POSITION DESCRIPTION – 2021

POSITION TITLE: **ICT Security Analyst**

POSITION NUMBER: **L8-001 - Rotational**

LOCATION: **FRCS HEAD OFFICE, SUVA**

REPORTS TO: **Deputy Director ICT**

THE ORGANIZATION

The Fiji Revenue & Customs Service (FRCS) is a statutory authority established under the FRCS Act 1998. FRCS is an agent for the State for administration and enforcement of Tax and Customs laws in Fiji. Our organizational Values are - One Organization; Leadership; Valuing Employees; Integrity; Results Focus; Partnership Development.

POSITION PURPOSE

The Security Analyst is an integral role that provides subject matter expertise in designing and implementation of IT security controls such as Identity and Access Management, Data Loss Prevention as well as detections, response and recovery controls. This role leads the transformation of security policy across of the enterprise architecture across all systems. The Security Analyst will execute assurance and advisory activities that contribute to the improvement of ICT's delivery capability through identifying insights and opportunities for efficiency and effectiveness of ICTs operations, services to the business, assets, and compliance obligations with the organisations policies and regulations. The Security Analyst collaborates with the ICT team in the development, implementation and ongoing improvement of cyber assessment tools, services, and business processes.

With a strong focus on customer service, fostering a culture of innovation, collaboration and technical excellence that is centred on business value, this role is expected to define and enforce ICT industry architecture principles and frameworks to align to FRCS's risk appetite and provide a secure environment for business services.

ACCOUNTABILITIES

KEY RESULTS AREAS	KEY ACCOUNTABILITIES
Enterprise Security Assurance	▪ Develops and communicates corporate information security policy, standards and guidelines. Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors environmental and market trends and pro-actively assesses impact on business strategies, benefits and risks. Ensures architectural principles are applied during design to reduce risk and drives adoption and adherence to policy, standards and guidelines. ▪ Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards. Support the delivery of enterprise security solutions design and work with the project delivery teams, enterprise engineers and solution designers to align the outcomes to IT security requirements. ▪ Establishes standards and procedures across the IT service lifecycle (including the development lifecycle) in the areas of systems integration and testing and ensures that practitioners adhere to them. ▪ Drive engagements with key business and technology stakeholders to capture business requirements, technology landscape and identify proper security

	principals and ensure IT security controls meet business requirements for performance and effectiveness. ▪ Establishing appropriate IT security design and architecture governance frameworks using (ISO) 27001-/27002/27005 and COBIT. Ensure processes in determining information and data flow are authorised and conform to security policy and standards. ▪ Collaborate and work closely with Security Consulting, System Engineering, Operations, Risk, Procurement, Legal, and fellow strategy and operations teams and functions. ▪ Recommends/designs structures and tools for systems which meet business needs and takes into account target environment, performance security requirements and existing systems. Delivers technical visualisation of proposed applications for approval by customer and execution by software developers. ▪ Reviews new business proposals and provides specialist advice on security issues and implications. Monitors the application and compliance of security administration procedures and reviews information systems for actual or potential breaches in security. ▪ Performs security risk, vulnerability assessments and business impact analysis ranging from small to large complexity information systems. Investigates suspected attacks and manages security incidents. Uses forensics where appropriate. ▪ Delivers objective insights into the existing of vulnerabilities, the effectiveness of defences and mitigating controls both already in place and those planned for future implementation. Takes responsibility for ensuring the integrity of testing activities.
Business Continuity & Availability Management	▪ Contributes to the creation and review of a systems capability strategy which meets the strategic requirements of the business. Develops models and plans to drive forward the strategy, taking advantage of opportunities to improve business performance. ▪ Uses consistent processes for identifying potential risk events, quantifying and documenting the probability of occurrence and the impact on the business. ▪ Develop simple, actionable, and repeatable metrics and report on FRCS's ICT security capability to the ICT Management.
Asset Management	▪ Produces and analyses registers and histories of authorised assets and verifies that all these assets are in a known state and location. Acts to highlight and resolve potential instances of unauthorised assets such as unlicensed copies of software. ▪ Promotes awareness of and commitment to asset control. Initiates assessment of consequences and risks arising from decisions to obtain, change or continue the possession or use of an asset, system or service. ▪ Work with the Senior IT Service Engineer to develop the IT Inventory annual plan ▪ Contributes to annual plan so that it is implemented on a timely basis
Stakeholder Engagement & Customer Service	▪ Ensures compliance between business strategies and information assurance by setting strategies, policies, standards and practices and leading the provision of information assurance expertise, advice and guidance across all of the organisation's information and information systems. ▪ Initiates development of innovative methods, practices and technology, to the benefit of organisation. ▪ Conducts internal training of staff in communicating and understanding fundamental cyber security practices, risks, and recommended mitigation tactics. Acting as an external spokesperson for cyber in support of our efforts and initiatives, you'll be responsible for staying abreast of industry standards and trends and maintaining relevant expertise.
Documentation	▪ Ensures that processes are documented and in place for consistent classification and management of system maintenance and configuration items, and for verification and audit of configuration records. ▪ Produces detailed designs and documents all work using required standards, methods and tools, including prototyping tools where appropriate.

	▪ Ensures that resolved incidents are properly documented and closed. ▪ Ensures that operational documentation for system software is fit for purpose and current.
Digital Transformation	▪ Assess new and emerging technology that can increase effectiveness of the FRCS security platform and automation delivery. ▪ Contributes strongly to the business service knowledge management system including the research and development of tools, processes and techniques. ▪ Work closely with the Records & Information Management team to establish appropriate information and data management security standards during the transition from paper based filing to digital form. ▪ Work in close collaboration with the team to implement components of the Technology 5year roadmap where this role is held accountable
Risk Management	▪ Provide mitigating strategies for technological risks where this role is held accountable. ▪ Work in partnership with the leadership team to address risks arising from the implementation of technology change initiatives.
Health, Safety, and Wellness	▪ Ensure compliance with relevant Occupational Health and Safety (OHS) obligations. ▪ Support and participate in health, safety and wellness initiatives.

DELEGATIONS

Delegations are in accordance with Leadership Team L5 powers as set out in the FRCS delegations framework.

Staff numbers: Direct reports – 0

PERSON SPECIFICATION

ESSENTIAL - Bachelor Degree in Computer Science, Information Technology, Engineering
- 8 years demonstrated industry experience in Cyber Security Risk Consulting or working in a complex environment.
Virtualisation and Cloud technologies
- ITIL certification

DESIRABLE CISM, CISSP and COBIT certification
Business Analysis, Project Management (PMP or similar) certification

PERFORMANCE COMPETENCY INDICATORS

As a leader in FRCS your performance is measured through two criteria:

- **Performance outcome criteria** for your area of responsibility. These are agreed and reviewed annually. You report monthly to the Deputy Director IT on progress, and provide mitigation strategies and timelines where agreed criteria are at risk of non-achievement.

- **Leadership competencies** - you report monthly to the Deputy Director IT on your leadership performance measured against the competencies for your role. These are set out below.

NB: These may change once the FRCS Leadership Competencies are finalized.

COMPETENCY	COMPETENCY DESCRIPTOR
PROCESS IMPROVEMENT	▪ Consistently good at identifying the necessary processes, and organising the right people to get things done ▪ Knows what to measure and how to measure so that complex processes can be refined and more can be achieved with fewer resources ▪ Can organise resources (people, funding, material, support) and use them effectively to get things done including managing multiple activities at once and recording information in a useful manner

DECISION & ANALYTICAL QUALITY	▪ Utilises a mixture of analysis, critical thinking, experiences, and judgement to make high quality, timely decisions, that produce ideas and solutions that are accurate and demonstrate sound judgement, risk management, and integrity ▪ Can use data mining techniques in discovering patterns in large quantities of data for further analysis and to reach sound conclusions
DRIVE FOR RESULTS	▪ Can be counted on to successfully exceed goals and expectations, continually pushing self and others for results ▪ A self-starter who demonstrates agility in multi-tasking where this is needed
COURAGEOUS CONVERSATION	▪ Is direct and honest in communication with others by providing timely, complete and "actionable" feedback (positive and critical) ▪ Takes a tough stand and faces up to problems with any person or in any situation when necessary
PRESENTATION, COMMUNICATION & VISUAL ART	▪ Effectively presents to a variety of audiences using visual communication methods as appropriate ▪ Commands attention and can read the audience, adjusting approach as needed ▪ Attempts to understand different interactive styles and adjust approach accordingly
LISTENING	▪ Consistently practices attentive and active listening and demonstrates an ability to accurately reflect the opinions of others even when he/she disagrees ▪ Demonstrates tolerance with people and processes by listening, checking and understanding information before making judgments or acting
PROBLEM SOLVING	▪ Uses rigorous logic and methods for trouble shooting, recognizing and solving difficult and/or hidden problems by providing effective solutions; and looks broadly for answers and searching beyond obvious answers for the best solutions ▪ Conducts high quality and honest analysis of information and data to aid in problem solving
SELF DEVELOPMENT	▪ Is personally committed to and actively works to continuously improve self ▪ Understands that different situations may call for different skills and approaches, works to strengths and compensates for weaknesses.

ICT Security Analyst - Position Description –