QUALIFICATION FILE

Application Documentation: Version 1 /01 September, 2016

NSDA Reference
To be added by NSDA

CONTACT DETAILS OF SUBMITTING BODY

Name and address of submitting body:

C-DAC, ACTS

ACTS, Innovation Park, S. No. 34/B/1,

Panchvati, Pashan, Pune 411 008

Name and contact details of individual dealing with the submission

Name: Shri. Aditya Kumar Sinha

Position in the organisation: Joint Director

Tel number(s): 020-25503155

E-mail address: saditya@cdac.in

List of documents submitted in support of the Qualifications File

1. Qualification File
2. Course Content

QUALIFICATION FILE

SUMMARY

Qualification Title and Code:	Certificate Course in Ethical Hacking and Information Security (CCEHIS)
Body/bodies which will award the qualification:	Centre for Development of Advanced Computing (C-DAC) organization of the Ministry of Electronics and Information Technology (MeitY), Ministry of Communications & Information Technology
Body which will accredit providers to offer the qualification:	C-DAC
Body/bodies which will be responsible for assessment:	C-DAC
Occupation(s) to which the qualification gives access:	The Certificate Course in Ethical Hacking and Information Security (CCEHIS). This course is aimed to provide skills on security programming which will help the students who want to make carrier in security domain as well as prepare them to keep pace with the changing face of technology and the requirements of the growing IT industry. After the completion of the course, students can work in area of Application Security or Ethical Hacking.
Proposed level of the qualification in the NSQF:	Level 7
Anticipated volume of training/learning required to complete the qualification:	320 hrs of classroom/lab learning (4 Months, 4 hrs 5 days in a week)
Entry requirements / recommendations:	Any Engineering /Science graduate with mathematics up to 10+2 level
Progression from the qualification:	The Certificate Course in Ethical Hacking and Information Security (CCEHIS). This course is aimed to provide skills on security programming which will help the students who want to make carrier in security domain as well as prepare them to keep pace with the changing face of technology and the requirements of the growing IT industry. These candidates will be trained in Application Security, Ethical Hacking and Management skills. After the completion of the course, students can work in area of Application Security or Ethical Hacking. Candidate can start from level 7 and lead to further levels.
Planned arrangements for RPL:	NA

QUALIFICATION FILE

International comparability where known:	There are many courses available on Application Security, Ethical Hacking but CDAC providing knowledge of management development program.

Formal structure of the qualification:

Title of NOS/unit or other component (include any identification code used)	**Mandatory/ Optional** Enter M or O for each unit/ component	**Estimated size (learning hours)** The total should be the same as the entry under "anticipated volume" above	**Level** In the NSQF, individual units or components of qualifications can have outcomes which put them at levels which are higher or lower than the whole qualification.
Java Programming with Crypto API	M	80	7
Application Security	M	70	7
Ethical Hacking	M	70	7
Management Development Program	M	60	7
Project	M	40	7

Please attach any document giving further detail about the structure of the qualification – eg a Curriculum or Qualification Pack.
Give details of the document here:

SECTION 1

ASSESSMENT

Body/Bodies which will carry out assessment:
C-DAC's Exam, Evaluation and Certification department will carry out assessment as per evaluation guideline finalized by Academic Council/ Academic Management Committee.

Will the assessment body be responsible for RPL assessment?

- Same will be finalised when the national RPL Policy will be finalised.
- Assessment is online through our E-Pariksha system or manually (OMR Based), depending on the strength of students.
- Issuance of qualification is centralized through C-DAC.

Describe the overall assessment strategy and specific arrangements which have been put in place to ensure that assessment is always valid, consistent and fair and show that these are in line with the requirements of the NSQF:

Assessment is a necessary and essential part of conducting the Certificate Course in Ethical Hacking

and Information Security (CCEHIS), as it provides important feedback and inputs to both the institute as well as the student. The institute gets an idea about the relative performance of each student, which also serves as feedback about the design and conduct of the course. The student gets a clear picture of his academic standing, individually and in comparison to his fellow students.

- A combined evaluation process is to be conducted for the course.
- The evaluation for each module must be completed as per guidelines given below. The mid-module /surprise test evaluation is mandatory and can be taken after discussion with the concerned faculty.
- Students are evaluated on a continuous and throughout the duration of the course to make a fair assessment of the skills acquired by them. To have a very uniform and fair assessment. The evaluation process is divided into two parts:
    - Continuous Assessment - CA (150 marks)
    - Course End Examination - CCE (150 marks)

Continuous Assessment :This is being done primarily by the respective faculty in the form of Lab tests, assignments, quizzes, submission of term reports, presentations etc. conducted (with the help of respective course co-coordinators) at regular intervals and as and when the portions of the subjects are completed. These are basically internal exams and local to the centre. This process is further categorized into two parts.

- Lab test
- Internal test : Assignment/Case Studies /quiz and other valuation methods like case study, viva, group discussion depending on the subject and the faculty

It is recommended to conduct Management Development Program and Organisational Behaviour sessions and also conduct surprise test for the development of soft skills, logical, analytical capabilities and managerial skills for the benefit of the students and also give assignments and conduct some surprise test related to Management Development Program and Organisational Behaviour.

The figures shown below indicate the weightage of each module in the final performance statement. The examination(s) for each module must be conducted for at least that number of marks. However, the centre may conduct evaluation for a higher number of marks, in which case the marks will be scaled down. For example, if the examination for the Operating Systems Concepts module is conducted for 100 marks, the marks earned by the student will be scaled down to out of 40.

A student must score a minimum of 40 percent marks in each component of the evaluation, and also in the aggregate score, in order to successfully clear the module. If a student scores more than 40% on aggregate but has scored less than 40% in one component of the evaluation, he will not be declared as passed.

The weight age for each component will normally be:

Theory examination – (CCEE)	150 marks
Laboratory examination, Internal marks	150 marks

(Internal marks: Lab Assignment Evaluation, Surprise Tests, attendance, Viva, Seminars)

The question papers for the theory as well as the laboratory examinations at all the centres will be set by C-DAC, ACTS, Pune. The centres according to guidelines provided by, ACTS, Pune, will conduct the evaluation of the laboratory and assignments locally.

Minimum Pass marks:

The minimum marks to be obtained for declaring a student pass in any module is as follows:

QUALIFICATION FILE

For 40 mark QP : 16 marks

For 20 mark QP : 8 marks

For 60 mark QP : 24 marks

Assessment is through E-Pariksha system.

About E-Priksha System:
ePariksha is a web based application for the automation of the examination process. The system provides a great control on exams from preparing question paper to scheduling exam and from monitoring exam to generate results.

ePariksha has a strong administration which provides complete system status in one glance.

It's Results & Reports generations functionality provides system details in all standard and required formats.

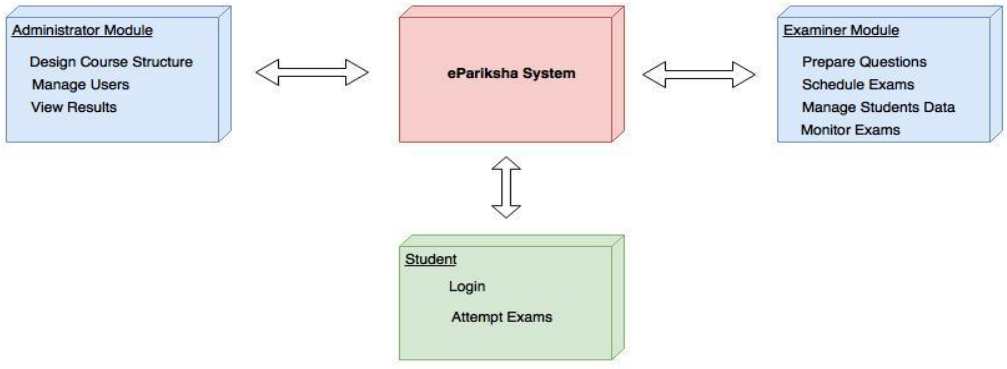
An image based, LAN based, secure, fault tolerant and scalable system through which examinations can be delivered "on demand" basis in selected examination centres spread across the country.

System Support:

- Decentralized mode of operation(LAN based)
- Question Paper approach
- Multi lingual and multi subject support
- Browser based

Components of the E-Parikhsa System Includes:

- **Administration Module**- To design course structure,Manage users,view results.
- **ePariksha System** –Assessment of students through online system.
- **Examiner Module** -To manage the examination related activity and conduct- i.e Registration data and question paper uploading, conduct of examination, response generation
- **Student Login** –Allows students to login and attempt exams.



Salient Features:

- Exam Resume - Power Failure Handling
- Random Question Paper
- User friendly Interface
- Question Bank
- Instant Result

QUALIFICATION FILE

- Live Monitoring of Exams & Assignment
- Time bound exams
- Multilingual support
- Handheld devices Support
- Responsive Design

Feedback System: C-DAC**'s** Advanced Computing Training School (ACTS) offers various courses and training programs through its own training centres and its network of Affiliated Training Centres (ATC) spread across the country. Each year, thousands of students and professionals are trained at these centres.

The purpose of the system i.e. Online Feedback System (OFS) is to develop a web application for getting the online faculty feedback by the students studying at centres and also at the various Authorized Training Centres (ATC) affiliated to for different training programs offered by C-DAC ACTS.

This system is for conducting "The Student Survey" for quality assurance of education. Students, Faculties and administrators can all benefit from survey. This is helpful in the continual improvements in teaching programs, processes as well as infrastructure and thereby enhancing the students' learning experience at C-DAC ACTS.

The Online Feedback System make the student feedback procedure centralized for all C-DAC centres as well as various Authorized Training Centres (ATCs) located across the country through which headquarter manager can manage student feedback of faculties as well as infrastructure studying at different training centres with different reports for feedback analysis.

Please attach any documents giving further information about assessment and/or RPL.
Give details of the document(s) here:

QUALIFICATION FILE

ASSESSMENT EVIDENCE

Each module should be evaluated as per the weightage there will be 150 questions to answer in 3 hours duration in Course End Exam as per the following distribution mentioned below given below.

Sr. No.	Module	Learning Outcome	Theory	Lab & IA	Total Marks
1	Java Programming with Crypto API	• Students will be able to write code in java related with security and cryptography. • They will be writing security protocols and will understanding SSL and TLS protocols.	40	50	**90**
2	Application Security	• Students will be given practical knowledge on MySQL database and also explore the security risk and threat. • They will also learn Python language which will help them to write scripting.	40	50	**90**
3	Ethical Hacking	• Students will understand principles of security management concepts. • Protection of information security. • Ethical Tacking. • Various attacks.	40	50	**90**
4	Management Development Program	• Students will get trained on conversation skills as well as problem solving skills.	30	-	**30**
5	Project	• Think critically, creatively and analytically in developing technological solutions to simple and complex problems.	Grade		
		Total	**150**	**150**	**300**

Complete a grid for each grouping of NOS, assessment unit or other component as listed in the entry on the structure of the qualification on page 1.

QUALIFICATION FILE

Title of NOS/Unit/Component:

Assessable outcomes	Assessment criteria for the outcome
Enter the learning outcomes /elements of competence which will be assessed.	List all the criteria applying to this element/outcome.
All the modules of Certificate Course in Ethical Hacking and Information Security (CCEHIS)	**A+ >= 85%,** **A >= 70% to < 85%** **B >= 60% to < 70 %** **C >= 50% to < 60%** **D >= 40% to < 50%** **F < 40%**

Means of assessment 1

Theory portion Assessment will be done through LAN based online system or paper mode. Paper will be Objective question based. Lab exam will be done separately as per evaluation Guidelines.

Means of assessment 2

Re-examinations:

The following conditions will be applicable for the course end re-exam:

- Students who do not appear for an exam on the scheduled date will not have an automatic right to re-examination. Only those students who, in the opinion of the centre/course coordinator have a genuine reason for being absent may be allowed to appear for a re-exam.
- Students who have failed an exam may be allowed to appear for a re-exam.
- The re-exam should be conducted following the same process as the regular examination.
- Students, who failed/remained absent in the Course End Examination conducted by , shall be allowed to appear in the re-examination only once.
- Students who remain absent or fail in the re-examination will not get any further chance for appearing for the re-examination. In such case the candidate can receive the Performance Statement and the certificate of participation without any grade.
- On evaluation of their answer sheets 20% of the marks obtained by the students will be deducted (towards de-rating for re-examination) for arriving at the final score, i.e. in order to clear the module test the student has to score a minimum of 48% marks instead of 40%.
- There will be no re-exam for the re-exam

Pass/Fail:

If Candidate scored below 40% in any of the component like Theory, lab or Internal will be consider as FAIL.

QUALIFICATION FILE

SECTION 2

SUMMARY EVIDENCE OF LEVEL

Level	Process Required	Professional Knowledge	Professional Skill	Core Skill	Responsibility
7	**Requires a command of wide-ranging specialised theoretical and practical skills, involving variable routine and non-routine contexts.**	**Wide-ranging factual and theoretical knowledge in broad contexts within a field of work or study.**	**Wide range of cognitive and practical skills required to generate solutions to specific problems in a field of work of study.**	**Good logical and mathematical skill understanding of social political and natural environment and organising information, communication and presentation skill.**	**Full responsibility for output of group and development**

Assessed outcome	Process Required	Professional Knowledge	Professional Skill	Core Skill	Responsibility
1. Java Programming with Crypto API 2. Application Security 3. Ethical Hacking 4. Management Development Program 5. Project	Person may carry out a job as Application Security Analyst, Application Security Manage, Hacker and Penetration Tester. This job demands a command of wide-ranging specialised theoretical and practical skills, involving variable routine and non-routine contexts.	•Java Code related with security and cryptography. •Security protocols and SSL and TLS. •MySQL database and also explore the security risk and threat. •Python language for scripting. •Principles of security management concepts. •Protection of information security. •Ethical Tacking. •Various attacks.	• Candidate can be Application Security Analyst, Application Security Manage, Hacker and Penetration Tester. • Candidates as System Analyst examines the system requirements and implement and configure and test feasible.	Candidate will be learning management Development Program and Organisational behaviour to communicate written and oral. Aptitude, basic understanding of social political and natural environment with good analytical and managerial skills	Candidate can perform well and responsible for output of group and development

QUALIFICATION FILE

SECTION 3

EVIDENCE OF NEED

What evidence is there that the qualification is needed?

Set up the Advanced Computing Training School (ACTS) in 1993 to meet the ever-increasing skilled manpower requirements of the Information Communication Technologies (ICT) industry as well as supplement its intellectual resource base for cutting-edge research and development. Over the years has designed and delivered various postgraduate and undergraduate degree and diploma programmes. In addition, imparts ICT training to state and national governments and agencies, strategic sectors, corporate and industries, foreign countries and international students, based on specific requirements.

What is the estimated uptake of this qualification and what is the basis of this estimate?

The application security market size is estimated to grow from USD 2.24 Billion in 2016 to USD 6.77 Billion by 2021, at a Compound Annual Growth Rate (CAGR) of 24.8% from 2016 to 2021. Application security protects web- and mobile-based applications from vulnerabilities via various security testing procedures, throughout the application development lifecycle.
(http://www.marketsandmarkets.com/Market-Reports/application-security-market-110170194.html)

If there was ever a time to get into the IT security field, it's now: The Bureau of Labor Statistics expects the sector to grow 37 percent by 2022, and according to a survey by the Ponemon Institute, demand for talent so outweighs supply that 40 percent of IT security positions are expected to go unfulfilled in 2014. The pay isn't bad, either: the average information security analyst in the U.S. makes over $90,000per year.
(http://intelligent-defense.softwareadvice.com/how-to-get-an-ethical-hacker-job-0714/)

What steps were taken to ensure that the qualification(s) does/do not duplicate already existing or planned qualifications in the NSQF?

NA

What arrangements are in place to monitor and review the qualification(s)? What data will be used and at what point will the qualification(s) be revised or updated?

Set up the Advanced Computing Training School (ACTS) in 1993 to meet the ever-increasing skilled manpower requirements of the Information Communication Technologies (ICT) industry as well as supplement its intellectual resource base for cutting-edge research and development. Over the years has designed and delivered various postgraduate and undergraduate degree and diploma programmes. In addition, imparts ICT training to state and national governments and agencies, strategic sectors, corporate and industries, foreign countries and international students, based on specific requirements.

The Education and Training activities of are governed and steered by Academic Council (AC) and Academic Management Committee (AMC). As per the Academic Council minutes and direction, a syllabus updation subcommittee is formed by combining members from different centres. The sub-committee gave their inputs for syllabus updation. The resource centre has conducted meetings for updating required modifications in the current syllabus of PG-Diploma. After that, minutes of the meeting with draft syllabus contents were circulated across all the participating centres for any suggestion and comments. If any suggestions come through discussion of all concerned members, we incorporate the same and circulate again for finalization. After that we make the source book and informed to all centres for their review.

SECTION 4

EVIDENCE OF RECOGNITION AND PROGRESSION

What steps have been taken in the design of this or other qualifications to ensure that there is a clear path

QUALIFICATION FILE

to other qualifications in this sector?

- This qualification has been designed in consultation with industry and domain expert keeping in mind today's need. Evaluation criteria have been added to ensure progression to related path ways identified as per career path.

Please attach any documents giving further information about any of the topics above.
Give details of the document(s) here:

1. Course Content

Certificate Courses in Ethical Hacking and Information Security

Sl. No.	Modules	Hours
1	Java Programming with Crypto API	80
2	Application Security	70
3	Ethical Hacking	70
4	Management Development Program	60
5	Project	40
	Total	**320**

Eligibility: Any Engineering /Science graduate with mathematics up to 10+2 level

Course Prerequisite: Candidate should have knowledge of computer & networking fundamentals and Basic Computer Programming with OOPs concepts.

Course Focus: This course is aimed to provide skills on security programming which will help the students who want to make carrier in security domain.

Detailed Syllabus

Java Programming with Crypto API

- Introduction to Java
- Java Overview, Data types, Arrays, Decision statements, Loops
- Classes, Package
- java.lang, java.util
- Java Interfaces
- Exception Handling
- Networking with Java
- JSP & Servlets
- Cryptography
- Java Cryptography Architecture
- Java Cryptography Extension
- SSL and TLS protocols
- A Basic of SSL client and Server
- Client side Authentication
- Managing SSL Session Information
- Dealing with HTTPS

Application Security

- MySQL
- Introduction to MySQL
- Installing and Configuring MySQL
- Creating and Dropping Database

QUALIFICATION FILE

- Queries in MySQL
- Overview of Regular Expression
- Web Application Security
- Web application Security Risks
- Identifying the Application Security Risks
- Threat Risk Modelling
- OWASP Top 10
- Secure Coding with Java
- Fundamentals
- Denial of Service
- Injection and Inclusion
- Buffer Overflows and Input Validation
- Access Control
- Python
- Introduction to Python
- Python Objects
- Strings
- Numbers
- Lists
- Sorting
- Dictionaries and Files
- Sockets with Python

Ethical Hacking

- Basics of Information System
- The changing nature of Information System
- Threats of Information System
- Threats and attacks
- Classification of Threads and attacks
- Protecting Information System Security
- Security in mobile and Wireless Computing
- Credit Card frauds in mobile and wireless Computing
- Security Policies and Measures in Mobile Computing
- Information Security Management
- Security Policy, Standards
- Responsibility for Information Security Management
- Building Blocks of Information Security
- Basic principal of Information Systems Security
- Information Security risk analysis
- Term and Definitions for Risk Analysis of Information Security
- Risk Management and Risk Analysis
- Data Privacy Fundamentals
- The Business Aspects of Penetration Testing
- The Technical Foundations of Hacking
- Foot printing and scanning
- Enumeration and Step-by-Step System Hacking
- Linux and Automated Security Assessment Tools
- Trojans and Backdoors
- Sniffers, session Hijacking and Denial of Service
- Web Server Hacking, Web application Vulnerabilities and Database Attacks
- Wireless Technologies, Security and Attacks
- IDS, Honeypots and Firewalls

QUALIFICATION FILE

- Cryptographic Attacks and Defenses
- Social Engineering and Physical Security
- Overview of Malware Reverse Engineering

Malware Reverse Engineering

- Types of Malware
- Malicious code Families
- Latest Trends in Malware
- Analysis of Malware

Management Development Program

Introduction to communication, Barriers to communication, Kind of communication, Confidence building Non-verbal Communication, Fluency and vocabulary, Synonyms, Antonyms, Grammar, Noun Pronoun, Verb, Adjective, Preposition, Conjunction, Words of Idioms & phrases, Sentence Construction, Fill up the blanks, Pronunciation, Conversation practice, Polite Conversation, Greeting, Logical reasoning, General Aptitude, Writing: Covering letter, Resume, Email, Presentation Skill, group discussion, Interview skills, Mock interview

Project