains open pending receipt of evidence that: (i) a regular schedule for vulnerability assessments

of websites and web-based applications has been established; and (ii) a protocol to control access to the use of internal vulnerability scanning tools and monitor their use has been developed.

User provisioning access controls for websites where required were adequate

34. The user provisioning access control procedures established for the United Nations Secretariat defined rules for user account management. User access to systems and applications should be controlled with procedures and mechanisms to request, grant, suspend, modify and terminate access and related privileges.

35. The majority of the 191 external facing websites were publicly accessible and therefore did not require user access provisioning and individual logins. Only seven websites required this type of access and a password. OIOS reviewed access provisioning for these websites and found that user provisioning access controls for these websites were adequate.

Incident management was generally adequate

36. An ICT service management framework should define the level of support required for incident management to ensure the continuous and reliable functioning of ICT operations. The framework should specify roles, tasks, and responsibilities of internal and external service providers and users. The framework should also detail criteria and processes to document the requirements of SLAs.

37. There were good control practices in place for incident management related to websites and social media including the documentation of incident management and request fulfillment policies. There were prompt responses and resolutions to incident tickets utilizing a consistent methodology and criteria and adequate logging, tracking and following of issues. In addition, there was adequate support and incident management responsibilities included in SLAs of third party hosting vendors. OIOS therefore concluded that system support and incident management for websites and social media was generally adequate.

Disaster recovery planning needed to be improved

38. According to the ICT Enterprise Application Roadmap, an ICT disaster recovery plan should be developed in conjunction with the business continuity plan (BCP), and provide recovery strategies to meet the objectives of the BCP. The BCP should define how an organization will continue operating in response to adverse events. The plan should include instructions defining the actions required by all parties responsible to ensure the continuation of operations under adverse conditions. ICT technical procedures of the United Nations Secretariat on disaster recovery require periodic testing (at least annually) to determine the plan's effectiveness and the Organization's readiness to execute the plan. The procedures also require that ICT service providers should have an approved disaster recovery plan that includes a test plan, the testing methodology, and the frequency of testing.

39. OIOS reviewed disaster recovery and business continuity planning for websites at Headquarters. DPI had an approved, adequate BCP in place that defined how it would continue operating in response to adverse events. The plan included websites and social media. OICT had an adequate contingency plan in place for the Webfarm at Headquarters. However, OIOS noted the following:

(i) The last full failover exercise of the complete Webfarm was conducted by OICT in August 2015, which was not in accordance with the ICT policy for periodic testing at least annually;

(ii) The disaster recovery plan did not include detailed procedures indicating predetermined functions to be performed during the exercise and no test plan including the testing methodology or frequency of testing; and

(iii) OICT adequately followed the Enterprise Backup Service 2016-2017 policy, system logs showed that the web files were backed up and moved off site as required, and data preservation and retention policies were complied with. However, there was no evidence that websites would be properly restored from the backups as no data restoration tests had been performed.

40. The absence of adequate disaster recovery planning for websites could lead to failure in timely recovery of ICT systems and applications, and unavailability of communications systems.

(4) OICT should finalize the United Nations Headquarters disaster recovery plan document and include: (i) a detailed plan of activities to be executed for failover and failback; and (ii) a standard procedure for annual testing of the disaster recovery plan for the United Nations Headquarters Webfarm.

OICT accepted recommendation 4 and stated that it developed the Information System Contingency Plan for the United Nations Headquarters Webfarm in September 2014. This plan will be further improved, including a detailed list of activities to be executed for failover and failback. Recommendation 4 remains open pending receipt of evidence that the Headquarters disaster recovery plan document has been updated to include: (i) a detailed plan of activities to be executed for failover; and (ii) a standard procedure for annual testing of the Disaster Recovery plan for the Headquarters Webfarm.

IV. ACKNOWLEDGEMENT

41. OIOS wishes to express its appreciation to the management and staff of DPI and DM for the assistance and cooperation extended to the auditors during this assignment.

(*Signed*) Eleanor T. Burns
Director, Internal Audit Division
Office of Internal Oversight Services

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of management of websites and social media at United Nations Headquarters

Rec. no.	Recommendation	Critical[1]/ Important[2]	C/ O[3]	Actions needed to close recommendation	Implementation date[4]
1	DPI, in collaboration with OICT, should establish a mechanism to ensure compliance with the requirements of the Organization's ICT project management framework for website development projects.	Important	O	Receipt of evidence that a mechanism has been established to ensure compliance with the Organization's ICT project management framework for website development projects.	31 December 2019
2	OICT, in collaboration with DPI, should establish: (i) a monitoring process to identify obsolete websites and links; and (ii) a procedure and timeframe to decommission obsolete websites.	Important	O	Receipt of evidence that OICT has established: (i) a monitoring process to identify obsolete websites and links; and (ii) a procedure and timeframe to decommission obsolete websites.	31 December 2018
3	OICT should: (i) establish regularly scheduled vulnerability assessments of websites and web-based applications; and (ii) control access to the use of internal vulnerability scanning tools and monitor their use.	Important	O	Receipt of evidence that: (i) a regular schedule for vulnerability assessments of websites and web-based applications has been established; and (ii) a protocol to control access to the use of internal vulnerability scanning tools and monitor their use has been developed.	31 December 2018
4	OICT should finalize the United Nations Headquarters disaster recovery plan document and include: (i) a detailed plan of activities to be executed for failover and failback; and (ii) a standard procedure for annual testing of the disaster recovery plan for the United Nations Headquarters Webfarm.	Important	O	Receipt of evidence that: (i) a regular schedule for vulnerability assessments of websites and web-based applications has been established; and (ii) a protocol to control access to the use of internal vulnerability scanning tools and monitor their use has been developed.	31 December 2017

[1] Critical recommendations address critical and/or pervasive deficiencies in governance, risk management or control processes, such that reasonable assurance cannot be provided with regard to the achievement of control and/or business objectives under review.
[2] Important recommendations address important (but not critical or pervasive) deficiencies in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.
[3] C = closed, O = open
[4] Date provided by DPI and DM in response to recommendations.

APPENDIX I

Management Response

DM/OUSG
Out: 28July2017
DM-2017-05945

United Nations Nations Unies

INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

TO: Mr. Gurpur Kumar, Deputy Director DATE: 28 July 2017
A: Internal Audit Division, Office of Internal Oversight Services

THROUGH: Christian Saunders, Director
S/C DE: Office of the Under-Secretary-General for Management

FROM: Mario Baez, Chief, Policy and Oversight Coordination Service
DE: Office of the Under-Secretary-General for Management

SUBJECT: **Draft report on an audit of management of websites and social media at United**
OBJET: **Nations Headquarters (Assignment No. AT2016/580/01)**

1. We refer to your memorandum dated 19 July 2017 regarding the above-subject draft report and provide you with comments of the Department of Management in the attached Appendix I.

2. Thank you for giving us the opportunity to provide comments on the draft report.

APPENDIX I

Management Response

Audit of management of websites and social media at United Nations Headquarters

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	DPI, in collaboration with OICT, should establish a mechanism to ensure compliance with the requirements of the Organization's ICT project management framework for website development projects.	Important	Yes	Deputy Director, Digital and Promotion Branch, News and Media Division, Department of Public Information; and Chief, Enterprise Application Centre, New York , OICT	31 December 2019	OICT has adopted the process-based PRINCE2 (Projects IN Controlled Environments) framework as its standard project management methodology. PRINCE2 is a widely accepted best-practice used across several industries. The current OICT governance framework makes wide use of PRINCE2-based templates for key project management artifacts and controls, including for website development. To the greatest degree possible, OICT is utilizing a template-based approach for the development and delivery of United Nations public websites. Built on Drupal, the approved ICT technology standard for Web Content Management Systems (WCMS), these websites are built in compliance with established DPI and OICT requirements for security, technology, accessibility, United Nations branding and multilingualism. To reduce overall costs and expedite pubic website delivery, OICT is minimizing the development effort required for public websites and promoting the configuration of these pre-developed templates. In the scenario where a template-based approach can be used, this is treated as a Request For Service (RFS) and is recorded and tracked accordingly. Only

[1] Critical recommendations address critical and/or pervasive deficiencies in governance, risk management or control processes, such that reasonable assurance cannot be provided with regard to the achievement of control and/or business objectives under review.

[2] Important recommendations address important (but not critical or pervasive) deficiencies in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						in cases where custom development is required, outside of the scope of a template, will it be managed using the PRINCE2 approach. This is to minimize the cost and effort associated with full project management support as well as to streamline and expedite public website delivery. The Enterprise Application Centre New York (EAC-NY), OICT is working with DPI to harmonize a common approach to requests for service and project management associated with public website development and delivery as described above.
2	OICT, in collaboration with DPI, should establish: (i) a monitoring process to identify obsolete websites and links; and (ii) a procedure and timeframe to decommission obsolete websites.	Important	Yes	Chief, Enterprise Application Centre, New York, OICT	31 December 2018	DPI is mandated with raising public awareness and support of the work of the United Nations through strategic communications campaigns, media and relationships with civil society groups. In addition, in accordance with its mandate and ST/AI/2001/5 on "United Nations Internet Publishing", DPI is accountable for the establishment of United Nations standards for public websites in the areas of branding, website accessibility and multilingualism, as well as to ensure coherence with the United Nations' overall strategic communications objectives and principles. At the same time, OICT is mandated to promote the transformation of the United Nations through the use of appropriate technology and to develop ICT policies, procedures and implementation practices throughout the Secretariat and to monitor compliance with them as part of the overall ICT Strategy (A/70/364). A core component

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						of these activities is the OICT Website Rationalization and Harmonization Programme that aims to standardize and consolidate the United Nations website portfolio and ensure compliance with prevailing controls and standards in cooperation with DPI. Following the first phase of public website review and remediation, OICT is proposing to undertake a second phase of this work programme in coordination with DPI to methodically address and remediate United Nations websites in cooperation with departmental website owners. This will include the establishment of a public website registry, which will include core information and metrics for all United Nations public websites and facilitating OICT and DPI ongoing review. It will be the responsibility of the departments to register their websites prior to initiating development and to ensure compliance with prevailing standards and controls through the development and production hosting stages. Departments will additionally be requested to appoint a focal point familiar with their public websites in order to retroactively review their existing websites and record them in the registry and to undertake required remediation including deletion of obsolete websites and links where necessary.
3	OICT should: (i) establish regularly scheduled vulnerability assessments of websites and web-based applications; and (ii) log and monitor the activities of persons who have access to run	Important	Yes	Chief, Global Security and Architecture Section, OICT	31 December 2018	OICT is in the process of establishing a protocol to ensure vulnerability assessments of websites and web-based applications are performed on a regular basis, based on the established methodology which defines

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	vulnerability scans.					different security levels and associated controls based on the characteristics of the web site or application. This protocol will include access control to and monitoring of the use of internal vulnerability scanning tools. OICT suggests amending part (ii) of the recommendation as follows: "control access to log and monitor the use of internal vulnerability scanning tools"
4	OICT should finalize Appendix C.10 UN Webfarm Information System Contingency Plan, of the United Nations Headquarters disaster recovery plan document and include (i) a detailed plan of activities to be executed for failover and failback, and (ii) a standard procedure for annual testing of the disaster recovery plan for the UN Webfarm.	Important	Yes	Chief, Enterprise Application Centre, New York and Regional Technology Center, OICT	31 December 2017	OICT developed the Information System Contingency Plan for United Nations Headquarters Webfarm in September 2014. This plan has been successfully tested on several occasions with the failover from the Primary Technology Center, New York to the Secondary Technology Center, New Jersey. This plan will be further improved, including a detailed list of activities to be executed for failover and failback.

United Nations Nations Unies

INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

TO: Mr. Gurpur Kumar, Deputy Director
A: Internal Audit Division, OIOS

DATE: 28 July 2017

REFERENCE:

THROUGH:
S/C DE:

FROM: Hua Jiang, Officer-in-Charge
DE: Department of Public Information

SUBJECT: **Assignment No. AT2016/580/01 – Draft report on an audit of the management of**
OBJET: **websites and social media at United Nations Headquarters**

1. I write with regard to your memorandum dated 19 July 2017, transmitting the draft report on the above-mentioned audit. I would like to thank OIOS for having taken into account comments and concerns previously raised by the Department of Public Information.

2. As requested, please find attached the completed Appendix I, including the target date and title of the individual responsible for implementing the recommendations.

3. Thank you.

cc: Ms. Jan Beagle, Under-Secretary-General, Department of Management
Mr. Janos Tisovzky, Acting Director, Strategic Communications Division, DPI
Mr. Salem Avan, Chief, Global Services Section, OICT, DM
Ms. Hua Jiang, Director, News and Media Division, DPI
Ms. Nancy Groves, Social Media, News and Media Division, DPI
Ms. Suzanne Shanahan, Chief of Service, Enterprise Application Centre, OICT, DM
Mr. Zachary Ikiara, Chief, Oversight and Coordination Support Unit, DM
Ms. Janet Wieser, Audit Focal Point, Department of Public Information
Mr. Ozzeir Khan, Audit Focal Point, OICT, Department of Management
Mr. Cynthia Avena-Castillo, Professional Practices Section, Internal Audit Division, OIOS

APPENDIX I

Management Response

Audit of the management of websites and social media at United Nations Headquarters

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	DPI, in collaboration with OICT, should establish a mechanism to ensure compliance with the requirements of the Organization's ICT project management framework for website development projects.	Important	YES	Deputy Director, Digital and Promotion Branch, NMD	31 DEC 2019	DPI will work with OICT to establish a mechanism to ensure compliance with the requirements of the Organization's ICT project management framework for website development projects. The mechanism will define the conditions under which website initiatives should be considered ICT projects requiring a PRINCE2 framework or can be treated as a request for service (RFS) and be recorded and tracked accordingly.
2	OICT, in collaboration with DPI, should establish: (i) a monitoring process to identify obsolete websites and links; and (ii) a procedure and timeframe to decommission obsolete websites.	Important				
3	OICT should: (i) establish regularly scheduled vulnerability assessments of websites and web-based applications; and (ii) log and monitor the activities of persons who have access to run vulnerability scans.	Important				
4	OICT should finalize Appendix C.10 UN Webfarm Information System Contingency Plan, of the United Nations Headquarters disaster recovery plan	Important				

[1] Critical recommendations address critical and/or pervasive deficiencies in governance, risk management or control processes, such that reasonable assurance cannot be provided with regard to the achievement of control and/or business objectives under review.

[2] Important recommendations address important (but not critical or pervasive) deficiencies in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

Management Response

Audit of the management of websites and social media at United Nations Headquarters

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	document and include (i) a detailed plan of activities to be executed for failover and failback, and (ii) a standard procedure for annual testing of the disaster recovery plan for the UN Webfarm.					