

JOB DESCRIPTION

Post Details:

Post Title:	Senior IT Change Manager	Organisational Element:	COO/NCSC
		Job Family:	Service Management
Rank/Grade:	G17		
Military/Civilian:	Civilian	Location:	Mons, BEL

Organisation context:

This is a position within the NATO Communications and Information Agency (NCI Agency), an organization of the North Atlantic Treaty Organization (NATO).

To strengthen the Alliance through connecting its forces, the NCI Agency delivers secure, coherent, cost effective and interoperable communications and information systems in support of consultation, command & control and enabling intelligence, surveillance and reconnaissance capabilities, for NATO, where and when required. It includes IT support to the Alliances' business processes (to include provision of IT shared services) to the NATO HQ, the Command Structure and NATO Agencies.

Organisational Element Statement of Functions:

The NATO Cyber Security Centre (NCSC) is responsible for planning and executing all lifecycle management activities for cyber security. In executing this responsibility, NCSC provides specialist cyber security-related services covering the spectrum of scientific, technical, acquisition, operations, maintenance, and sustainment support, throughout the lifecycle of NATO Communications and Information Systems (CIS). The NCSC enables secure conduct of the Alliance's operations and business In the context of NATO's C4ISR. The NCSC provides cyber security services and operational support to NCIA customers and users, as well as to all other elements of the Agency; this includes all Business Areas, Programme Offices, CIS Support Units/Elements, and the Agency Ops centre. The NCSC is responsible for providing the broad spectrum of services in the following specialist security areas: Cyber Security, Cyber Defence, Defensive Cyberspace Operations and support to Allied operations and Missions (AOM). In executing its responsibilities, the NCSC provides lifecycle security risk management services for all NATO CIS. The NCSC leads in the development of the new capabilities and innovation in Cyber Security.

Job role description:

This post pertains to the execution of the change management practice in support of the addition, modification or removal of an IT service or service component, system, software, patches, hardware, and products across all security domains and networks operated, managed, controlled or maintained by the organisation. This involves ensuring that IT changes are recorded, evaluated, managed through their lifecycle, authorized, scheduled and successfully deployed so as to minimize the impact on our customers and avoid change-related

incidents and conflicts between IT services.

Duties and Responsibilities:

Strategic planning:

- Contributes to the development of policies, standards and guidelines for strategy development and planning.
- Develops and communicates plans to drive forward the strategy and related change planning.
- Provides support and guidance to help stakeholders adhere to the approach.
- Ensures that all stakeholders are aware of the strategic management approach and timetables.
- Collates information and creates reports and insights to support strategy management processes.

Emerging technology monitoring:

- Supports monitoring of the external environment and assessment of emerging technologies.
- Contributes to the creation of reports, technology road mapping and the sharing of knowledge and insights.

Risk management:

- Carries out risk management activities within a specific function, technical area or project of medium complexity.
- Identifies risks and vulnerabilities, assesses their impact and probability, develops mitigation strategies and reports to the business.
- Involves specialists and domain experts as necessary.

Requirements definition and management:

- Defines and manages scoping, requirements definition and prioritisation activities for initiatives of medium size and complexity.
- Contributes to selecting the requirements approach.
- Facilitates input from stakeholders, provides constructive challenge and enables effective prioritisation of requirements.
- Establishes requirements baselines, obtains formal agreement to requirements, and ensures traceability to source.

Configuration management:

- Proposes and agrees the configuration items (CIs) to be uniquely identified with naming conventions.
- Puts in place operational processes for secure configuration, classification and management of CIs, and for verifying and auditing configuration records.
- Develops, configures and maintains tools (including automation) to identify, track, log and maintain accurate, complete and current information.
- Reports on the status of configuration management.
- Identifies problems and issues and recommend corrective actions.

Change control:

- Leads the assessment, analysis, development, documentation and implementation of changes.
- Develops implementation plans for complex requests for change.
- Reviews proposed implementations and evaluates the risks to the integrity of the product and service environment.
- Ensures appropriate change approval is applied to changes.

- Reviews the effectiveness of change implementation.
- Identifies, evaluates and manages the adoption of appropriate tools, techniques and processes for change control.

IT Service Change Management:

- Analyses and presents the pros and cons of potential risks to IT service changes.
- Designs approaches and templates for the implementation and review of IT service changes.
- Directs and monitors the implementation of IT service changes and procedures.
- Determines methods and processes for IT service changes.
- Compares change impact-assessing approaches with other industry professionals or organizations.
- Evaluates the effectiveness of change management through professional group discussions.

System Development Life Cycle:

- Clarifies the similarities and differences among life cycles; easily labels and describe each phase.
- Explains the basic concepts of a structured approach to application development.
- Describes associated standards, procedures and guidelines for the system development life cycle.
- Highlights the major phases, activities, checkpoints and deliverables in the system life cycle.

Additional duties for this post:

Technical Review Board (TRB):

- Organises informal technical review boards to assess the change viability, technical details and potential way ahead.
- Understands and is able to articulate constraints (financial/technical/workforce), risks and impacts relating to the Change Request.
- Utilising TRB sessions, ensures that all Change Requests are properly prepared (investigated, evaluated and risk assessed) for consideration by the D-CAB.

Domain and Enterprise Change Advisory Board (CAB):

- Plans and Organises CABs to address pending Change Requests.
- Runs the meeting and facilitates discussions with technical and management stakeholders.
- Documents CAB meeting minutes and rendered decisions.

Other Duties:

- Performs any other duties as may be required.

Education, Experience and Training (essential):

Education:

A minimum requirement of a Bachelor's degree at a nationally recognised/certified University in a related discipline and 3 years post-related experience. Or exceptionally, the lack of a university degree may be compensated by the demonstration of a candidate's particular abilities or experience that is/are of interest to NCI Agency, that is, at least 10 years extensive and progressive expertise in duties related to the function of the post.

Experience:

- 3 years of practical experience in managing change request from initiation to closure while engaging with relevant process owners and stakeholders.
- Experience in leading small teams.

Education, Experience and Training (desirable):

Education:

- University degree in Computer Science, Technology domain.

Experience:

- Previous Change Manager Experience in Cyber Security domain.
- Knowledge/Experience of Cyber Security services (SIEM, NIPS/IDS, FPC, Malware and Forensics, Penetration Testing and Hardening, Vulnerability scanning), commercial tools and technologies.
- Technical background and hands-on experience in network (Cisco/Juniper), systems (Linux/Windows), virtualisation (VMware/Hyper-V), back-up and recovery solutions.

Training/Certifications:

- ITIL Foundation Certification.
- ITIL v3 Transition or ITIL v4 equivalent Certification.
- Prince2 Foundation Certification.

Behavioural competencies:

- *Creating and Innovating* - Produces new ideas, approaches, or insights; creates innovative products or designs; produces a range of solutions to problems.
- *Delivering Results and Meeting Customer Expectations* - Focuses on customer needs and satisfaction; sets high standards for quality and quantity; monitors and maintains quality and productivity; works in a systematic, methodical and orderly way; consistently achieves project goals.
- *Adapting and Responding to Change* - Adapts to changing circumstances; tolerates ambiguity; accepts new ideas and change initiatives; adapts interpersonal style to suit different people or situations; shows an interest in new experiences.

Language:

A thorough knowledge of one of the two NATO languages, both written and spoken, is essential and some knowledge of the other is desirable.

NOTE: Most of the work of the NCI Agency is conducted in the English language

