QUALIFICATION FILE

Cybersecurity Analyst

☒ Short Term Training (STT) ☐ Long Term Training (LTT) ☐ Apprenticeship

☐ Upskilling ☐ Dual/Flexi Qualification ☐ For ToT ☐ For ToA

☐General ☐ Multi-skill (MS) ☐ Cross Sectoral (CS) ☒ Future Skills ☐ OEM

NCrF/NSQF Level: 5

Submitted By:

IIT Guwahati

Table of Contents

Section 1: Basic Details

<table>
<tr><td>1.</td><td>Qualification Name</td><td colspan="2">Cybersecurity Analyst</td></tr>
<tr><td>2.</td><td>Sector/s</td><td colspan="2">IT-ITeS</td></tr>
<tr><td>3.</td><td>Type of Qualification: ☒ New ☐ Revised ☐ Has Electives/Options ☐OEM</td><td>NQR Code & version of existing/previous qualification: (change to previous, once approved)
QG-05-IT-04149-2025-V1-IITG</td><td>Qualification Name of existing/previous version:</td></tr>
<tr><td>4.</td><td>a. OEM Name
b. Qualification Name
(Wherever applicable)</td><td colspan="2"></td></tr>
<tr><td>5.</td><td>National Qualification Register (NQR) Code &Version
(Will be issued after NSQC approval)</td><td>QG-05-IT-04149-2025-V1-IITG</td><td>6. NCrF/NSQF Level: 5</td></tr>
<tr><td>7.</td><td>Award (Certificate/Diploma/Advance Diploma/ Any Other (Wherever applicable specify multiple entry/exits also & provide details in annexure)</td><td colspan="2">CERTIFICATE</td></tr>
<tr><td>8.</td><td>Brief Description of the Qualification</td><td colspan="2">The “CyberSecurity Analyst” course aims to create skilled Cyber Security professionals. Upon course completion, students will attain proficiency in areas of core cybersecurity areas of Network security, Cloud security and penetration testing. Students will also gain practical exposure to areas like implementing IAM, ensuring compliances according to standards like ISO27001, DPDPA, SOC2 Type2, Handling SIEM tools, incident reporting & management and fundamentals of data security in industry. The course gives students a healthy mix of theoretical core cybersecurity concepts and practical learning of cybersecurity industry tools and best practices.</td></tr>
<tr><td>9.</td><td>Eligibility Criteria for Entry for Student/Trainee/Learner/Employee</td><td colspan="2">a. Entry Qualification & Relevant Experience:
<table>
<tr><th>S. No.</th><th>Academic/Skill Qualification (with Specialization - if applicable)</th><th>Required Experience (with Specialization - if applicable)</th></tr>
<tr><td>1</td><td>Completed 4 year UG (in case of 4 year UG)**</td><td>No experience required</td></tr>
<tr><td>2</td><td>Completed 2nd year of Diploma after 12th **</td><td>No experience required</td></tr>
<tr><td>3</td><td>Completed 3 year of Diploma after 10th **</td><td>1.5 year relevant experience **</td></tr>
<tr><td>4</td><td>12th Grade pass</td><td>3-year relevant experience **</td></tr>
<tr><td>5</td><td>Previous relevant Qualification of NSQF Level 4.5</td><td>1.5 year relevant experience **</td></tr>
</table>
** Experience in IT, Electronics, Electrical, Computer Science field</td></tr>
</table>

<table>
<tr><td></td><td></td><td colspan="2">b. Age:</td></tr>
<tr><td>10.</td><td>Credits Assigned to this Qualification, Subject to Assessment (as per National Credit Framework (NCrF))</td><td>23</td><td>11. Common Cost Norm Category (I/II/III) (wherever applicable): NA</td></tr>
<tr><td>12.</td><td>Any Licensing requirements for Undertaking Training on This Qualification (wherever applicable)</td><td colspan="2">NA</td></tr>
<tr><td>13.</td><td>Training Duration by Modes of Training Delivery (Specify Total Duration as per selected training delivery modes and as per requirement of the qualification)</td><td colspan="2">☐ Offline ☐ Online ☒Blended
<table><tr><th>Training Delivery Modes</th><th>Theory (Hours)</th><th>Practical (Hours)</th><th>OJT Mandatory (Hours)</th><th>OJT Recommended (Hours)</th><th>Total (Hours)</th></tr><tr><td>Classroom (offline)</td><td></td><td>78</td><td>60</td><td></td><td rowspan="2">690</td></tr><tr><td>Online</td><td>252</td><td>300</td><td></td><td></td></tr></table>(Refer Blended Learning Annexure for details)</td></tr>
<tr><td>14.</td><td>Aligned to NCO/ISCO Code/s (if no code is available mention the same)</td><td colspan="2">2522.0201 Security Analyst
3513.0200 Computer Security Specialist</td></tr>
<tr><td>15.</td><td>Progression path after attaining the qualification (Please show Professional and Academic progression)</td><td colspan="2">Horizontal Progression
1. Cybersecurity Analyst
2. SOC Analyst
3. Cloud Security Analyst

Vertical Progression
1. Cybersecurity Analyst
2. Cybersecurity Specialist
3. Cybersecurity Architect
4. Director of Cybersecurity
5. Chief Information Security Officer</td></tr>
<tr><td>16.</td><td>Other Indian languages in which the Qualification & Model Curriculum are being submitted</td><td colspan="2">Hindi and English</td></tr>
<tr><td>17.</td><td>Is similar Qualification(s) available on NQR-if yes, justification for this qualification</td><td colspan="2">☐ Yes ☒ No URLs of similar Qualifications:</td></tr>
<tr><td>18.</td><td>Is the Job Role Amenable to Persons with Disability</td><td colspan="2">☒ Yes ☐ No
If “Yes”, specify applicable type of Disability: PwD</td></tr>
<tr><td>19.</td><td>How Participation of Women will be Encouraged</td><td colspan="2">1. Awareness and Outreach Programs
2. Mentorship and Networking Opportunities</td></tr>
</table>

		3. Inclusive Learning Environments **4. Flexible Learning Options** **5. Industry Partnerships**	
20.	**Are Greening/ Environment Sustainability Aspects Covered** *(Specify the NOS/Module which covers it)*	☐ **Yes** ☒ **No**	
21.	**Is Qualification Suitable to be Offered in Schools/Colleges**	**Schools** ☐ **Yes** ☐ **No** **Colleges** ☒ **Yes** ☐ **No**	
22.	**Name and Contact Details of Submitting / Awarding Body SPOC** *(In case of CS or MS, provide details of both Lead AB & Supporting ABs)*	**Name:** Prof. Gaurav Trivedi **Email:** trivedi@iitg.ac.in **Contact No.:** +91 -8011000783 **Website:** https://www.iitg.ac.in/trivedi/index.html	
23.	**Final Approval Date by NSQC:** *08.05.2025*	**24. Validity Duration: 3 years**	**25. Next Review Date: 08.05.2028**

Section 2: Module Summary

NOS/s of Qualifications

(In exceptional cases these could be described as components)

Mandatory NOS/s:

Specify the training duration and assessment criteria at NOS/ Module level. For further details refer to the curriculum document.

***Th.**-Theory **Pr.**-Practical **OJT**-On the Job **Man.**-Mandatory Training **Rec.**-Recommended **Proj.**-Project*

S. No	NOS/Module Name	NOS/Module Code & Version *(if applicable)*	Core/ Non-Core	NCrF/NSQF Level	Credits as per NCrF	Training Duration (Hours)					Assessment Marks					
						Th.	Pr.	OJT-Man.	OJT-Rec.	Total	Th.	Pr.	Proj.	Viva	Total	Weightage (%) *(if applicable)*
1.	Working with Kali Linux	IITG/CSA01/ NoS/N01	Core	5	1	10	20	0	0	30	10	0	0	0	10	3
2.	Network Security	IITG/CSA01/ NoS/N02	Core	5	2	22	23	15	0	60	10	5	0	0	15	5
3.	Introduction to coding and cybersecurity	IITG/CSA01/ NoS/N03	Core	5	1	8	17	5	0	30	10	5	0	0	15	5
4.	Incident detection with SIEM	IITG/CSA01/ NoS/N04	Core	5	2.5	22	38	15	0	75	20	10	0	0	30	10
5.	Introduction to Capture the Flags	IITG/CSA01/ NoS/N05	Core	5	1	10	20	0	0	30	0	20	0	0	20	7
6.	Security Operations and IAM	IITG/CSA01/ NoS/N06	Core	5	2	20	40	0	0	60	10	5	0	0	15	5
7.	Web Application Testing	IITG/CSA01/ NoS/N07	Core	5	3	30	50	10	0	90	10	10	0	0	20	7
8.	Software Development Security	IITG/CSA01/ NoS/N08	Core	5	3.5	35	70	0	0	105	20	10	0	0	30	10
9.	Government Risk and Compliance	IITG/CSA01/ NoS/N09	Core	5	1.5	15	30	0	0	45	20	5	10	0	35	11
10.	Data Security and AI security	IITG/CSA01/ NoS/N10	Core	5	1.5	20	20	5	0	45	20	5	10	0	35	11
11.	Capstone Project	IITG/CSA01/ NoS/N11	Core	5	2	20	30	10	0	60	0	40	40	0	80	16

S. No	NOS/Module Name	NOS/Module Code & Version *(if applicable)*	Core/ Non-Core	NCrF/NSQF Level	Credits as per NCrF	Training Duration (Hours)					Assessment Marks					
						Th.	Pr.	OJT-Man.	OJT-Rec.	Total	Th.	Pr.	Proj.	Viva	Total	Weightage (%) *(if applicable)*
12.	Employability Skills	DGT/VSQ/N0102	Non-Core	5	2	40	20	0	0	60	40	10	0	0	50	10
Duration (in Hours) / Total Marks					23	252	378	60	0	690	170	125	60	0	355	100

Optional NOS/s:

S. No	NOS/Module Name	NOS/Module Code & Version *(if applicable)*	Core/ Non-Core	NCrF/NSQF Level	Credits as per NCrF	Training Duration (Hours)					Assessment Marks					
						Th.	Pr.	OJT-Man.	OJT-Rec.	Total	Th.	Pr.	Proj.	Viva	Total	Weightage (%) *(if applicable)*
						0	0	0	0	0	0	0	0	0	0	0
Duration (in Hours) / Total Marks						0	0	0	0	0	0	0	0	0	0	0

Assessment - Minimum Qualifying Percentage

*Please specify **any one** of the following:*

Minimum Pass Percentage – Aggregate at qualification level: 70 % *(Every Trainee should score specified minimum aggregate passing percentage at qualification level to successfully clear the assessment.)*

Minimum Pass Percentage – NOS/Module-wise: __% *(Every Trainee should score specified minimum passing percentage in each mandatory and selected elective NOS/Module to successfully clear the assessment.)*

Section 3: Training Related

1.	**Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	**B.Tech in CS / IT / EC / EE / allied areas, MCA, B-Level 'IT' with 2 years of experience in the Cybersecurity Industry / In similar roles as Qualification Name or Progression Paths as mentioned above** **No platform qualification needed**
2.	**Master Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	**IIT Guwahati Professors** **No platform qualification needed**

3.	**Tools and Equipment Required for Training**	☐Yes ☒No (*If "Yes", details to be provided in Annexure)*
4.	**In Case of Revised Qualification, Details of Any Upskilling Required for Trainer**	

Section 4: Assessment Related

1.	**Assessor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	**B.Tech in CS / IT / EC / EE / allied areas, MCA, B-Level 'IT' with 4 years of experience in the Cybersecurity Industry / In similar roles as Qualification Name or Progression Paths as mentioned above** **No platform qualification needed**
2.	**Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	**B.Tech in CS / IT / EC / EE / allied areas, MCA, B-Level 'IT' with 5 years of experience in the Cybersecurity Industry / In similar roles as Qualification Name or Progression Paths as mentioned above** **No platform qualification needed**
3.	**Lead Assessor's/Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	**B.Tech in CS / IT / EC / EE / allied areas, MCA, B-Level 'IT' with 5 years of experience in the Cybersecurity Industry / In similar roles as Qualification Name or Progression Paths as mentioned above** **No platform qualification needed**
4.	**Assessment Mode** *(Specify the assessment mode)*	**Online**
5.	**Tools and Equipment Required for Assessment**	☒ Same as for training ☐ Yes ☐ No *(details to be provided in Annexure-if it is different for Assessment)*

Section 5: Evidence of the need for the Qualification

Provide Annexure/Supporting documents name.

1.	**Latest Skill Gap Study (not older than 2 years) (Yes/No):** Yes
2.	**Latest Market Research Reports or any other source (not older than 2 years) (Yes/No):** Yes
3.	**Government /Industry initiatives/ requirement (Yes/No):** Yes
4.	**Number of Industry validation provided:** 6
5.	**Estimated nos. of persons to be trained and employed:** 500
6.	**Evidence of Concurrence/Consultation with Line Ministry/State Departments:** *Yes* If "No", why:

Section 6: Annexure & Supporting Documents Check List

Specify Annexure Name / Supporting document file name

1.	**Annexure:** NCrF/NSQF level justification based on NCrF level/NSQF descriptors *(Mandatory)*	*Yes*
2.	**Annexure:** List of tools and equipment relevant for qualification *(Mandatory, except in case of online course)*	*A minimum 4GB RAM laptop along with an internet connection.*
3.	**Annexure:** Detailed Assessment Criteria *(Mandatory)*	*Yes*
4.	**Annexure:** Assessment Strategy *(Mandatory)*	*Yes*
5.	**Annexure:** Blended Learning *(Mandatory, in case selected Mode of delivery is "Blended Learning")*	*Yes*
6.	**Annexure:** Multiple Entry-Exit Details *(Mandatory, in case qualification has multiple Entry-Exit)*	*No, no multiple Entry-Exit*
7.	**Annexure:** Acronym and Glossary *(Optional)*	*Yes*
8.	**Supporting Document:** Model Curriculum *(Mandatory – Public view)*	*Yes*
9.	**Supporting Document:** Career Progression *(Mandatory - Public view)*	*Yes*
10.	**Supporting Document:** Occupational Map *(Mandatory)*	*Yes*
11.	**Supporting Document:** Assessment SOP *(Mandatory)*	*Yes*
12.	**Any other document you wish to submit:**	

Annexure: Evidence of Level

NCrF/NSQF Level Descriptors	Key requirements of the job role/ outcome of the qualification	How the job role/ outcomes relate to the NCrF/NSQF level descriptor	NCrF/NSQF Level
Professional Theoretical Knowledge/Process	**Professional Theoretical Knowledge** 1. Demonstrate a comprehensive understanding of **Linux systems**, including Kali Linux, and its key services, as a foundation for cybersecurity.	The curriculum imparts **comprehensive theoretical knowledge** of cybersecurity concepts such as networking, incident detection, web application security, ethical hacking, and	5

	2. Apply advanced **networking concepts** such as IP addressing, OSI/TCP-IP models, subnetting, and traffic analysis to secure network environments. 3. Gain proficiency in **programming and secure coding practices** to identify and mitigate security vulnerabilities. 4. Understand the fundamentals of **Incident Detection and Response** using SIEM tools and techniques for triaging and alert analysis. 5. Acquire in-depth knowledge of **cybersecurity operations**, including Security Operations Center (SOC) management, identity access management (IAM), and cloud-native SIEM deployments. **Practical Process Knowledge** 1. Conduct **vulnerability assessments** and **penetration testing** for web applications, networks, and systems using tools like Nessus, Trivy, and Burp Suite. 2. Implement **firewalls, sniffers, and packet analyzers** to secure network communications. 3. Perform **ethical hacking** exercises, including footprinting, reconnaissance, vulnerability identification, and exploitation techniques. 4. Set up and configure testing environments for web applications and container security, identifying vulnerabilities and proposing mitigation strategies. 5. Execute **cloud security measures** by managing secure access controls, data protection, and compliance. **Technical and Operational Expertise** 1. Develop and implement **ISO 27001 compliance frameworks**, maintaining audit readiness and certification processes. 2. Ensure data protection through strategies aligned with the **Digital Personal Data Protection (DPDP) Act**, including data classification, anonymization, and pseudonymization techniques.	compliance frameworks like ISO 27001 and DPDP. Specialized topics like **AI in cybersecurity** and **threat modeling** demonstrate advanced knowledge in contemporary cybersecurity challenges, aligning with higher-level theoretical expertise. Students are trained in **practical cybersecurity techniques**, such as using sniffers, firewalls, penetration testing tools (e.g., Nessus, Trivy), and SIEM solutions for real-world problem-solving. Hands-on **Capture the Flag (CTF)** challenges, such as Crypto Hunt and OSINT Hung, allow learners to apply skills to solve practical cybersecurity issues, enhancing analytical and technical competencies. The curriculum emphasizes clear **communication of findings and reports**, such as creating vulnerability assessments and reporting security issues to developers. Strong use of **IT tools and techniques**, including ELK Stack, Burp Suite, and AI-based tools, supports learners in applying IT skills to professional practices. Core principles of **secure coding practices** and the use of programming tools address the need for logical, methodical approaches to problem-solving. The **capstone projects** and **virtual SOC demonstrations** help learners take ownership of complex cybersecurity processes and manage security operations in team settings.	

	3. Leverage AI technologies for **threat detection, vulnerability management, and incident response** while addressing ethical and privacy challenges. 4. Utilize tools like ELK Stack, FortiSIEM, and AI-based platforms for real-time data monitoring and analysis. 5. Handle real-world scenarios through **Capture the Flag (CTF)** challenges such as Crypto Hunt, OSINT Hung, and The Last Key, to strengthen practical skills. **Compliance and Risk Management** 1. Identify and manage **cybersecurity risks** by integrating compliance requirements with technical controls. 2. Build a solid foundation in **governance, risk, and compliance (GRC)** to align cybersecurity practices with organizational goals. 3. Evaluate and implement **data security frameworks**, including encryption, Data Loss Prevention (DLP), and monitoring/auditing measures. **Leadership and Strategic Skills** 1. Design and manage secure system architectures within the **Software Development Lifecycle (SDLC)**, incorporating DevSecOps principles. 2. Contribute to cross-functional collaboration by effectively **communicating security findings** and remediation strategies to development teams. 3. Apply **threat modeling and vulnerability identification** techniques to proactively secure systems and infrastructure. **Critical Thinking and Problem-Solving** 1. Analyze complex cybersecurity challenges, develop solutions, and execute them effectively in dynamic environments. 2. Develop actionable plans from vulnerability reports and communicate findings to stakeholders for resolution.	Emphasis on **secure system design** within the SDLC and DevSecOps principles prepares students to handle both individual responsibilities and team collaboration in organizational contexts.	

	3. Engage in strategic planning for securing the perimeter through **capstone projects** and security assessments.		
Professional and Technical Skills/ Expertise/ Professional Knowledge	**1. Professional Knowledge** ● Comprehensive understanding of **Linux systems** (e.g., Kali Linux) and their key services to establish secure computing environments. ● Proficiency in **networking concepts**, including IP addressing, subnetting, OSI/TCP-IP models, and network topologies. ● In-depth knowledge of **cybersecurity frameworks and compliance standards**, such as ISO 27001 and the DPDP Act. ● Expertise in **incident detection and response** using tools like SIEM and FortiSIEM. ● Theoretical grounding in **ethical hacking techniques**, including reconnaissance, scanning, enumeration, and system exploitation. ● Advanced knowledge of **AI in cybersecurity**, including LLM-based tools and AI-driven threat detection. **2. Technical Skills/Expertise** ● Hands-on experience with **vulnerability assessment and penetration testing tools** (e.g., Nessus, Trivy, Burp Suite, Wireshark). ● Practical skills in setting up and managing **firewalls, sniffers, and packet analyzers** for secure communication and network monitoring. ● Advanced expertise in **web application security testing**, including OWASP Top 10 vulnerabilities and manual/automated testing techniques. ● Competence in **malware analysis**, employing static and dynamic analysis techniques.	The curriculum equips learners with a deep understanding of **network security, incident detection, secure coding, and compliance frameworks** like ISO 27001 and the DPDP Act, aligning with the descriptor's emphasis on theoretical depth. Advanced knowledge in emerging areas such as **AI-driven threat detection**, **container security**, and **cloud-native SIEMs** reflects expertise in a dynamic cybersecurity field. Hands-on experience with tools like **Nessus, Burp Suite, Wireshark, and ELK Stack** develops practical skills for addressing cybersecurity challenges. The ability to perform **vulnerability assessments**, **penetration testing**, and **malware analysis** ensures proficiency in generating solutions for real-world security threats. Advanced tasks such as **threat hunting**, **cloud security implementation**, and **data masking** demonstrate mastery in applying technical knowledge to solve complex problems. The ability to **write and present detailed vulnerability reports**, communicate risks, and recommend mitigations aligns with the need for strong communication skills. Logical reasoning is emphasized in tasks such as **risk analysis**, **incident response**, and **threat modeling**. Proficiency in using IT tools for **network monitoring, testing, and securing systems** demonstrates alignment with professional practices. The curriculum prepares learners to independently handle **incident detection**,	5

	• Proficiency in **cloud security**, implementing IAM, securing cloud infrastructures, and managing container vulnerabilities. • Advanced capabilities in **data encryption, masking, and pseudonymization** for robust data protection. **3. Process Knowledge** • Knowledge of **SOC implementation** and the processes for asset management, alert triaging, and compliance handling. • Familiarity with the **secure software development lifecycle (SDLC)** and DevSecOps principles. • Expertise in **threat modeling**, risk assessment, and mitigation strategies for cybersecurity operations. • Understanding of **regulatory compliance processes**, including ISO audits, data classification, and reporting vulnerabilities. **4. Professional Expertise** • Ability to independently conduct **security assessments**, analyze risks, and implement controls to mitigate vulnerabilities. • Skills in **collaborative problem-solving** with cross-functional teams for secure system design and remediation planning. • Leadership in managing cybersecurity projects, including **capstone projects** on perimeter security and compliance assessments. • Adaptability in addressing unpredictable challenges in dynamic cybersecurity environments. **5. Advanced and Emerging Skills** • Application of **AI and machine learning** for incident response, vulnerability management, and proactive threat detection.	**vulnerability scanning**, and **system hardening** tasks. Real-world simulations, such as **Capture the Flag (CTF)** exercises, develop problem-solving abilities and decision-making skills in unpredictable cybersecurity scenarios. Responsibility is highlighted in tasks like **SOC management**, **compliance audits**, and **secure architecture design**, where learners must balance technical and organizational requirements. Exposure to emerging technologies, such as **AI-based security tools** and **container scanning**, ensures learners stay relevant in a rapidly evolving field. Participation in **practical exercises, workshops**, and certifications fosters a growth-oriented mindset, ensuring adaptability to future challenges. Continuous learning is embedded in areas like **ethical hacking**, **data encryption**, and **secure SDLC**, providing opportunities for specialization and career advancement. The curriculum integrates **networking, programming, compliance frameworks, and cloud security** knowledge to create a holistic understanding of cybersecurity. Practical application in scenarios like **web application testing, AI security**, and **data classification** bridges theoretical knowledge with real-world execution. Multi-domain integration is exemplified in **capstone projects** and **compliance workshops**,	

	• Securing modern environments through **containerized applications**, employing advanced tools like Trivy. • Knowledge of **future-ready techniques**, including coding vulnerability mitigation and securing development pipelines. • Expertise in handling **data security and classification frameworks**, incorporating advanced techniques like data loss prevention (DLP). **6. Cross-Domain Integration** • Integration of knowledge from **networking, programming, and compliance frameworks** to design end-to-end secure architectures. • Ability to apply cybersecurity knowledge to real-world scenarios, such as **CTF challenges** and compliance workshops. • Bridging gaps between **data security, AI-driven solutions, and traditional cybersecurity strategies** for holistic security management.	where learners apply cross-functional knowledge to secure systems and networks.	

Employment Readiness & Entrepreneurship
Skills & Mind-set/Professional Skill
	1. Employment Readiness Skills
	
	• **Communication Skills**:
	  ○ Ability to effectively articulate security findings, vulnerability reports, and remediation strategies to stakeholders, including technical and non-technical audiences.
	  ○ Proficiency in creating detailed, actionable reports on **cybersecurity incidents**, **vulnerability analysis**, and compliance status.
	• **Analytical Thinking**:
	  ○ Critical thinking to evaluate complex cybersecurity threats and design appropriate countermeasures.
		The curriculum emphasizes **incident detection and response**, equipping learners with decision-making skills to prioritize and address cybersecurity threats.
		Real-world exercises, such as **Capture the Flag (CTF) challenges**, hone problem-solving abilities by simulating dynamic scenarios.
		Learners develop the capacity to analyze and mitigate risks through structured approaches in tasks like **vulnerability assessments**, **malware analysis**, and **ethical hacking**.
		The ability to write **detailed vulnerability reports** and present findings to stakeholders aligns with communication requirements.
		Collaborative projects, such as **SOC implementation and virtual tours**, foster
			5

	○ Decision-making skills for prioritizing alerts and handling triage in Security Operations Centers (SOC). ● **Problem-Solving Skills**: ○ Proficiency in identifying and mitigating vulnerabilities in real-world scenarios, such as through **Capture the Flag (CTF)** challenges and simulated exercises. ○ Applying advanced cybersecurity techniques to solve unpredictable and dynamic problems in cloud, network, and application security. ● **Technical Adaptability**: ○ Demonstrates the ability to learn and work with new tools and technologies, such as AI-based security tools, cloud-native SIEMs, and DevSecOps practices. ○ Stays updated with emerging cybersecurity trends and threats, ensuring relevance in the fast-evolving field. **2. Entrepreneurial Mind-Set** ● **Innovation and Initiative**: ○ Encourages the development of novel approaches to securing systems, data, and networks. ○ Capacity to design unique cybersecurity solutions, leveraging tools like Nessus, Burp Suite, or Trivy, for industry-specific challenges. ● **Leadership Skills**: ○ Takes ownership of projects, such as **capstone assignments** on perimeter security and compliance assessments. ○ Guides teams in identifying and mitigating risks during the implementation of secure architectures. ● **Strategic Thinking**:	teamwork and cross-functional engagement, preparing learners for real-world environments. Skills in presenting complex cybersecurity concepts in a simplified manner enhance employability across diverse industries The curriculum instills leadership skills through **capstone projects** on perimeter security, compliance assessments, and secure architecture design. Strategic thinking is cultivated through tasks like **threat modeling**, **risk management**, and **long-term security planning**. Learners are encouraged to take ownership of cybersecurity challenges, aligning with the entrepreneurial focus on innovation and initiative The curriculum prepares learners to handle evolving threats through continuous exposure to **emerging technologies**, such as AI-driven security tools and cloud-native solutions. Exercises in **incident detection, vulnerability mitigation, and compliance** train learners to adapt to rapid changes in cybersecurity landscapes. Resilience is developed through hands-on activities, enabling learners to maintain composure and effectiveness under pressure. Practical knowledge of tools like **Nessus, Trivy, Burp Suite**, and **FortiSIEM** equips learners with industry-relevant IT expertise. Skills in **time management and task prioritization** are developed through structured project work and practical exercises. Professionalism is reinforced by tasks requiring clear communication, ethical behavior, and a customer-oriented approach in handling security assessments. Continuous learning is embedded in the curriculum through exposure to **CTF challenges**, workshops, and emerging cybersecurity domains.	

	○ Ability to evaluate long-term security implications and align cybersecurity strategies with business goals. ○ Integrates knowledge of **compliance frameworks** (ISO 27001, DPDP Act) with organizational objectives for sustainable growth. ● **Risk and Resource Management**: ○ Skilled in balancing security investments with risk priorities, optimizing resource allocation in small or large organizations. ○ Provides insights into cost-effective tools and processes for startups and enterprises. **3. Professional Skills for Employment and Entrepreneurship** ● **Team Collaboration**: ○ Works efficiently in cross-functional teams, including developers, compliance officers, and IT staff, to enhance organizational security posture. ○ Contributes effectively in **SOC environments**, leveraging collective expertise to detect, respond, and prevent cybersecurity incidents. ● **Project Management**: ○ Capable of planning and executing security projects, such as **virtual SOC tours**, **compliance workshops**, and **penetration testing** exercises. ○ Manages time, resources, and deliverables to meet tight deadlines in dynamic environments. ● **Customer-Oriented Approach**: ○ Understands client requirements and tailors cybersecurity solutions to meet specific needs, fostering trust and business growth. ○ Develops **user-friendly reports and recommendations** to bridge the gap	Learners are encouraged to innovate and explore new techniques for securing systems, such as **container vulnerability mitigation** and **secure SDLC implementation**. A growth-oriented mindset is developed through entrepreneurial tasks, such as designing **customized security solutions** and balancing security investments with organizational goals.	

	between technical complexities and customer understanding. ● **Entrepreneurial Resilience**: ○ Demonstrates adaptability to overcome challenges in launching and scaling security-focused ventures. ○ Balances technical expertise with business acumen to identify and capitalize on cybersecurity market opportunities. **4. Lifelong Learning and Self-Motivation** ● **Continuous Skill Development**: ○ Commitment to learning emerging trends, tools, and techniques, such as **AI in cybersecurity**, **container security**, and **data masking**. ○ Engages in professional certifications and workshops to maintain relevance in the field. ● **Problem Ownership**: ○ Takes proactive measures in resolving security issues, ensuring accountability and precision. ○ Embraces a growth-oriented mindset to tackle new challenges in cybersecurity and business environments.		
Broad Learning Outcomes/Core Skill	**1. Broad Learning Outcomes** ● **Foundational Understanding of Cybersecurity**: ○ Develop a thorough understanding of key cybersecurity concepts, including **network security, ethical hacking, incident detection, and compliance frameworks**. ○ Gain hands-on experience in using industry-standard tools for **vulnerability assessment, penetration testing**, and **security monitoring**.	The curriculum provides a foundational understanding of **cybersecurity principles**, such as **network security, ethical hacking, incident detection, and compliance**. Learners gain cross-domain expertise by integrating concepts from **cloud security, AI-driven cybersecurity tools, and secure software development**.	5

	• **Critical Thinking and Analytical Skills**:
	  ○ Ability to critically assess threats and vulnerabilities, analyze their impact, and design appropriate mitigation strategies.
	  ○ Evaluate the effectiveness of security controls and tools in real-world scenarios.
	• **Cross-Domain Integration**:
	  ○ Integrate knowledge of **cloud security, data protection, and software development security** to create holistic security architectures.
	  ○ Apply cybersecurity principles across domains such as **web application testing, AI security**, and **identity management**.
	• **Emerging Technologies and Trends**:
	  ○ Understand and leverage emerging technologies, including **AI-driven tools**, **cloud-native SIEMs**, and advanced **data encryption techniques**.
	  ○ Adapt to evolving cybersecurity challenges, such as securing **AI systems** and mitigating risks in **containerized applications**.
	
	2. Core Skills
	
	• **Problem-Solving and Decision-Making**:
	  ○ Identify, analyze, and solve complex cybersecurity issues using a structured approach.
	  ○ Make informed decisions during incident detection and response, prioritizing alerts and resources effectively.
	• **Technical Proficiency**:
	  ○ Master tools like **Nessus, Wireshark, Trivy, Burp Suite, and ELK Stack** for analyzing and securing systems.
	  ○ Perform practical tasks, such as **packet analysis, web application security testing**, and **malware analysis**.
	• **Communication and Reporting**:
		Practical applications like **web application testing, vulnerability scanning, and SOC management** ensure learners can connect theoretical knowledge with real-world challenges.
		
		Learners are trained to critically analyze threats and vulnerabilities using tools like **Nessus, Burp Suite**, and **Wireshark**.
		Exercises such as **Capture the Flag (CTF)** challenges and **malware analysis workshops** develop strong problem-solving capabilities.
		Real-world simulations and **incident response training** enhance critical thinking by exposing learners to unpredictable scenarios.
		Skills in preparing and presenting **detailed vulnerability reports** align with professional communication standards.
		Learners practice articulating technical findings to stakeholders, including **developers, compliance teams, and senior management**.
		Collaborative tasks, such as **SOC implementation** and **team-based incident response**, reinforce communication skills.
		The curriculum fosters teamwork through **SOC virtual tours**, where learners collaborate to detect and mitigate threats.
		Cross-functional engagement in projects like **compliance audits** and **perimeter security design** prepares learners for workplace collaboration.
		Learners are trained to balance individual responsibilities with team objectives, ensuring smooth coordination
		The integration of **AI in cybersecurity** and **cloud security techniques** prepares learners to tackle emerging industry trends.
		Learners engage in practical workshops and certifications, fostering a commitment to lifelong learning.	

	○ Develop skills in **writing detailed vulnerability reports**, incident response documentation, and compliance assessments. ○ Communicate technical findings to diverse audiences, bridging the gap between technical teams and non-technical stakeholders. ● **Collaboration and Teamwork**: ○ Work effectively within cross-functional teams in **SOC environments** and during large-scale projects. ○ Collaborate with developers, compliance officers, and IT teams to achieve organizational security goals. ● **Time Management and Organizational Skills**: ○ Plan and execute projects like **perimeter security assessments, compliance workshops**, and CTF challenges within specified timelines. ○ Manage multiple tasks efficiently while maintaining accuracy and attention to detail. **3. Lifelong Learning and Adaptability** ● **Commitment to Continuous Improvement**: ○ Stay updated with industry advancements through certifications, training programs, and self-learning. ○ Participate in **workshops, CTF challenges**, and other practical exercises to enhance skills and knowledge. ● **Adaptability to Evolving Threats**: ○ Quickly adapt to new cybersecurity threats and technologies, applying learned concepts to mitigate risks. ○ Demonstrate resilience and innovation in dynamic and unpredictable cybersecurity environments.	Exposure to advanced tools and frameworks ensures adaptability to rapidly evolving cybersecurity landscapes. Emphasis on **ethical hacking techniques** ensures learners understand the legal and ethical boundaries of cybersecurity practices. Responsibility is instilled through tasks like **incident triaging**, **vulnerability management**, and **compliance workshops**. Learners are trained to approach cybersecurity challenges with integrity and accountability. Practical exercises, such as **malware analysis, penetration testing**, and **data classification**, bridge the gap between theory and application. Capstone projects like **perimeter security design** and **compliance implementation** integrate cross-domain knowledge into practical use cases. Workshops and simulations provide hands-on experience, preparing learners for real-world cybersecurity roles	

	Core Competencies Developed ● **Technical Mastery**: ○ Proficient in using security tools and implementing technical solutions to protect systems, networks, and data. ● **Strategic Thinking**: ○ Develop strategies for long-term security improvements while addressing immediate threats. ● **Professional Integrity**: ○ Maintain ethical standards while conducting cybersecurity operations, ensuring trust and accountability.		
Responsibility	**1. Threat Identification and Risk Analysis** ● **Monitoring and Detection**: ○ Continuously monitor networks and systems for suspicious activities using tools like **SIEM (Security Information and Event Management)**. ○ Detect, investigate, and respond to security incidents in real time. ● **Risk Assessment**: ○ Assess organizational vulnerabilities through regular security audits, penetration testing, and threat modeling. ○ Evaluate the likelihood and impact of potential cyber threats and propose risk mitigation strategies. **2. Incident Response and Management** ● **Incident Handling**: ○ Respond promptly to security incidents, including malware attacks, data breaches, and phishing attempts.	The cybersecurity analyst role emphasizes independent decision-making in **incident detection**, **response management**, and **risk mitigation**. Learners are trained to analyze and prioritize threats autonomously, ensuring quick and effective resolutions. Exercises in **malware analysis**, **vulnerability scanning**, and **threat modeling** prepare learners to handle high-stakes decisions under pressure Through **capstone projects** and **SOC management simulations**, learners take ownership of security operations and guide team efforts. Responsibility is demonstrated in **coordinating incident responses**, delegating tasks, and ensuring timely reporting to stakeholders. Managing compliance processes, such as **ISO 27001 implementation** and **DPDP Act adherence**, highlights accountability in maintaining organizational security standards Emphasis on **ethical hacking techniques** instills a strong sense of responsibility to act within legal and ethical boundaries.	5

	○ Analyze incident patterns to develop and improve response protocols. ● **Post-Incident Analysis**: ○ Conduct forensic investigations to identify the root cause of incidents and recommend preventive measures. ○ Document incident reports and create playbooks for future reference. **3. Security Operations** ● **Network and System Security**: ○ Implement and manage **firewalls, intrusion detection systems (IDS), sniffers**, and other security controls. ○ Ensure all endpoints, including servers, workstations, and mobile devices, are securely configured and monitored. ● **Patch Management**: ○ Regularly update systems and applications to protect against known vulnerabilities. ○ Ensure timely deployment of security patches to mitigate risks. **4. Compliance and Policy Enforcement** ● **Regulatory Compliance**: ○ Ensure organizational security practices comply with frameworks such as **ISO 27001**, **GDPR**, or the **Digital Personal Data Protection (DPDP) Act**. ● **Policy Development**: ○ Assist in creating and enforcing cybersecurity policies and guidelines for employees. ○ Conduct awareness programs to educate employees on best practices, such as recognizing phishing attempts.	Learners develop skills to conduct audits, monitor systems, and report vulnerabilities while ensuring confidentiality and data integrity. Training in **compliance frameworks** ensures alignment with organizational and regulatory requirements. Collaborative activities, such as **virtual SOC tours**, reinforce shared responsibility in detecting and mitigating cybersecurity threats. Learners are trained to work effectively with **developers, IT teams, and compliance officers** to address vulnerabilities and implement security solutions. Cross-functional engagement in projects like **cloud security implementation** highlights the ability to balance individual and team responsibilities Learners are trained to adapt to evolving cybersecurity threats by leveraging emerging tools, such as **AI-driven solutions** and **container security platforms**. Resource allocation during **incident triaging** and **alert management** demonstrates their ability to manage time, tools, and human resources effectively. Hands-on experience with **real-world simulations**, such as CTF challenges, prepares learners to respond to dynamic situations responsibly Responsibility for personal growth is emphasized through exposure to advanced topics like **AI in cybersecurity** and **secure SDLC practices**. Learners are encouraged to pursue certifications and participate in workshops, fostering a commitment to continuous improvement. Practical training ensures learners remain adaptable and ready for future advancements in the cybersecurity field	

	5. Data Protection and Privacy ● **Data Security**: ○ Implement encryption, masking, and pseudonymization techniques to protect sensitive data. ○ Monitor for unauthorized access or data exfiltration attempts. ● **Backup and Recovery**: ○ Establish robust backup and disaster recovery plans to minimize data loss in the event of an attack. **6. Vulnerability Management** ● **Vulnerability Scanning**: ○ Regularly scan for vulnerabilities using tools like **Nessus**, **Burp Suite**, or **Trivy**. ○ Perform static and dynamic analysis of systems and applications to identify weaknesses. ● **Remediation**: ○ Collaborate with development and IT teams to patch vulnerabilities and implement secure coding practices. **7. Advanced Threat Hunting** ● **Proactive Defense**: ○ Hunt for advanced threats that may bypass traditional defenses, such as zero-day vulnerabilities. ○ Use tools like **ELK Stack**, **FortiSIEM**, and **AI-driven solutions** to enhance threat detection capabilities. ● **Malware Analysis**: ○ Analyze malware behavior to understand its impact and develop countermeasures.		

	8. Reporting and Communication ● **Documentation**: ○ Prepare detailed reports on system vulnerabilities, incident analysis, and compliance status. ○ Maintain logs and documentation required for audits and compliance reviews. ● **Stakeholder Communication**: ○ Act as a liaison between technical teams and business stakeholders to convey security risks and solutions. ○ Present actionable insights and recommendations for improving the organization's security posture. **9. Research and Continuous Learning** ● **Staying Updated**: ○ Stay informed about the latest cyber threats, attack vectors, and security technologies. ○ Participate in training, certifications, and workshops to continuously improve skills. ● **Tool Mastery**: ○ Regularly explore new tools and frameworks for enhancing security monitoring, detection, and prevention. **10. Collaboration with Teams** ● **Cross-Functional Engagement**: ○ Work closely with IT, DevOps, and compliance teams to align security measures with organizational goals. ○ Collaborate with external vendors and security service providers for advanced threat analysis and mitigation.		

NCrF Level Descriptors	Key requirements of the job role/ outcome of the qualification	How the job role/ outcomes relate to the NCrF/NSQF level descriptor	NCrF/NSQF Level
Minimum entry criteria for undergoing Short Term Training (STT) - Minimum Education	Completed 1st year of 3-year/ 4-years UG • Pursuing 1st year of 3-year/ 4-years UG and continuing education • Completed 1st year of diploma (after 12th) • Pursuing 1st year of 2-year diploma after 12th	Completed 1st year of 3-year/ 4-years UG • Pursuing 1st year of 3-year/ 4-years UG and continuing education • Completed 1st year of diploma (after 12th) • Pursuing 1st year of 2-year diploma after 12th Our course has the same eligibility criteria as of the NCrF level descriptors for Level 5	5
Minimum entry criteria for undergoing Short Term Training (STT) - Experience	No Experience Required	No Experience Required	5
Minimum Range of Notional hours - In Multiple of 30)	480 to 570 Notional Hours of Training	In our course the total notional hours is 690.	5
Employability Skills (ES) to be Included in the notional hours	60	In our course the total ES notional hours is 60.	5

Annexure: Tools and Equipment (Lab Set-Up)

List of Tools and Equipment

No tools and equipment required apart from a Laptop and an internet connection.

Batch Size:

S. No.	Tool / Equipment Name	Specification	Quantity for specified Batch size

Classroom Aids

The aids required to conduct sessions in the classroom are:

No aids required as a prerequisite to attend the classes apart from a Laptop and an Internet Connection.

1.
2.

Annexure: Industry Validations Summary

Provide the summary information of all the industry validations in table. This is not required for OEM qualifications.

S. No	Organisation Name	Representative Name	Designation	Contact Address	Contact Phone No	E-mail ID	LinkedIn Profile *(if available)*
1	OptiQ	Keshav Murthy	CEO	H1901 No, Hustle hub, Ground Floor, 175, 19th Main Rd, Sector 4, HSR Layout, Bengaluru, Karnataka 560102	6363 098 970	keshav@optiq.ai	https://www.linkedin.com/in/keshava-murthy-a9a389104/
2	Dr Droid	Siddarth Jain	Co-Founder	4th floor, Hustlehub 1703, 17th Cross Rd, next to taco bell, Sector 4, HSR Layout, Bengaluru, Karnataka 560102	95821 48040	siddarth@drdroid.io	https://www.linkedin.com/in/siddarth-jain227/

3	Creatormon Private Limited	Chandan Yadav	Co-founder and CTO	90B, Delhi Gurgaon Expressway, Sector 18, Gurugram	9899284156	chandan@wishlink.com	https://www.linkedin.com/in/chandan-yadav-1011/
4	Electorq Technologies	Shubham Srivastava	Co-Founder	K–258/635,636 Lane,3,Westend Marg,Saiyadul Ajaib, Sainik Farm, New Delhi	95826 10467	qutub@electorq.com	https://www.linkedin.com/in/shubham-srivastava-4ab945128/
5	ParkSmart	Prateek Garg	CTO	BR-26, Sector 116, Noida,Uttar Pradesh	9717278729	prateek@parksmart.in	https://www.linkedin.com/in/prateekgarg95/
6	Quinn Care Private Limited	Mohit Kinra	Co-Founder	404, 22nd Cross, 27th Main, Sector 2, HSR Layout, Bangalore, India - 560102	98911 41917	mohit@quinn.live	https://www.linkedin.com/in/kinra/

Annexure: Training & Employment Details

Training and Employment Projections:

Year	Total Candidates		Women		People with Disability	
	Estimated Training #	Estimated Employment Opportunities	Estimated Training #	Estimated Employment Opportunities	Estimated Training #	Estimated Employment Opportunities
1	500	1000	150	300	5	10
2	1000	1500	300	450	20	40
3	2000	2500	600	800	50	80

Data to be provided year-wise for next 3 years

Training, Assessment, Certification, and Placement Data for previous versions of qualifications:

Qualification Version	Year	Total Candidates				Women				People with Disability			
		Trained	Assessed	Certified	Placed	Trained	Assessed	Certified	Placed	Trained	Assessed	Certified	Placed

Applicable for revised qualifications only, data to be provided year-wise for past 3 years.

List Schemes in which the previous version of Qualification was implemented:

1.
2.

Content availability for previous versions of qualifications:

☐ Participant Handbook ☐ Facilitator Guide ☐ Digital Content ☐ Qualification Handbook ☐ Any Other:

Languages in which Content is available:

Annexure: Blended Learning

Blended Learning Estimated Ratio & Recommended Tools:

Refer NCVET "Guidelines for Blended Learning for Vocational Education, Training & Skilling" available on:
https://ncvet.gov.in/sites/default/files/Guidelines%20for%20Blended%20Learning%20for%20Vocational%20Education,%20Training%20&%20Skilling.pdf

S. No.	Select the Components of the Qualification	List Recommended Tools – for all Selected Components	Offline : Online Ratio
1	☐Theory/ Lectures - Imparting theoretical and conceptual knowledge	Presentations Reference Material	1:2
2	☐Imparting Soft Skills, Life Skills, and Employability Skills /Mentorship to Learners	Self-Learning Videos Curated Digital content Presentations Reference Material	1:2
3	☐Showing Practical Demonstrations to the learners	Presentations	1:2
4	☐Imparting Practical Hands-on Skills/ Lab Work/ workshop/ shop floor training	Online Projects	1:2
5	☐Tutorials/ Assignments/ Drill/ Practice	Online Question Bank Proctored Online tests	1:2
6	☐Proctored Monitoring/ Assessment/ Evaluation/ Examinations	Proctored Online tests	0:1
7	☐On the Job Training (OJT)/ Project Work Internship/ Apprenticeship Training	Proctored Online tests	0:1

Annexure: Detailed Assessment Criteria

Detailed assessment criteria for each NOS/Module are as follows:

NOS/Module Name	Assessment Criteria for Performance Criteria/Learning Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Working with Kali Linux (IITG/CSA01/NoS/N01)	Learn Python basics and environment setup.	4	0	0	0
	Understand Linux file management and cybersecurity concepts. Get introduced to Kali Linux, its services, and shell utilities (wget, curl, grep).	5	0	0	0
	Develop skills in Python and Bash scripting, piping, and redirection.	1	0	0	0
	Total Marks	**10**	**0**	**0**	**0**
Network Security (IITG/CSA01/NoS/N02)	Understand security controls and networking concepts.	3	1.5	0	0
	Learn traffic analysis using packet analyzers and sniffers.	5	1.5	0	0
	Gain knowledge of firewalls, SIEM, VLAN, and VPN technologies.	2	2	0	0
	Total Marks	**10**	**5**	**0**	0

Introduction to coding and cybersecurity (IITG/CSA01/NoS/N03)	Learn programming fundamentals (syntax, variables, debugging) using languages like Python.	2	5	0	0
	Understand cybersecurity basics: malware, encryption, password security, and the CIA triad.	3	0	0	0
	Explore networking essentials: LAN, WAN, TCP/IP, and IP addressing.	5	5	0	0
	Total Marks	**10**	**10**	0	0
Incident detection with SIEM (IITG/CSA01/NoS/N04)	Learn basic concepts, solutions, and deployment of SIEM.	10	3	0	0
	Understand incident detection at application, insider, network, and host levels.	5	3	0	0
	Gain knowledge of SOC fundamentals, including alert triaging, compliance, and implementation.	5	4	0	0
	Total Marks	**20**	**10**	0	0
Introduction to Capture the Flags (IITG/CSA01/NoS/N05)	Learn the basics of Capture the Flag competitions and their importance in cybersecurity.	0	2	0	0
	Understand key CTF categories: cryptography, web exploitation, reverse engineering, and forensics.	0	3	0	0
	Practice real-world problem-solving through beginner-friendly CTF platforms like HackTheBox and TryHackMe.	0	15	0	0
	Total Marks	**0**	**20**	0	0
Security operations and Identity and Access Management (IAM) (IITG/CSA01/NoS/N06)	Learn asset management and authentication/identification management.	3	2	0	0
	Understand integrating identity as a third-party service and authorization mechanisms.	3	3	0	0
	Study the identity and access provisioning lifecycle.	4	0	0	0
	Total Marks	**10**	**5**	0	0
Web Application Penetration Testing (IITG/CSA01/NoS/N07)	Learn OWASP tools, insecure deserialization, clickjacking, and testing methodologies (black box, white box, fuzzing).	2	2	0	0
	Understand cryptography, hashing, digital signatures, API security, and patch management.	2	2	0	0
	Study malware types, ransomware, detection, and analysis; ethical hacking techniques including footprinting, scanning, enumeration, and vulnerability analysis.	2	2	0	0

	Explore system hacking, sniffing, social engineering, DoS, session hijacking, evading IDS, firewalls, honeypots, web server hacking, SQL injection, wireless network hacking, and security for mobile platforms and IoT.	4	4	0	0
	Total Marks	**10**	**10**	0	0
Software Development Security (IITG/CSA01/NoS/N08)	Secure SDLC	5	10	0	0
	Threat Hunting	10	20	0	0
	Designing Security Architecture	5	10	0	0
	Vulnerability Scanning	10	20	0	
	CTF OSINT Hung	5	10	0	
	Total Marks	**35**	**70**	0	0
Government risk & compliance (IITG/CSA01/NoS/N09)	Understand government risk management and compliance requirements.	5	2	0	0
	Learn how to implement and maintain industry-specific regulations.	5	1	0	0
	Develop strategies for aligning business practices with government standards.	10	2	0	0
	Total Marks	**20**	**5**	0	0
Data Security and AI Security (IITG/CSA01/NoS/N10)	Learn data classification, masking, and encryption techniques.	3	0	0	0
	Understand privacy management and regulatory compliance.	3	0	0	0
	Develop strategies for protecting data across various environments.	4	3	0	0
	Understand the use of AI and LLMs in cybersecurity.	3	0	0	0
	Learn about AI security challenges and mitigation strategies.	3	0	0	0
	Explore the impact of AI on cybersecurity and protective measures.	4	2	0	0
	Total Marks	**20**	**5**	0	0
Capstone Project (IITG/CSA01/NoS/N11)	Securing the Perimeter	10	10	0	0
	Security assessment	10	10	0	0
	Compliance Assessment	10	10	0	0
	Data Security Assessment	10	10	0	0
	Total Marks	**40**	**40**	**0**	0
Employability Skills (DGT/VSQ/N0102)	Employability Training	40	20	0	0
	Total Marks	**40**	**20**	**0**	0

Annexure: Assessment Strategy

This section includes the processes involved in identifying, gathering, and interpreting information to evaluate the Candidate on the required competencies of the program.

Mention the detailed assessment strategy in the provided template.

Assessment System Overview:

- Students are given regular assignments and activities on the course platform after each topic is covered. These are evaluated by expert mentors and through live assignment testing processes and feedback is provided.
- Timed contests are held weekly to evaluate students' understanding of concepts covered that week.
- Mock interviews with industry experts are conducted after completion of each module to assess application of concepts.
- Online assessment will be proctored by engaging a third party. The course access of this third party will be with IIT Guwahati and the participants.
- Offline assessment will be invigilator based. Final assessment will be offline in Test centers across India. Participants who will be doing the course in IIT Guwahati campus will be evaluated by course Instructor. For the participants joining through remote centres will be evaluated by sending external experts from IIT Guwahati.
- Remote centres will be NIT's, Govt Colleges and Private colleges which has adequate resources and good internet connectivity.
- Software licences for this program will be provided by IIT Guwahati and also IIT Guwahati will provide a cloud-based utility setup to access these licences remotely (VPN).
- Certified Assessors will be deployed for executing the assessment.

Testing Environment:

- Assignments are completed by students individually on the online platform.
- Timed contests are also conducted online with remote proctoring to prevent cheating.
- Mock interviews are conducted via video conferencing tools.

Assessment Quality Assurance:

- Assignment questions are set by faculty and reviewed by the academic coordinator for alignment to topics covered.
- Timed contest questions are verified by a second subject matter expert.
- Mock interviews are vetted by industry experts with at least 5 years of relevant experience.
- The assessment will have scenario based open book test and one-to-one online viva.
- Theory and Practical assessments will have to be completed in the specified time as given in Module Summary.
- Questions are mapped to all the different modules.
- The Assessors and Trainers have the required education and relevant experience in their field with ToA certified ToT Certified.

Evidence Gathering:

- Student assignment responses, timed contest scores, and mock interview recordings/notes comprise the assessment evidence.
- The online assessments will be saved in the cloud/drive and can be assessed whenever required.

Verification:

- Plagiarism checks are done on assignments using software.
- Timed contests are proctored remotely to prevent cheating.
- Mock interviews are recorded for review.
- Monthly Feedbacks on various aspects of the course, including content clarity, instructional effectiveness, user interface, and overall satisfaction and analyze assessment results to evaluate whether learners are meeting the intended learning outcomes.

Documentation:

- Assessment records are maintained on the learning management platform.
- Assessment data and evidence is archived digitally.
- The online assessments will be saved in the cloud/drive and can be assessed whenever required.

Assessment Strategy:

- Focus on regular formative assessments for feedback rather than high stakes exams.
- Assess both theoretical knowledge and practical application through assignments, contests, and interviews.
- Use industry experts to design and conduct mock interviews to evaluate application of skills.
- Maintain integrity through plagiarism checking, proctoring, and recording of assessment evidence.
- Document assessment data digitally for easy access, review and analysis.

Annexure: Acronym and Glossary

Acronym

Acronym	Description
AA	Assessment Agency
AB	Awarding Body
ISCO	International Standard Classification of Occupations
NCO	National Classification of Occupations
NCrF	National Credit Framework
NOS	National Occupational Standard(s)
NQR	National Qualification Register
NSQF	National Skills Qualifications Framework
OJT	On the Job Training

Glossary

Term	Description

National Occupational Standards (NOS)	NOS define the measurable performance outcomes required from an individual engaged in a particular task. They list down what an individual performing that task should know and also do.
Qualification	A formal outcome of an assessment and validation process which is obtained when a competent body determines that an individual has achieved learning outcomes to given standards
Qualification File	A Qualification File is a template designed to capture necessary information of a Qualification from the perspective of NSQF compliance. The Qualification File will be normally submitted by the awarding body for the qualification.
Sector	A grouping of professional activities on the basis of their main economic function, product, service or technology.
Long Term Training	Long-term skilling means any vocational training program undertaken for a year and above. https://ncvet.gov.in/sites/default/files/NCVET.pdf