

Role Description

Manager, Cyber Governance, Risk and Assurance



Cluster	NSW Parliament
Agency	Department of Parliamentary Services
Division/Branch/Unit	Corporate Services /IT Services
Location	Sydney, CBD
Classification/Grade/Band	Clerk Grade 9/10
Role Number	TBA
ANZSCO Code	TBA
PCAT Code	TBA
Date of Approval	TBA
Agency Website	http://www.parliament.nsw.gov.au

Agency overview

Administratively, the Parliament comprises three main Departments: the Department of Parliamentary Services (DPS), Department of the Legislative Council (LC), and the Department of the Legislative Assembly (LA). The Chief Executive is the head of the Department of Parliamentary Services, and the Clerk of the Legislative Council and Clerk of the Legislative Assembly are the Heads of their respective House Departments. The House Departments are responsible for providing procedural advice to the Council and the Assembly, and their respective members, on parliamentary proceedings in each House and Committees; undertaking protocol functions, providing corporate and executive support, House specific administrative/research services and generating content/engagement strategies relating to the activities of the House and its committees.

DPS is responsible for providing corporate and other common services across the Parliament as a whole. It comprises the following Divisions; Parliament Services and Corporate Services, and two project Branches; Digital Transformation and Capital Works Strategy & Delivery.

The Parliament Services Division comprises administrative and support services specific to the institution of Parliament. This includes the Hansard, Library and Research Branch, the Communications, Engagement and Education branch and the Parliamentary Catering Unit.

The Corporate Services Division comprises of the corporate functions that provides services to all staff and Members across Parliament House. This includes the Financial Services & Governance Branch, People, Property & Security Branch, IT Services Unit and Planning and Performance Unit.

The Parliament's ultimate governance body includes the Presiding Officers and the Chief Executive, DPS and the Clerks of the Legislative Council and Legislative Assembly, supported by a contemporary governance framework.

Primary purpose of the role

The Manager, Cyber Governance, Risk and Assurance will be responsible for ensure the effective implementation and oversight of cybersecurity governance, risk management, and assurance frameworks to protect the NSW Parliament's information assets and ensure compliance with relevant government policies.

Key accountabilities

- Develop and implement comprehensive cyber governance frameworks to ensure effective management of cybersecurity policies, procedures, and controls.
- Conduct routine risk assessments to identify and evaluate cybersecurity risks. Develop and implement risk mitigation strategies and monitor their effectiveness.
- Ensure the Parliament of NSW complies with relevant cybersecurity policies, regulations, standards, and best practices. Oversee the preparation and submission of compliance reports and audits.
- Develop, update, and enforce cybersecurity policies and standards. Ensure that policies are communicated effectively and adhered to across the Parliament.
- Design and deliver cybersecurity awareness and training programs to educate the Parliament staff on security best practices and the importance of compliance.
- Plan and conduct regular assurance activities, including internal audits and assessments, to verify the effectiveness of cybersecurity controls and identify areas for improvement.
- Engage with key stakeholders, including the senior executive team, members and their staff, to communicate cybersecurity risks, governance initiatives, and assurance findings. Prepare and present regular reports on cybersecurity posture and risk management activities.
- Support NSW Parliament ICT strategies and plans, through the provision of cyber security related advice, information and/or training to relevant stakeholders to facilitate the appropriate interpretation and implementation of cyber security best practice.
- Prepare executive management level, analytical reports, discussion papers and memos in Plain-English, to inform, assess alternatives, recommend actions, and promote new ideas or strategies in relation to cyber security.

Key challenges

- Effectively working on simultaneous policy, governance and/or training initiatives and projects to the required standards and timeframes.
- Translating highly technical and technically based concepts into the business context and obtaining support from stakeholders and operational staff.
- Staying abreast of emerging issues and maintaining up to date knowledge on cyber security, cyber risk and ICT trends, while providing timely and relevant advice on emerging topics or issues.
- Continually building knowledge of best practice regarding cyber security preparedness and awareness techniques

Key relationships

Who	Why
Parliamentary	
Presiding Officers / House Department Clerks and Chief Executive	<ul style="list-style-type: none"> Develop strategic relationships and provide expert advice to influence decisions, support initiatives and promote effective communications and collaboration across Parliament
Internal	
Reporting Line Manager	<ul style="list-style-type: none"> Provide advice and contribute to decision making. Identify emerging issues/risks and their implications, and propose solutions Receive guidance and provide regular updates on key projects issues and priorities. Escalate issues, advise and receive instructions.
Division/Branch Leadership Team	<ul style="list-style-type: none"> Collaborate and build effective relationships to ensure the optimisation of project milestone. Respond to requests for information or assistance and escalate sensitive issues.
ICT Operations	<ul style="list-style-type: none"> Provide advice and contribute to decision making. Communicate latest issues and trends in cyber security. Develop mitigation plans to remediate identified vulnerabilities.
Customers	<ul style="list-style-type: none"> Develop training and communication plans to increase cyber security awareness.
External	
NSW Government agencies	<ul style="list-style-type: none"> Report on NSW Parliament cyber security posture and compliance with NSW Cyber security policy. Receive guidance and support for issues relating to NSW Parliaments cyber security risk management and compliance reporting needs.
Vendors and suppliers	<ul style="list-style-type: none"> Communicate needs, facilitate business transactions and resolve issues. Manage relationships with Parliament's suppliers of business critical products, consulting and managed services.

Role dimensions

Decision making

- The Manager, Cyber Governance Risk and Assurance will have autonomy over decisions under their direct control. It would refer to the Senior Manager, Cyber Governance and Security Operations or the branch director for decisions that require significant change or are likely to require approval from a higher level of management.

Reporting line

- The role accounts and reports to the Senior Manager, Cyber Governance and Security Operations

Direct reports

- One Cyber Governance and Risk Specialists / Analysts

Budget/Expenditure

As per the approved DPS Financial Delegations.

Essential Requirements

- Demonstrated knowledge and experience in cybersecurity governance and risk management domain
- Tertiary qualifications or industry certifications in cybersecurity governance and risk management.





Capabilities for the role

The NSW Public Sector Capability Framework applies to all NSW public sector employees. The Capability Framework is available at www.psc.nsw.gov.au/capabilityframework


This role also utilises an occupation specific capability set which contains information from the Skills Framework for the Information Age (SFIA). The capability set is available at www.psc.nsw.gov.au/capabilityframework/ICT

Capability summary

Below is the full list of capabilities and the level required for this role. The capabilities in bold are the focus capabilities for this role. Refer to the next section for further information about the focus capabilities.

NSW Public Sector Capability Framework		
Capability Group	Capability Name	Level
 Personal Attributes	Display Resilience and Courage	Adept
	Act with Integrity	Adept
	Manage Self	Adept
	Value Diversity and Inclusion	Intermediate
 Relationships	Communicate Effectively	Adept
	Commit to Customer Service	Intermediate
	Work Collaboratively	Adept
	Influence and Negotiate	Adept
 Results	Deliver Results	Adept
	Plan and Prioritise	Adept
	Think and Solve Problems	Adept
	Demonstrate Accountability	Advanced
 Business Enablers	Finance	Intermediate
	Technology	Advanced
	Procurement and Contract Management	Adept
	Project Management	Intermediate

Occupation / profession specific capabilities

Capability Set	Category, Sub-category and Skill	Level and Code
	Strategy & Architecture, Technical Strategy & Planning, Methods & Tools	Level 5 – METL
	Solution Development & Implementation, Systems Development, Information Content Authoring	Level 4 – INCA
	Strategy & Architecture, Information Strategy, Information Content publishing	Level 4 - ICPM

Focus capabilities

The focus capabilities for the role are the capabilities in which occupants must demonstrate immediate competence. The behavioural indicators provide examples of the types of behaviours that would be expected at that level and should be reviewed in conjunction with the role's key accountabilities.

NSW Public Sector Capability Framework

Group and Capability	Level	Behavioural Indicators
Personal Attributes Display Resilience and Courage	Adept	<ul style="list-style-type: none"> Remain composed and calm and act constructively in highly pressured and unpredictable environments Give frank, honest advice in response to strong contrary views Accept criticism of own ideas and respond in a thoughtful and considered way Welcome new challenges and persist in raising and working through novel and difficult issues Develop effective strategies and show decisiveness in dealing with emotionally charged situations and difficult or controversial issues
Personal Attributes Manage Self	Adept	<ul style="list-style-type: none"> Keep up to date with relevant contemporary knowledge and practices Look for and take advantage of opportunities to learn new skills and develop strengths Show commitment to achieving challenging goals Examine and reflect on own performance Seek and respond positively to constructive feedback and guidance Demonstrate and maintain a high level of personal motivation
Relationships Communicate Effectively	Adept	<ul style="list-style-type: none"> Present with credibility, engage diverse audiences and test levels of understanding Translate technical and complex information clearly and concisely for diverse audiences Create opportunities for others to contribute to discussion and debate Contribute to and promote information sharing across the organization Manage complex communications that involve understanding and responding to multiple and divergent viewpoints Explore creative ways to engage diverse audiences and communicate information

NSW Public Sector Capability Framework

Group and Capability	Level	Behavioural Indicators
Relationships Influence and Negotiate	Adept	<ul style="list-style-type: none"> Adjust style and approach to optimise outcomes Write fluently and persuasively in plain English and in a range of styles and formats Influence others with a fair and considered approach and present persuasive counter-arguments Work towards mutually beneficial 'win-win' outcomes Show sensitivity and understanding in resolving acute and complex conflicts and differences Identify key stakeholders and gain their support in advance Establish a clear negotiation position based on research, a firm grasp of key issues, likely arguments, points of difference and areas for compromise Anticipate and minimise conflict within the organisation and with external stakeholders
Results Plan and Prioritise	Adept	<ul style="list-style-type: none"> Consider the future aims and goals of the team, unit and organisation when prioritising own and others' work Initiate, prioritise, consult on and develop team and unit goals, strategies and plans Anticipate and assess the impact of changes, including government policy and economic conditions, on team and unit objectives and initiate appropriate responses Ensure current work plans and activities support and are consistent with organisational change initiatives Evaluate outcomes and adjust future plans accordingly
Results Demonstrate Accountability	Advanced	<ul style="list-style-type: none"> Design and develop systems to establish and measure accountabilities Ensure accountabilities are exercised in line with government and business goals Exercise due diligence to ensure work health and safety risks are addressed Oversee quality assurance practices Model the highest standards of financial probity, demonstrating respect for public monies and other resources Monitor and maintain business-unit knowledge of and compliance with legislative and regulatory frameworks Incorporate sound risk management principles and strategies into business planning
Business Enablers Technology	Advanced	<ul style="list-style-type: none"> Champion the use of innovative technologies in the workplace Actively manage risk to ensure compliance with cyber security and acceptable use of technology policies Keep up to date with emerging technologies and technology trends to understand how their application can support business outcomes Seek advice from appropriate subject-matter experts on using technologies to achieve business strategies and outcomes Actively manage risk of breaches to appropriate records, information and knowledge management systems, protocols and policies

