An

Audit Course Report

on

Cyber Security

Submitted to

Department of Computer Engineering

PDEA's Collage of Engineering Manjari BK

Pune -412307

Submitted By

Aniket Bhausaheb Khedkar

TE Comp **Roll no:- 66**

Exam seat no.

CERTIFICATE

This is to certify that the below mentioned third year engineering students have carried out the necessary Audit course report on "Cyber Security" in the department of Computer Engineering.

PDEA's College of Engineering, Manjari BK, Pune 412307. They have completed this Audit course report under my guidance in satisfactory manner in October 2019 of third year engineering.

Aniket Bhausaheb Khedkar TE Comp Roll No:- 66

Computer Engineering students have successfully completed an Audit course report on "Cyber Security" towards The fulfillment of their Degree in Computer Engineering in academic year 2022 -2023 .

The Performance of each of these students during the courses was very good.

Date:

Guide	HOD Computer Dept.	Principal
Prof. S.V.Phulari	Dr. R.V.Patil	Dr. R.V.Patil

ACKNOWLEDGEMENT

Apart from the efforts of all the team members, the selection of this Audit course report topic depends largely on encouragement and guidance of our teachers. We take this opportunity to express our gratitude to the teachers who have been instrumental in the approval of this project topic. We would like to show our greatest appreciation to teachers and other staff members.

We can't think them enough for their tremendous supports and help. They motivated and encouraged us very time while selecting the proper Audit course report topic. Without their encouragement and guidance we would not have been able to select the proper topic.The contribution and support received from all the team members including **Aniket Bhausaheb Khedkar** is vital. The team spirit shown by all has made our Audit course report successful.

TE COMP

Roll No:- 66

ABSTRACT

Human error is the leading cause of data breaches, so you need to equip staff with the knowledge to deal with the threats they face.
Training courses will show staff how security threats affect them and help them apply best-practice advice to real-world situations. Web application vulnerabilities are a common point of intrusion for cyber criminals.
As applications play an increasingly critical role in business, it is vital to focus on web application security. Network security is the process of protecting the usability and integrity of your network and data. This is achieved by conducting a network penetration test, which scans your network for vulnerabilities and security issues. Leadership commitment is the key to cyber resilience. Without it, it is very difficult to establish or enforce effective processes. Top management must be prepared to invest in appropriate cyber security resources, such as awareness training.

Cyber attacks cost organizations billions of pounds and can cause serious damage. Impacted organizations stand to lose sensitive data, and face fines and reputational damage. IT Governance has a wealth of security experience. For more than 15 years, we've helped hundreds of organizations with our deep industry expertise and pragmatic approach.

Contents

Preface

Over the course of just a few years, cyber security has grown into one of the most significant risk management challenges facing virtually every type of organization. Is the internal audit function keeping pace with this rapidly changing area of risk? This report examines this question and, based on a survey of internal audit and cyber security professionals, offers some observations on how internal audit departments are adapting in order to address cyber security risks.

A decade ago, the internal audit function evolved and adapted to the increasingly important role that information technology (IT) was playing in all aspects of business operations. Today, internal audit faces the need to adapt once again to address the critical risks associated with cyber security.

Recognizing this need, the Internal Audit Foundation and Crowe, in collaboration with The Institute of Internal Auditors' (IIA's) Audit Executive Center, conducted a limited survey of IIA members in order to understand how internal audit has begun to adapt to this new risk landscape.

This report offers a summary of key findings from that research and provides insights into some current internal audit and cyber security policies and practices. In addition, the report's authors draw on industry experience and observation based on their working relationships with internal audit functions across a broad range of industries.