A gamification platform focused on cybersecurity awareness

1	**Problem Statement**	To create an engaging gamification platform that enhances cybersecurity awareness across the organisation.
2	**Technology Area**	Cybersecurity

3	**Project Introduction**	Security professionals face challenges in delivery of security awareness trainings as these trainings are perceived as a punishment or chores by users. Human risk element in the context of cybersecurity demands 100% coverage of cyber security awareness trainings for employees in the organisation in addition to vendors, suppliers and other stakeholders which is one of the mandatory clauses under ISO27001 standard.
		In addition to coverage, Cyber security awareness trainings demands both learning and behavioural change so that mistakes are not repeated by users. Skinner's theory of user conditioning suggests that learning and behaviour change are the result of both reinforcement and punishment. Gamification of any training or awareness campaign combines both reinforcement and punishment by introducing elements of games in various scenarios and has shown to boost engagement by 60% (https://gitnux.org/gamification-statistics/).
		• Purpose of the challenge - To create an engaging gamification platform that enhances cybersecurity awareness across the organisation.
		• Target audience – Gamification platform to cater cybersecurity awareness training for following roles:
		  ○ Employees of organisation
		  ○ Top management
		  ○ System administrators who are managing the IT infrastructure

4	**Description**	**1. Gamification platform overview**
		• Duration - 1 month with daily micro-learning activities and higher levels are unlocked only after completion of lower levels for each user.
		• Key Objectives - Increase cyber security awareness by 50% (measured by pre and post assessments).
		• Components:
		  ○ Learning Modules comprising of interactive e-learning content, multimedia lessons covering various cybersecurity topics, adaptive learning paths based on user role and prior knowledge and bite-sized modules (5-15 minutes each) for easy consumption
		  ○ Case studies of real-world security incidents and their resolutions
		  ○ Infographics and quick reference guides, visually appealing summaries of key concepts
		  ○ Role specific simulations (e.g., for users - phishing email identification exercises, for top management – crisis management scenarios, for admins – breach detection and response simulations).
		  ○ Decision-making exercises under time pressure

		• Gamification Elements:
		  ○ Point system: Points awarded for completed activities, correct answers, and speed, bonus points for exceptional performance or going beyond requirements, point multipliers for streak maintenance (e.g., daily logins)
		  ○ Challenges and missions: Daily cybersecurity tips with associated micro-tasks, weekly themed challenges (e.g., "Password Security Week"), special event challenges tied to real-world security occurrences
		  ○ Progress tracking: Personal dashboards showing completed modules and scores, visual skill trees representing different security domains, completion percentages for each major topic area
		  ○ Discussion forums: Moderated spaces for sharing experiences and asking questions, expert corners for deep dives into specific security topics, idea submission boards for platform and security improvement suggestions
		  ○ Leaderboards
		  ▪ Global Leaderboards: Showing top performers across the entire organization
		  ▪ Role-specific Leaderboards: Separate rankings for Users, Management, and System Administrators
		  ▪ Departmental/group Leaderboards: Encourages friendly competition between different departments/groups
		  ▪ Topic-specific Leaderboards: Highlights top performers in specific security domains
		  ○ Narrative and Theming
		  ▪ Overarching Storyline: Cohesive narrative that ties learning modules together e.g., users can take on roles as "cyber defenders" protecting a virtual organization
		  ▪ Character Progression: Users can customize and upgrade their virtual "security expert" avatar as they progress
		  ○ Feedback Mechanisms
		  ▪ Immediate Feedback: Instant results and explanations after quizzes or scenario challenges, encouraging messages for correct answers and constructive guidance for mistakes
		  ▪ Progress Notifications: Alert users of level-ups, newly unlocked content, or approaching milestones, weekly email digests summarizing progress and suggesting next steps
		2. Platform Requirements
		• Core features
		  ○ User Management: Role-based access control (RBAC)

		for Users, Management, and Admins, integration with existing enterprise authentication systems, user profile management with customizable avatars and progress tracking o Content Management System (CMS): Easy-to-use interface for creating and updating learning modules, support for various content types (text, video, interactive elements), Support for various content types (text, video, interactive elements) o Learning Management System (LMS) Integration: Compatibility with common LMS standards (SCORM, xAPI), progress tracking and reporting across all learning activities, customizable learning paths based on user roles and performance o Gamification Engine: Point system with configurable rules and weightings, badge and achievement system with custom design, leaderboards with filtering options (by department/group, role, time-period) o Simulation and scenario builder: Tool for creating interactive cybersecurity scenarios, branching logic for decision-based outcomes, real-time feedback mechanisms for user choices o Assessment and Quizzing System: Various question types (multiple choice, true/false, short answer, etc.), randomized question banks to prevent memorization, timed assessment options with auto-submit functionality. o Reporting and analytics: Comprehensive dashboards for individual and group performance, export functionality for data analysis (CSV, Excel, PDF formats), Custom report builder for management and compliance purposes. o Communication tools: Announcement system for platform-wide notifications, integration with enterprise email for important alerts. • User Interface o Design Principles: Clean, modern interface adhering to GIGW 3.0 guidelines, responsive design for seamless use across desktop and mobile devices o Engagement Elements: Dynamic content blocks (e.g., "Challenge of the Day", "Security Tip"), visual progress indicators (progress bars, completion percentages), interactive tour for new users and feature introductions • Technical Specifications o Platform will be hosted on cloud o Number of concurrent users should be in the range of 2000 (for any live challenge or campaign) o Provision of data backup and redundancy **3. Cybersecurity Content** • Core topics for all users

		○ Fundamentals of Information Security ▪ Basic cybersecurity concepts and terminology ▪ The CIA triad: Confidentiality, Integrity, and Availability ▪ Overview of common threats and attack vectors ○ Password Security ▪ Creating strong, unique passwords ▪ Password management tools and best practices ▪ Multi-factor authentication (MFA) ○ Social Engineering Awareness ▪ Recognizing phishing attempts (email, voice, SMS) ▪ Social media security and privacy ▪ Physical security and tailgating prevention ○ Data Protection ▪ Handling sensitive information ▪ Secure file sharing and storage practices ▪ Data classification and its importance ○ Mobile Device Security ▪ Securing smartphones and tablets ▪ Safe use of public Wi-Fi ▪ Mobile app permissions and risks ○ Incident Reporting ▪ Identifying and reporting security incidents ▪ The importance of timely reporting ▪ Escalation procedures ○ Email Security ▪ Advanced phishing identification techniques ▪ Safe handling of attachments and links ▪ Email encryption basics ○ Safe Web Browsing ▪ Recognizing malicious websites ▪ Understanding HTTPS and SSL/TLS ▪ Safe download practices ○ Workstation Security ▪ Keeping software and operating systems updated ▪ Using antivirus and anti-malware tools ▪ Clean desk policy and screen locking ○ Remote Work Security ▪ VPN usage and best practices ▪ Securing home networks ▪ Balancing productivity and security in remote settings • Top Management specific content ○ Cybersecurity Risk Management ▪ Understanding the cybersecurity threat landscape ▪ Risk assessment and mitigation strategies

		▪ Balancing security with business objectives ○ Compliance and Regulations ▪ Overview of relevant cybersecurity regulations (e.g., IT Act, Personal Data Protection Act etc) ▪ Industry-specific compliance requirements ▪ Implications of non-compliance ○ Incident Response Planning ▪ Components of an effective incident response plan ▪ Role of leadership in cybersecurity incidents ▪ Crisis communication during security breaches ○ Security Awareness Program Management ▪ Fostering a culture of security ▪ Measuring the effectiveness of security training ▪ Allocating resources for cybersecurity initiatives ○ Third-party Risk Management ▪ Assessing vendor security practices ▪ Contract considerations for data protection ▪ Monitoring and managing third-party access • System Administrator-Specific Content ○ Network Security ▪ Firewall configuration and management ▪ Intrusion detection and prevention systems ▪ Network segmentation and access controls ○ System Hardening ▪ Operating system and application hardening techniques ▪ Patch management best practices ▪ Secure configuration management ○ Identity and Access Management ▪ Implementing and managing access controls ▪ Privileged account management ▪ Single Sign-On (SSO) and directory services ○ Encryption Technologies ▪ Data-at-rest and data-in-transit encryption ▪ Key management practices ▪ Implementing PKI and certificate management ○ Log Management and Security Information and Event Management (SIEM) ▪ Setting up effective logging ▪ Log analysis for threat detection ▪ SIEM tool configuration and management ○ Vulnerability Management ▪ Conducting vulnerability assessments ▪ Penetration testing methodologies ▪ Remediation prioritization and management ○ Cloud Security ▪ Securing cloud environments (IaaS, PaaS, SaaS)

		▪ Cloud access security brokers (CASB) ▪ Shared responsibility models **4. Learning Objectives** • For All Users ○ Understand basic cybersecurity concepts and their importance ○ Recognize common cyber threats and attack methods ○ Apply best practices for personal and organizational cybersecurity ○ Know how to report potential security incidents ○ Implement advanced practices for securing personal workstations and devices ○ Demonstrate proficiency in identifying sophisticated phishing attempts ○ Apply secure practices in remote work environments • For Top Management ○ Evaluate cybersecurity risks and their potential business impact ○ Develop strategies for promoting a strong security culture ○ Make informed decisions on cybersecurity investments and policies ○ Lead effectively during cybersecurity incidents • For System Administrators ○ Design and implement robust security architectures ○ Demonstrate proficiency in configuring and managing security tools ○ Develop and execute incident response and recovery procedures ○ Stay current with emerging threats and mitigation techniques
5	**Roles & Responsibilities of C-DOT**	C-DOT will provide technical development assistance, and financial support to the project partner(s) selected through a process of evaluation and due diligence conducted by a committee of subject experts. Wherever deemed necessary and depending upon the project type (i.e. co-development or fully outsourced), C-DOT may arrange resources, equipment, training, testing infrastructure, mandatory clearances, statutory permissions, and provide gap funding to the partner(s) in realizing the respective target deliverables. Development costs of the module, whether developed from scratch or derived from existing background technology of partner(s), shall be borne by C-DOT. C-DOT shall use the final solution for integration with production grade software. C-DOT reserves the right to modify and enhance the solution and provide it to C-DOT customers or another Partner(s). C-DOT shall engage with Partner(s) on a non-exclusive basis and shall retain its right to develop similar projects/products through other

		developmental programs.
6	**Roles & Responsibilities of Partner(s)**	The Partner(s) may build the required module afresh or by modifying pre-existing background technologies available with them. As per the project demand or project type, the Partner(s) may utilize the available test and infrastructure facilities offered by C-DOT with no/some financial implication for its usage. All commercial proposals shall include necessary cloud infrastructure cost as per requirements, manpower and cost breakup (Capital, Consumables, Travel, DA, Training, Contingency, Overhead, GST etc.). The proposal should include minimum of two years support for enhancements and capacity building for future enhancements in the product. Participation in the project shall be on a non-exclusive basis. All partner(s) shall be required to demonstrate commitment to the project by entering into a formal agreement with C-DOT as per the CCRP policy.
7	**Expected Deliverables**	Web-based gamification platform for cybersecurity awareness which can hosted on-prem or as SaaS on cloud complying to description (Sl. No. 4).
8	**Ownership of Background & Foreground IP**	All technologies created during the project shall be owned by the respective development partner(s), individually or collectively as the case may be. Any agreement required for collective ownership shall be settled directly by the concerned partners, but the ownership/IPR of the final solution shall rest with C-DOT only with all the deliverables including complete source code etc.