QUALIFICATION FILE – Standalone NOS—OEM

Certified Information Security Manager (CISM)-ISACA

☐ Horizontal/Generic ☒ Vertical/Specialization

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

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

NCrF/NSQF Level: 6

Submitted By:

IT-ITeS Sector Skills Council NASSCOM (SSC NASSCOM)

Plot No. – 7, 8, 9 & 10, Sector – 126,

Noida, Uttar Pradesh - 201303

Table of Contents

Section 1: Basic Details

<table>
<tr><td>1.</td><td>NOS-Qualification Name</td><td colspan="2">Certified Information Security Manager (CISM)-ISACA</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</td><td>NQR Code & version of the existing /previous qualification: (change to previous, once approved)</td><td>Qualification Name of the existing/previous version: (previous, once approved)</td></tr>
<tr><td>4.</td><td>National Qualification Register (NQR) Code & Version (Will be issued after NSQC approval.)</td><td>NG-06-IT-045592025-V1-NASSCOM, v1.0</td><td>5. NCrF/NSQF Level: 6</td></tr>
<tr><td>6.</td><td>Brief Description of the Standalone NOS</td><td colspan="2">The Certified Information Security Manager (CISM) certification, offered by ISACA, is a globally recognized credential for information security professionals looking to enhance their skills in assessing risks, implementing effective governance, and proactively responding to incidents. It demonstrates expertise in information security governance, information security risk management, information security programs, and incident management, making it highly valued in roles that require information security.</td></tr>
<tr><td>7.</td><td>Eligibility Criteria for Entry for a 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>Relevant Experience (with Specialization - if applicable)</th></tr>
<tr><td>•</td><td>• Pursuing first year of 2-year PG after completing 3 year UG degree in relevant field
• Pursuing PG diploma after 3 year UG degree
• Pursuing final year of 4 year UG Hons.</td><td>5 years of relevant experience</td></tr>
</table></td></tr>
</table>

		• Completed 4 year UG Hons. With relevant experience	

b. Age <Please specify age only in case of any legal restrictions>: **18**

8.	**Credits Assigned to this NOS-Qualification, Subject to Assessment** *(as per National Credit Framework (NCrF))*	6	**9. Common Cost Norm Category (I/II/III)** *(wherever applicable)*: **II**
10.	**Any Licensing Requirements for Undertaking Training on This Qualification** *(wherever applicable)*	N/A	
11.	**Training Duration by Modes of Training Delivery** *(Specify **Total Duration** as per selected training delivery modes and as per requirement of the qualification)*		

Training Delivery Mode	Theory (Hours)	Practical (Hours)	Total (Hours)
Classroom (offline)	0	0	0
Online	16	160	176

☐ Offline Only ☐ ✓ Online Only ☐ Blended

(Refer Blended Learning Annexure for details)

<table>
<tr><td>12.</td><td>Assessment Criteria</td><td>
<table>
<tr><th>Theory (Marks)</th><th>Practical (Marks)</th><th>Project (Marks)</th><th>Viva (Marks)</th><th>Total (Marks)</th><th>Passing %age</th></tr>
<tr><td>400</td><td>400</td><td>-</td><td>-</td><td>800</td><td>56.25%</td></tr>
</table>
</td></tr>
<tr><td>13.</td><td>Is the NOS Amenable to Persons with Disability</td><td>☐ ✓ Yes ☐ No If “Yes”, specify applicable type of Disability:

The training and examination processes can accommodate individuals with motor disabilities. Special requests for additional assistance or adjustments can also be considered on a case-by-case basis to ensure accessibility and inclusivity.</td></tr>
<tr><td>14.</td><td>Progression Path After Attaining the Qualification, wherever applicable (Please show Professional and Academic progression)</td><td>N/A</td></tr>
<tr><td>15.</td><td>How participation of women will be encouraged?</td><td>N/A</td></tr>
<tr><td>16.</td><td>Other Indian languages in which the Qualification & Model Curriculum are being submitted</td><td>(Please provide assurance and plan for developing the qualification in other Indian Languages as per training requirement) N/A</td></tr>
<tr><td>17.</td><td>Is similar NOS available on NQR-if yes, justification for this qualification</td><td>☐✓ Yes ☐ No URLs of similar Qualifications:
https://www.nqr.gov.in/qualifications/3479

CISM is a more advanced qualification that requires significant professional experience and higher academic credentials. While this course focuses on managing information security infrastructure, CISM is more well-rounded and addresses a wider array of domains such as security governance, information security risk management, and incident management. It is designed to prepare candidates for relatively senior roles in the information security management space.</td></tr>
</table>

		https://www.nqr.gov.in/qualifications/11508 CISM is a more advanced qualification that requires significant professional experience and higher academic credentials. While this course focuses primarily on information security policy review, CISM is more well-rounded and addresses multiple domains in the information security space. It is designed to prepare candidates for relatively senior roles in the information security management space. https://www.nqr.gov.in/qualifications/11513 CISM is a more advanced qualification that requires significant professional experience and higher academic credentials. While this course focuses primarily on installing/configuring information security devices, CISM is more well-rounded and addresses multiple domains in the information security space. It is designed to prepare candidates for relatively senior roles in the information security management space.	
18.	**Name and Contact Details Submitting / Awarding Body SPOC** *(In case of CS or MS, provide details of both Lead AB & Supporting ABs)*	**Name:** Namrata Kapur **Email:** namrata@nasscom.in **Contact No.:** 9953951045 **Website:** https://www.sscnasscom.com/	
19.	**Final Approval Date by NSQC:07/10/2025**	**20. Validity Duration:** 3 years	**21. Next Review Date: 07/10/2028**

Section 2: Training Related

1.	**Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	To become an ISACA-accredited trainer, the trainer must pass the CISM exam and hold a CISM certification.
2.	**Master Trainer's Qualification and experience in the relevant sector (in years)** *(as per NCVET guidelines)*	NA
3.	**Tools and Equipment Required for the Training**	☐✓Yes ☐No *(If "Yes", details to be provided in Annexure)*
4.	**In Case of Revised NOS, details of Any Upskilling Required for Trainer**	**N/A**

Section 3: Assessment Related

1.	**Assessor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	Online assessment by NCVET approved Assessment Agencies so the assessor qualification & experience is relevant sector of IT-ITeS will be as per the guideline of NCVET or University.
2.	**Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines), (wherever applicable)*	N/A
3.	**Lead Assessor's/Proctor's Qualification and experience in relevant sector (in years)** *(as per NCVET guidelines)*	N/A
4.	**Assessment Mode** *(Specify the assessment mode)*	**Mode: ☐ ✓Online Only ☐ Offline Only ☐ Blended**
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 4: Evidence of the Need for the Standalone NOS

Provide Annexure/Supporting documents name.

1.	Government /Industry initiatives/ requirement (Yes/No): N/A
2.	Number of Industry validation provided: N/A
3.	Estimated number of people to be trained: 1500-2100 *(consolidated for next 3 years)*
4.	Evidence of Concurrence/Consultation with Line/State Departments (In case of regulated sectors): (Yes/No): N/A If "No", why:

Section 5: Annexure & Supporting Documents Check List

Specify Annexure Name / Supporting document file name

1.	**Annexure:** NCrF/NSQF level justification based on NCrF/NSQF descriptors *(Mandatory)*	✓
2.	**Annexure:** List of tools and equipment relevant for NOS *(Mandatory, except in case of online course)*	✓
3.	**Annexure:** Performance and Assessment Criteria *(Mandatory)*	✓
4.	**Annexure:** Assessment Strategy *(Mandatory)*	✓
5.	**Annexure:** Blended Learning *(Mandatory, in case selected Mode of delivery is Blended Learning)*	N/A
6.	**Annexure:** Acronym and Glossary *(Optional)*	
7.	**Annexure/Supporting Document:** Standalone NOS-Performance Criteria Details Annexure/Document with	✓

	PC-wise detailing as per NOS format (Mandatory- Public view)	
8.	**Supporting Document:** Model Curriculum *(Mandatory – Public view)*	✓

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	**Information Security Governance and Strategy**: Knowledge of information security strategy development, information governance frameworks, and legal/regulatory requirements. **Information Security Risk Management**: Knowledge of emerging risk landscape and techniques for risk assessment, response, and monitoring. **Information Security Program Development and Management**: Resources, asset classifications, and	• Advanced knowledge about a multidisciplinary/ interdisciplinary/ crossdisciplinary field of technology/ skills/ job role, with specialized in depth knowledge in one or more related fields. • Has awareness and knowledge of the emerging and futuristic developments and issues in the chosen fields of technology/ skills/ job role.	6

	frameworks for information security and knowledge about managing information security programs.		
Professional and Technical Skills/ Expertise/ Professional Knowledge	**Technical Competency for Information Security Governance:** Familiarity with developing, implementing, and maintaining security policies as well as creating organizational structures that support security initiatives. **Incident Management:** Expertise in developing and implementing risk response plans. **Technical Competency for Information Security Program Development**: Skills to identify security requirements and develop security programs.	● Possesses a range of advanced cognitive, professional, and technical skills required for performing and accomplishing complex tasks relating to the chosen fields of technology/ skills/ job role. ● Wide range of cognitive and practical skills required to create innovative and feasible solutions to complex problems and situations in uncertain environments. ● Skills to adapt to the future of work and to the demands of the fast pace of innovations and technological developments. ● Understanding and application of techno-commercial aspect of technology/associated skills or job role.	6
Employment Readiness & Entrepreneurship Skills & Mind-set/Professional Skill	**Global Recognition:** The certification is respected worldwide, opening doors	● Organizing, analyzing, interpreting and acting on the information and effectively communicating and	6

	to opportunities in diverse sectors. **Entrepreneurial Skills:** Candidates learn to assess IT systems for startups or businesses, providing consultancy services in information security management. **Adaptability:** The qualification ensures readiness for roles across finance, healthcare, government, and other sectors relying on IT systems. **Detail-Oriented Problem-Solving:** A systematic approach to identifying issues in IT controls and suggesting evidence-based solutions. **Ethics and Professionalism:** Adherence to ISACA's code of professional conduct ensures candidates maintain high standards of integrity and responsibility.	presenting/ using its outcome for decision making. ● A keen sense of observation, enquiry, and capability for asking relevant/ appropriate questions.	

Broad Learning Outcomes/Core Skill	**Core Information Security Management Knowledge:** Understanding of assessing risks, implementing effective governance, and responding to incidents. **Communication Skills:** Ability to present audit findings clearly and persuasively to stakeholders. **Analytical Thinking:** Skills to assess complex IT environments and suggest improvements.	● Applies advanced theoretical knowledge and specialized professional and technical skills involving complex variable environment and contexts. ● Evaluation and improvement of processes, procedures, and work or study activities. ● Examine and assess the implications and consequences of emerging developments and critical issues. ● Make judgments in a range of situations by critically reviewing and consolidating evidence and risks. ● Exercises judgment based on evaluation of evidence from a range of sources to arrive at solutions to complex real-life problems in chosen fields of technology/ skills/ job role.	6
Responsibility	**Safeguarding IT Assets:** Ensuring the confidentiality, integrity, and availability of information systems. **Strategic Alignment:** Aligning IT governance with business objectives to	● Responsible for managing activities like planning, resourcing, processes, people, within broad parameters and with complete accountability for determining, achieving, and evaluating personal and group outcomes.	6

	maximize organizational value. **Risk Mitigation:** Identifying and addressing IT-related risks proactively.	• Exercise full management and supervision of unpredictable work. • The exercise of full personal responsibility and accountability for the initiatives undertaken and the outputs/outcomes of own work as well as of the group as a team member/ leader.	

Annexure: Tools and Equipment (lab set-up)

List of Tools and Equipment

Batch Size:

S. No.	Tool / Equipment Name	Specification	Quantity for specified Batch size
1.	Computer	i3/i5 with 16GB Ram	one per learner
2.	Installed Browser	Modern Browser	installed on the computer
3.	Internet	Stable internet with at least 40 mbps speed	internet access for the learners

Classroom Aids

The aids required to conduct sessions in the classroom are:

1. N/A

Annexure: Industry Validations Summary

S. No	Organization Name	Representative Name	Designation	Contact Address	Contact Phone No	E-mail ID	LinkedIn Profile *(if available)*

Annexure: Training Details

Training Projections:

Year	Estimated Training # of Total Candidates	Estimated training # of Women	Estimated training # of People with Disability
2025	300-500	ISACA's will continue to meet its goal in India of putting forward offerings that work for all individuals. We will encourage the use of our CISA trainings at universities and other venues with a strong women's presence, to ensure that significant numbers of women will be able to obtain training.	N/A
2026	500-700	See above	N/A
2027	700-900	See above	N/A

Data to be provided year-wise for next 3 years.

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 NOS	List Recommended Tools – for all Selected Components	Offline: Online Ratio
1	☐Theory/ Lectures - Imparting theoretical and conceptual knowledge	NA	

2	☐Imparting Soft Skills, Life Skills and Employability Skills /Mentorship to Learners	NA	
3	☐Showing Practical Demonstrations to the learners	NA	
4	☐Imparting Practical Hands-on Skills/ Lab Work/ workshop/ shop floor training	NA	
5	☐Tutorials/ Assignments/ Drill/ Practice	NA	
6	☐Proctored Monitoring/ Assessment/ Evaluation/ Examinations	NA	
7	☐On the Job Training (OJT)/ Project Work Internship/ Candidate Training	NA	

Annexure: Standalone NOS- Performance Criteria details

1. Description:

The Certified Information Security Manager (CISM) certification, offered by ISACA, is a globally recognized credential for professionals with expertise in assessing risks, implementing effective governance, and proactively responding to incidents. CISM is a more advanced qualification that requires significant professional experience and higher academic credentials. It is designed to prepare candidates for relatively more senior roles in the information security audit space.

2. Scope:

The scope covers the following:

The CISM Exam covers 4 domains:

- Information Security Governance (17%)
- Information Security Risk Management (20%)
- Information Security Program (33%)
- Incident Management (30%)

3. Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC 1. Analyze, plan and develop information security strategies.

PC 2. Analyze and identify potential information security risks, threats and vulnerabilities to perform at management level.

PC 3. Manage information security programs, including security control, testing, comms and reporting and implementation.

PC 4. Prepare a business to respond to incidents and guide recovery.

4. **Knowledge and Understanding (KU):**

The individual on the job needs to know and understand:

KU1. Culture, regulations and structure involved in enterprise governance.

KU2. Information about identifying and countering information security risks

KU3. Resources, asset classifications and frameworks for information security.

KU4. Tools, evaluation and containment methods for incident management.

5. Generic Skills (GS):

User/individual on the job needs to know how to:

GS1. English language reading and writing

GS2. Advanced computer knowledge

GS3. Communication skills

GS4. Collaboration skills

GS5. Problem analysis

GS6. Problem solving skills

Annexure: Assessment Criteria

Detailed PC-wise assessment criteria and assessment marks for the NOS are as follows:

S. No.	Assessment Criteria for Performance Criteria	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC 1.	Analyze, plan and develop information security strategies. (17%)	68	68		
PC 2.	Analyze and identify potential information security risks, threats and vulnerabilities to perform at (20%)	80	80		
PC 3.	Manage information security programs, including security control, testing, comms and reporting and implementation. (33%)	132	132		
PC 4.	Prepare a business to respond to incidents and guide recovery. (30%)	120	120		
Total Marks		**400**	**400**		

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.

1. Assessment System Overview:

.

Exam Duration:

Exam Fees: Exam registration fees are based on membership status at the time of exam registration.

Exam Structure:

Exam Format

For Testing Centers

2. Testing Environment:

3. Assessment Quality Assurance levels/Framework:

4. Types of evidence or evidence-gathering protocol:

5. Method of verification or validation:

6. Method for assessment documentation, archiving, and access

Annexure: Acronym and Glossary

Acronym

Acronym	Description
AA	Assessment Agency
AB	Awarding Body
NCrF	National Credit Framework
NOS	National Occupational Standard(s)
NQR	National Qualification Register
NSQF	National Skills Qualifications Framework

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.