



# governmentattic.org

*"Rummaging in the government's attic"*

Description of document: Corporation for National and Community Service (CNCS)  
Enterprise Risk Management (ERM) Program records,  
2016

Requested date: 08-November-2016

Released date: 09-November-2016

Posted date: 28-November-2016

Source of document: FOIA Request  
Corporation for National and Community Service  
Office of the General Counsel  
Attn: Freedom of Information Act Officer  
250 E Street, SW  
Washington, DC 20525  
Fax: (202) 606-3467  
Email: [FOIA@cns.gov](mailto:FOIA@cns.gov)

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

# Corporation for National and Community Service

NationalService.gov



November 9, 2016

## Via email

Re: Freedom of Information Act Request # 2017-5

This letter is a response to the Freedom of Information Act (FOIA) request that the Corporation for National and Community Service (CNCS) received from you on November 8, 2016. You asked for “a copy of the CNCS Enterprise Risk Management Strategy document(s).”

Your request is granted in full; I have attached a copy of the requested record. Nothing has been withheld from the record, and there is no fee for this response.

If you have any questions, please feel free to contact me at (202) 606-6747. You may also contact CNCS's FOIA Public Liaison, Wilsie Y. Minor, at (202) 606-6673 or by email at [wminor@cns.gov](mailto:wminor@cns.gov).

Sincerely,

A handwritten signature in blue ink, appearing to read 'Stephanie A. Soper'.

Stephanie A. Soper  
FOIA Officer

Enclosure: CNCS Enterprise Risk Management Policy

**Corporation for National and Community Service  
Policies and Procedures**

---

**Policy Number:** 250  
**Revision:** 1

**Effective Date:** October 28, 2016

**Subject:** Enterprise Risk Management (ERM) Program

Purpose: Establish authority and responsibility for implementing CNCS's ERM program, an integrated, comprehensive approach to identify, prioritize, and manage risk throughout the agency.

Who is Covered: This policy and associated procedures apply to all CNCS staff.

Policy Replaced: Enterprise Risk Management (ERM) Program dated June 9, 2016.

Originating Office: Office of the CEO

---

**Approved By:**



**Wendy Spencer  
Chief Executive Officer**

**Contents**

**Section A – Overview ..... 3**

What is the purpose of this policy? ..... 3

To whom does this policy apply?..... 3

What is the authority for this policy? ..... 3

What is ERM? ..... 3

What is the link between ERM and Internal Controls?..... 4

**Section B – Roles and Responsibilities ..... 4**

What is CNCS’s ERM governance structure? ..... 4

Who serves on the Risk Management Council (RMC), and what are their responsibilities for carrying out the ERM program?..... 5

**Section C – Other Information..... 7**

**Attachments**

Charter: Risk Management Council

Charter: Risk and Assessment Committee

# Enterprise Risk Management Program

## Section A – Overview

### What is the purpose of this policy?

This document establishes the policy for the Corporation for National and Community Service’s (CNCS’s) Enterprise Risk Management (ERM) program. The ERM program provides a framework for proactively identifying, prioritizing, and managing risk as a management strategy for achieving the agency’s strategic goals and objectives. The program seeks to integrate risk management into all CNCS operations to help achieve desired agency outcomes. ERM will help CNCS and its operating programs and units work collaboratively and efficiently to identify and manage agency-wide risks.

CNCS defines risk as the effect of uncertainty on objectives—the likelihood that we will not achieve what we intend to, and the resulting harm.

The ERM program establishes a structure to help CNCS:

- Increase the likelihood of successfully delivering on the agency’s goals and objectives;
- Encounter fewer unanticipated outcomes;
- Better identify, assess, prioritize, and manage risks;
- Clearly describe to customers and other stakeholders what the agency is doing to manage its risks; and
- Reduce redundancy of scarce resources dedicated to management initiatives and improve integration among risk management methods to ensure cost effective implementation.

### To whom does this policy apply?

This policy applies to all CNCS staff, programs, and operational units.

### What is the authority for this policy?

The Office of Management and Budget (OMB) [Circular A-11](#), “Preparation, Submission, and Execution of the Budget” states that federal agencies are expected to manage risks and challenges related to delivering the organization’s mission. Numerous other OMB circulars and laws provide federal ERM requirements, including the current draft revision of [Circular A-123](#), “Management’s Responsibility for Internal Controls and Enterprise Risk Management.”

### What is ERM?

ERM is a management culture that can help agencies to properly identify and manage risks to performance, especially those risks related to achieving strategic objectives. ERM addresses a full spectrum of an organization’s risk, including but going beyond internal controls. It encompasses all areas of organizational exposure to risk (financial, operational, reporting, compliance, governance, strategic, reputational, etc.).

ERM is carried out by following a process that prioritizes and manages risk exposure as part of an interrelated risk portfolio (e.g., information technology, human capital, privacy, grants, and facilities) rather than as functional silos (e.g., financial and reporting risk). In other words, ERM is a process for identifying all the risks from various parts of the organization and assessing and

prioritizing those risks at the entity-wide level to ensure that a portfolio view of risk is available at the highest levels of leadership to help inform decision-making.

An ERM process will be applied across CNCS. Unifying efforts across the agency will ensure that strategies and actions are informed by a common understanding of risk, which is an essential component to inform priorities and the allocation of resources. Risk management practices at all levels will be integrated to better inform decision-making and priority-setting. Incorporating risk information and analysis into strategic and operational decision-making is fundamental to agency success. Identification of potential risks, and avoidance or mitigation of those risks, is a critical management responsibility to make informed business decisions.

Emerging risks to CNCS objectives will be actively identified and managed. Consistent and disciplined consideration and treatment of risk will strengthen day-to-day processes, making decisions more transparent and defensible, encouraging innovation, and ensuring planned outcomes are achieved. ERM will become a visible and integral part of CNCS culture allowing the agency to fulfill its mission and goals.

### **What is the link between ERM and Internal Controls?**

Requirements for internal controls are described in [OMB Circular A-123](#), “Management’s Responsibility for Internal Control.” These requirements focus on the management of internal controls to support reasonable assurance that management has met three objectives of internal controls:

- Operations: Effectiveness and efficiency of operations
- Reporting: Reliability of reporting for internal and external use
- Compliance: Compliance with applicable laws, regulations, and policies.

Both ERM and internal control activities provide risk management support to an agency in different but complementary ways. ERM does not exclude internal control activities, nor does ERM replace internal controls. ERM embraces the disciplined foundation of A-123 policy on internal control, which includes the structure of recommended controls, procedures, accountability, and program management. Because ERM draws on an interrelated risk portfolio, it is important to understand the controls related to key organizational risks and how these controls can be used to mitigate or reduce the level of exposure to risk.

### **Section B – Roles and Responsibilities**

Because ERM is a management culture, the activities of ERM occur as a result of coordinated management efforts directed under CNCS’s ERM governance structure.

### **What is CNCS’s ERM governance structure?**

CNCS’s implementation of the ERM program is governed and supported by the following entities:

- Risk Management Council
- Risk and Assessment Committee
- CNCS’s Office of the Chief Risk Officer (OCRO)

Collectively, these groups—in coordination with the CEO—are responsible for providing

governance, decision making, and execution of the ERM Program.

**Who serves on the Risk Management Council (RMC), and what are their responsibilities for carrying out the ERM program?**

The RMC is the group of senior advisors that will assist the CEO in overseeing the ERM program, which includes advising the CEO on critical risks identified at the lower ERM governance levels, helping the CEO to prioritize identified risks and appropriate resources to treat them, and ensuring that internal controls are in place and corrective action completed. The COO chairs the RMC and has designated the following to serve on the Council:

- Chief of Staff
- Chief Operating Officer
- Chief of Program Operations
- Chief Risk Officer
- General Counsel

The RMC will meet quarterly, and as needed, to assess and prioritize risks and mitigation strategies to recommend to the CEO.

The Inspector General will be invited to submit questions, brief, or advise the RMC on an ad hoc basis, as requested by the Inspector General or the RMC. The RMC will brief the Inspector General on decisions made by the RMC.

The RMC satisfies the objectives of a number of federal risk management policies that call for senior management engagement on risk and governance issues. The Council will:

- Provide an agency-wide risk portfolio aligned to the agency's strategic objectives, as described in OMB Circular A-11, section 270
- Act as the CNCS Oversight Body under the Government Accountability Office's Standards of Internal Control in the Federal Government
- Provide Tier 1 governance of CNCS's Information Security under National Institute of Standards and Technology Standard 800-37

**Who serves on the Risk and Assessment Committee (RAC), and what are their responsibilities for carrying out the ERM program?**

The RAC consists of representative from each functional unit or program in the Corporation. The RAC will assist the Office of the Chief Risk Officer in implementing the agency's risk assessments and monitoring activities and will serve as a liaison between the Office of the Chief Risk Officer and the agency's functional areas and programs. The Chief Risk Officer chairs the RAC.

The RAC will meet quarterly and as needed to provide recommendations to the RMC. The RAC may also convene subject matter experts as appropriate to ensure proper execution of the agency's ERM strategy.

**What is the role of the Office of the Chief Risk Officer (OCRO) in implementing the ERM program?**

The OCRO is the office assigned to implement the ERM program. The OCRO will:

- Provide subject matter expertise and training to the CEO, senior leadership, and managers on

matters related to risk management and internal controls initiatives and the implementation and effective functioning of the ERM program

- Provide project management and subject matter expertise to assist managers and staff in carrying out specific ERM activities (such as risk assessment of specific business practices, and analyses of appropriate policies and procedures to mitigate those risks)
- Determine the design and methodology for, and then conduct the annual internal controls assessments related to OMB Circular A-123 and other activities under the ERM Framework
- Provide guidance to its requisite governance bodies, as well as the RMC
- Provide guidance on actions by other CNCS offices regarding opportunities for improvement or needed corrective actions identified in monitoring areas of risk to CNCS operations.

### **Who else is responsible for carrying out CNCS's ERM Program?**

Effective ERM requires the engagement of the CNCS Board of Directors and all staff at every level, including internal contractors.

***CEO and Board of Directors*** – The CEO and CNCS Board of Directors are responsible for ensuring that all CNCS managers and staff:

- Understand the importance of the ERM program
- Work to achieve the objectives of the ERM program
- Provide goals and objectives to focus and inform the ERM program
- Drive change necessary to adopt a business culture conducive to ERM
- Oversee the ERM program to assess whether it is meeting its objectives
- Communicate with key stakeholders, including external parties, regarding the ERM program
- Ensure CNCS takes timely corrective actions to address risk.

***Senior Leadership and Managers*** – CNCS senior leadership and managers are responsible for:

- Actively supporting and participating in ERM activities
- Holding themselves and staff accountable for carrying out their ERM program responsibilities under this policy and as assigned
- Evaluating and communicating risk in a timely manner to governance bodies responsible for evaluating risk
- Taking prompt corrective actions to address and mitigate risks.

***Staff and internal Contractors*** – All CNCS non-management staff and internal contractors are responsible for:

- Carrying out their duties and responsibilities in accordance with specific CNCS policies and procedures that pertain to their specific positions
- Attending training on risk management and the ERM program
- Supporting and participating in ERM activities, including assessments of whether policies and practices are properly designed and followed
- Bringing known instances of risk (including non-compliance with law, regulations, or CNCS policies and procedures) to the attention of appropriate CNCS managers
- Contributing their thoughts and ideas as to how to improve policies and procedures and

enhance compliance with them.

## **Section C – Other Information**

### **Where is additional information about the ERM Framework and ERM Infrastructure available?**

CNCS maintains an ERM Resource Area located on the CNCS OCRO page. This resource area will serve as the centralized source of information pertinent to the CNCS ERM Program and is intended to facilitate the timely dissemination of information and updates for CNCS staff's support of the overall ERM Program and supporting infrastructure.

### **What is the communication plan related to this policy?**

The CEO will inform all CNCS staff when this policy is cleared and posted on the CNCS Intranet. The Policy Coordinator will also update the policies posted on CNCS's intranet policy page. The OCRO will design and coordinate additional communications and training for staff and stakeholders. The OCRO will also be responsible for reviewing and updating this policy on an annual basis and ensuring approval of the SRMC for any changes.

### **What is the training plan related to this policy?**

OCRO will provide annual training for all CNCS staff via a GEM Series session on CNCS's ERM program. Training on the CNCS ERM program will also be made available via CNCS's Learning Management System. Annual training will be available for all CNCS staff, and will be required as part of new employee orientation. OCRO will work with other CNCS offices to provide additional guidance and training as needed. Additionally, the Director and staff of OCRO will provide training at staff meetings and/or program conferences upon request.

## **Charter: Risk Management Council**

### **Purpose**

The purpose of the Risk Management Council (RMC) is to oversee CNCS's Enterprise Risk Management (ERM) program and advise the CEO on critical risk issues.

### **Actions**

In providing oversight and accountability of ERM efforts, the SRMC will:

1. Meet on a regular basis;
2. Ensure the completion of a comprehensive risk assessment process;
3. Develop an agency-wide risk portfolio aligned with CNCS strategic objectives;
4. Ensure that internal controls are in place to mitigate risk; and
5. Ensure that corrective and risk mitigation actions are completed.

### **Composition**

The RMC is composed of:

1. Chief Operating Officer (Chair)
2. Chief of Staff
3. Chief of Program Operations
4. Chief Risk Officer
5. General Counsel

### **Meetings**

The RMC will meet on a quarterly basis, and more frequently as needed. The RMC may request ad hoc meetings with relevant managers and business process owners.

The RMC will review progress reports and respond to requests for decision submitted by the Risk and Assessment Committee (RAC) .

The RMC will accept and respond to questions submitted by the Inspector General. Additionally, the Inspector General will be provided the opportunity to attend RMC meetings on an ad hoc basis to present information related to risk management.

The RMC will review this charter and revise, if necessary, on an annual basis.

## **Charter: Risk and Assessment Committee**

### **Purpose**

The purpose of the Risk and Assessment Committee (RAC) is to ensure support for and proper execution of CNCS's Enterprise Risk Management (ERM) program and agency wide risk assessment activities.

### **Actions**

In support of CNCS's ERM efforts, the RAC will:

1. Meet on a regular basis
2. Analyze the results of risk assessments
3. Report the results of risk assessments
4. Manage CNCS's internal control program
5. Manage CNCS's Improper Payment Elimination and Reduction Improvement Act program
6. Manage CNCS's grants monitoring program
7. Engage key process owners on an ad hoc basis to achieve ERM objectives.

In support of CNCS's ERM efforts, the Chair of the RAC will:

1. Seek guidance from the Risk Management Council (RMC)
2. Report to the RMC
3. Operationalize RMC directives.

### **Composition**

The RAC is composed of: the Chief Risk Officer (Chair) and representatives of each functional unit and program.

### **Meetings**

The RAC will meet quarterly, and more frequently as needed. Key business process owners may be invited to attend meetings as required to achieve RAC objectives.

The RAC will submit progress reports and requests for decisions to the Risk Management Council.

The RAC will review this charter and revise, if necessary, on an annual basis.