Government of Pakistan

National Vocational and Technical Training Commission

Prime Minister Youth Skills Development Program

"Skills for All"

Course Contents / Lesson Plan
Course Title: Cyber Security for Financial Institutions
Duration: 1 Month

Trainer Name	
Author Name	• **Khwaja Mansoor-ul-Hassan, Assistant Professor Cyber Security Department Air University Islamabad** • **Abdul Basit Shahid, Assistant Manager Security Operation Center, Habib Bank Limited (HBL)** • **Malik Maaz Mehboob, Sr. Consultant Cyber Security at Corvit Systems Pvt. Ltd.** • **Muhammad Nasir Khan, Ex-DD(VT),SS & C Wing, NAVTTC**
Course Title	**Cyber Security for Financial Institutions**
Objectives and Expectations	**Employable skills and hands-on practice in Cyber Security for Financial Institutions** **Objective:** The objective of the Cybersecurity for Financial Institutions course is to equip participants with the knowledge and practical skills necessary to protect financial institutions from cyber threats. This course covers the implementation of advanced cybersecurity measures, including network security, vulnerability assessments, penetration testing, ISMS and PCI-DSS compliance, incident response, and the protection of electronic payment systems. By the end of the course, participants will be proficient in securing financial networks, safeguarding sensitive data, and mitigating evolving cybersecurity risks within the financial ecosystem. **Expectations:** **By the end of this course, participants are expected to:** **i.** **Demonstrate Proficiency in Financial Cybersecurity:** Participants will be able to explain the role of cybersecurity in the financial ecosystem, identify key threats, and propose solutions to enhance the security of financial institutions. **ii.** **Apply Enterprise Network Security Concepts:** Participants will understand firewall architectures, intrusion detection systems, and honeypots and apply these concepts to secure financial networks. **iii.** **Conduct Vulnerability Assessments and Penetration Testing:** Participants will be skilled in performing reconnaissance, scanning, enumeration, and system hacking techniques as part of penetration testing exercises and will generate vulnerability assessment reports for financial institutions. **iv.** **Implement ISMS and PCIDSS Compliance:** Participants will be able to design, implement, and monitor Information Security Management Systems based on ISO/IEC 27001 standards, ensuring compliance with financial regulations like PCIDSS. **v.** **Manage Incident Response:** Participants will be capable of developing and executing comprehensive incident response plans,

	including containment, eradication, and recovery from cybersecurity incidents in financial institutions. **vi. Mitigate Emerging Threats:** Participants will be equipped to identify and respond to emerging cybersecurity threats specific to financial institutions, using advanced mitigation strategies. **vii. Adopt Ethical Cybersecurity Practices:** Participants will follow ethical guidelines in their cybersecurity work, making informed decisions that uphold professional standards and promote public trust in financial systems. **Employable Skills:** **i. Cybersecurity Strategy:** Develop security strategies for financial institutions. **ii. Network Security:** Configure/manage firewalls, IDS, and honeypots. **iii. Penetration Testing:** Conduct penetration tests and vulnerability assessments. **iv. ISMS Compliance:** Implement ISMS (ISO/IEC 27001). **v. PCIDSS Compliance:** Secure payment systems and ensure compliance. **vi. Incident Response:** Develop and execute incident response plans. **vii. E-Payment Security:** Secure online banking and e-payment systems. **Hands-on Practice:** **i. Firewall Configuration:** Set up and configure firewalls and honeypot integration. **ii. Intrusion Detection:** Use tools like Snort to detect and respond to network intrusions. **iii. Penetration Testing:** Perform vulnerability assessments, network scanning, enumeration, and system hacking using ethical hacking techniques. **iv. E-Payment Security:** Secure electronic banking platforms and simulate attacks on e-payment systems. **v. ISMS Implementation:** Draft ISMS policies and implement ISO/IEC 27001 security controls for a simulated financial organization. **vi. PCI-DSS Auditing:** Conduct a mock audit to ensure compliance with Payment Card Industry Data Security Standards.
Entry-level of trainees	Course of Cyber Security for Financial Institutions proposed entry level is minimum bachelors/FSC/ICS/ IT diploma holder in relevant subject, so expectations from the trainees are: • Basic understanding of IT and computer networks. • Familiarity with computer systems and operating systems. • No prior knowledge of Electronic Banking

Learning Outcomes of the course	**The content of this lesson plan is adopted from the internationally recognized PECB certification course, " ISO/IEC 27001 Lead Implementer" ensuring alignment with global standards and practices. For further reference, the link to the source material is provided below:** **Understanding Financial Cybersecurity:** • Participants will be able to describe the financial ecosystem, identify the role of fintech companies, and articulate the importance of cybersecurity in maintaining the confidentiality, integrity, and availability of financial data. **Network Security Management:** • Participants will demonstrate proficiency in configuring and managing firewalls, intrusion detection systems (IDS), and honeypots, and will be able to implement effective security measures for enterprise networks. **Penetration Testing and Vulnerability Assessment:** • Participants will be skilled in performing footprinting, network scanning, enumeration, and system hacking, and will be able to identify vulnerabilities and recommend appropriate remediation strategies. **ISMS Implementation:** • Participants will be able to design, implement, and monitor an Information Security Management System (ISMS) in accordance with ISO/IEC 27001 standards, including risk assessment, policy development, and compliance monitoring. **PCI-DSS Compliance:** • Participants will understand and apply the requirements of the Payment Card Industry Data Security Standard (PCIDSS) to protect cardholder data and ensure secure payment processes. **Incident Response and Management:** • Participants will develop and execute comprehensive incident response plans, including preparation, detection, analysis, response, and recovery, based on NIST SP 800-61 guidelines. **E-Payment and Online Banking Security:** • Participants will be able to secure electronic payment mechanisms and online banking systems, addressing potential threats and implementing protective measures. **Emerging Threats and Mitigation:** • Participants will identify and respond to emerging cybersecurity threats, including malware, ransomware, and social engineering attacks, and will apply mitigation strategies to protect financial institutions. **Ethical and Professional Conduct:** • Participants will understand and apply ethical principles and professional conduct in cybersecurity, ensuring adherence to industry standards and fostering trust in financial systems.
Course Execution Plan	The total duration of the course: **1 months (4 Weeks)** Class hours: **4 hours per day** Theory: **40%** Practical: **60%** Weekly hours: **(8 Hrs Theory) + (12 Hrs Lab) = 20 hours per week** Total contact hours: **80 hours**

Companies offering jobs in the respective trade	**Microfinance Banks, including but not limited to:** • FINCA Microfinance Bank Ltd. • HBL Microfinance Bank. • Telenor Microfinance Bank Ltd. • Mobilink Microfinance Bank Ltd. • U Microfinance Bank Ltd. • APNA Microfinance Bank Ltd. **Commercial / Private Banks, including but not limited to:** • Habib Bank Limited • Meezan Bank Ltd. • Faysal Bank Ltd. • Askari Bank Ltd. • Standard Charted Bank (Pakistan) Ltd. • RAAST by State Bank of Pakistan • 1LINK Limited
Job Opportunities	• Cybersecurity Analyst • Network Security Engineer • Penetration Tester (Ethical Hacker) • Information Security Manager • Compliance Analyst • Incident Response Specialist • Cyber Risk Consultant • E-Payment Security Specialist • Vulnerability Assessor • Regulatory Compliance Officer
No of Students	25
Learning Place	Classroom / Computer Lab
Instructional Resources	**Online Courses and Tutorials:** 1. Payment Card Industry Data Security Standard PCI-DSS: https://www.cybrary.it/course/pcidss 2. ISO/IEC 27001 Lead Auditor: https://www.skillfront.com/ISO-IEC-27001-Information-Security-Associate 3. Ethical Hacking Essentials – EC Council: https://www.eccouncil.org/train-certify/ethical-hacking-essentials-ehe/ 4. Network Defense Essentials – EC Council: https://www.eccouncil.org/train-certify/network-defense-essentials-nde/ 5. Incident Response Lifecycle Course: https://www.cybrary.it/course/incident-response-lifecycle **Books and References:** 1. Cryptography and Network Security (William Stallings): https://www.amazon.com/Cryptography-Network-Security-Principles-Practice/dp/0133354695 2. Ethical Hacking and Defense (EC-Council): https://store.eccouncil.org/product/cehv12-courseware/ 3. PCI DSS: A Practical Guide to implementing and maintaining compliance, Third Edition (Steve Wright):

https://www.amazon.com/Pro-Android-Kotlin-Developing-Jetpack/dp/1484287444

4. ISO 27001 controls – A guide to implementing and auditing (Bridget Kenyon): https://www.oreilly.com/library/view/iso-27001-controls/9781787781467/
5. ACM Code of Ethics and Professional Conduct (ACM): https://www.acm.org/binaries/content/assets/about/acm-code-of-ethics-booklet.pdf

Practice and Experimentation:

1. Oracle Virtual Box: https://www.virtualbox.org/
2. Kali Linux Operating System: https://github.com/index
3. The Social-Engineer Toolkit (SET): https://github.com/trustedsec/social-engineer-toolkit
4. Snort IPS: https://www.snort.org/
5. Nmap The Network Mapper: https://nmap.org/
6. Nessus Vulnerability Scanner: https://www.tenable.com/products/nessus
7. The ISO27k Toolkit: https://www.iso27001security.com/html/toolkit.html
8. Nessus Vulnerability Scanner: https://www.tenable.com/products/nessus
9. Virus Total: https://www.virustotal.com/gui/home/upload
10. Any. Run – Interactive Online Malware Sandbox: https://any.run/

MODULES

Scheduled Weeks	Module Title	Days	Learning Units	Home Assignment
Week 1	**Introduction to Cybersecurity in Financial Institutions and Enterprise Network Security**	**Day 1**	**Understanding Cybersecurity in the Financial Ecosystem** • Describe the financial ecosystem. • Analyze the role of fintech companies within the ecosystem. • Explain the fundamentals of cybersecurity. • Evaluate the importance of cybersecurity in fintech. • Assess the importance of cybersecurity in maintaining the CIA (Confidentiality, Integrity, Availability) of the financial ecosystem. • Examine the impact of cyber threats on financial stability and trust. • Discuss case studies of cyberattacks on financial institutions.	**Task#1**

		Day 2	**Explore Electronic Banking** • Outline the E-Payment Mechanism. • Describe payment through the card system. • Compare E-Cheque and E-Cash. • Identify E-Payment threats and protections. • Explore E-Marketing, including home shopping. • Examine E-Marketing strategies. • Analyze Tele-Marketing practices.	
		Day 3	**Secure Enterprise Network with Firewalls** • Understand Firewall Architecture. • Explain the concept of the Demilitarized Zone (DMZ). • Differentiate between types of firewalls. • Explore honeypots and their types.	
		Day 4	**Secure Enterprise Network with Firewalls** • Describe IDS (Intrusion Detection System) and IPS (Intrusion Prevention System). • Examine Intrusion Detection/Prevention tools. • Analyze IDS/IPS and their rules. • Evaluate firewalls for mobile security.	

		Day 5	**Secure Enterprise Network with Firewalls** • Identify methods for evading firewalls. • Propose IDS/Firewall evasion counter-measures. • Configure a honeypot on an operating system.	
Week 2	**Vulnerability Assessment and Penetration Testing**	**Day 1**	**Analyze Footprinting and Reconnaissance** • Define Footprinting Concepts. • Apply Footprinting Methodology. • Utilize search engines for Footprinting. • Investigate Footprinting through Web Services. • Examine Footprinting through Social Networking Sites. • Conduct Website Footprinting. • Perform Whois Footprinting. • Explore DNS Footprinting. • Assess Network Footprinting. • Employ Social Engineering for Footprinting. • Develop Footprinting Countermeasures.	**Task#2**
		Day 2	**Master Network Scanning** • Understand Network Scanning Concepts. • Utilize Scanning Tools. • Conduct Host Discovery. • Perform Port and Service Discovery. • Identify OS Discovery techniques (Banner Grabbing/OS Fingerprinting). • Explore scanning methods beyond IDS and Firewalls. • Create Network Diagrams.	

		Day 3	**Explore Enumeration Techniques** • Define Enumeration Concepts. • Conduct NetBIOS Enumeration. • Apply SNMP Enumeration techniques. • Execute LDAP Enumeration. • Investigate NTP and NFS Enumeration. • Perform SMTP and DNS Enumeration. • Examine Other Enumeration Techniques and develop Enumeration Countermeasures.	
		Day 4	**Conduct Vulnerability Analysis** • Understand Vulnerability Assessment Concepts. • Classify Vulnerabilities and assess different types. • Evaluate Vulnerability Assessment Solutions and Tools. • Analyze Vulnerability Assessment Reports.	
		Day 5	**Master System Hacking** • Understand System Hacking Concepts. • Gain Access to system. • Crack Passwords. • Exploit Vulnerabilities. • Escalate Privileges. • Maintain Access. • Execute Applications. • Hide Files. • Clear Logs.	

Week 3	**ISMS (with ISO 27001/27002) and Incident Response**	**Day 1**	**Explore Information Security Management System (ISMS) Concepts as Required by ISO/IEC 27001** • Identify Standards and Regulatory Frameworks. • Understand Information Security Management System (ISMS). • Examine Fundamental Principles of Information Security Management Systems. • Analyze the Organization and Clarify Information Security Objectives. • Assess the Existing Management System.	**Task#3**
		Day 2	**Plan the Implementation of an ISMS Based on ISO/IEC 27001** • Obtain Leadership and Approval for the ISMS Project. • Determine the ISMS Scope. • Develop Information Security Policies. • Perform a Risk Assessment. • Prepare the Statement of Applicability and Facilitate Top Management's Decision to Implement the ISMS. • Define the Organizational Structure of Information Security. • Establish the Document Management Process. • Design Security Controls and Draft Specific Policies & Procedures. • Formulate a Communication Plan. • Create a Training and Awareness Plan.	

		Day 3	**Manage ISMS Monitoring, Measurement, Continuous Improvement, and Certification Audit Preparation** • Implement security controls. • Handle Incident Management. • Oversee Operations Management. • Monitor, measure, analyze, and evaluate ISMS performance. • Conduct Internal Audits. • Review Management processes. • Address non-conformities. • Promote Continual Improvement. • Prepare for the certification audit.	
		Day 4	**Implement PCIDSS Compliance Measures** **Build and Maintain a Secure Network** • **Install** and maintain a firewall configuration to protect cardholder data (Requirement 1). • **Avoid** using vendor-supplied defaults for system passwords and other security parameters (Requirement 2). **Protect Cardholder Data** • **Protect** stored cardholder data (Requirement 3). • **Encrypt** transmission of cardholder data across open, public networks (Requirement 4). **Maintain a Vulnerability Management Program** • **Use** and regularly update anti-virus software (Requirement 5). • **Develop** and maintain secure systems and applications (Requirement 6). **Implement Strong Access Control Measures** • **Restrict** access to cardholder data by business need-to-know (Requirement 7). • **Assign** a unique ID to each person with computer access (Requirement 8).	

			• **Restrict** physical access to cardholder data (Requirement 9). **Regularly Monitor and Test Networks** • **Track** and monitor all access to network resources and cardholder data (Requirement 10). • **Regularly test** security systems and processes (Requirement 11). **Maintain an Information Security Policy** • **Maintain** a policy that addresses information security (Requirement 12).	
		Day 5	**Implement NIST Incident Response Procedures - NIST SP 800-61** **Preparation** • **Develop** an Incident Response Policy and Plan. • **Establish** the Incident Response Team (IRT) Structure. • **Provide** Tools and Resources. **Detection and Analysis** • **Identify** Indicators of Compromise. • **Perform** Event Correlation and Analysis. • **Document** Incidents. **Response Planning** • **Design** Response Procedures and Strategies. • **Create** Communication Plans. • **Coordinate** with External Parties. **Containment, Eradication, and Recovery** • **Implement** Containment	

			Strategies. • **Eradicate** Threats. • **Execute** Recovery Procedures. • **Validate** Recovery. **Post-Incident Activity** • **Extract** Lessons Learned. • **Complete** Post-Incident Reporting. • **Update** Policies and Procedures. **Continuous Improvement** • **Review** and **Enhance** the Incident Response Plan. • **Incorporate** Feedback into Training.	
Week 4	**Emerging Threats, Mitigations and Ethical Considerations**	**Day 1**	**Analyze Types of Cybersecurity Threats** • Define Malware. • Differentiate between Viruses and Worms. • Identify Cryptojacking. • Explore Fileless Malware. • Assess Ransomware. • Examine Advanced Persistent Threats (APTs). • Understand Distributed Denial of Service (DDoS) attacks. • Investigate Man-in-the-Middle (MitM) attacks. • Evaluate State-Sponsored and Insider Threats.	**Task#4**

		Day 2	**Identify Social Engineering Attacks** • Differentiate Phishing Variants. • Explain Baiting and Pretexting. • Understand Business Email Compromise (BEC). • Define Social Engineering Concepts. • Apply Social Engineering Techniques. • Recognize Insider Threats. • Detect Impersonation on Social Media. • Identify Identity Theft. • Develop Social Engineering Countermeasures.	
		Day 3	**Implement Top Ten Cybersecurity Mitigation Strategies** • Update and Upgrade Software Immediately. • Secure Privileges and Accounts. • Enforce Signed Software Execution Policies. • Develop a System Recovery Plan. • Manage Systems and Configurations Actively. • Hunt for Network Intrusions Continuously. • Utilize Modern Hardware Security Features. • Segregate Networks Using Application-Aware Defenses. • Integrate Threat Reputation Services. • Transition to Multi-Factor Authentication.	

		Day 4	**Explore Sandboxing in Cybersecurity** • **Definition and Concept of Sandboxing** • **Define** Sandboxing and its concept. • **Explain** its importance in Cybersecurity. • **Illustrate** the analogy of a sandbox as a safe environment. **Types of Sandboxing** • **Describe** Application Sandboxing. • **Explain** Web Browser Sandboxing. • **Identify** Security Sandboxing. • **Discuss** Network Sandboxing. • **Explore** Cloud-based or Virtual Sandboxing. • **Understand** Developer Sandboxing. **Challenges of Sandboxing** • **Evaluate** Resource Intensity. • **Assess** Management Time. • **Address** False Positives and False Negatives. **Benefits of Sandboxing** • **Enhance** Security. • **Protect** Privacy. • **Improve** Operational Efficiency.	
		Day 5	**Adhere to the Code of Ethics and Professional Conduct** **General Ethical Principles** • **Contribute** to Society and Human Well-being. • **Avoid** Harm. • **Demonstrate** Honesty and Trustworthiness. • **Ensure** Fairness and Avoid Discrimination. • **Respect** Intellectual Property. • **Protect** Privacy. • **Honor** Confidentiality. **Professional Responsibilities** • **Strive** for High Quality. • **Maintain** Professional Competence.	

			• **Understand** and Respect Rules. • **Accept** and **Provide** Professional Reviews. • **Evaluate** Systems Thoroughly. • **Work** Within Areas of Competence. • **Foster** Public Awareness. • **Access** Resources Appropriately. • **Design** Secure Systems. **Professional Leadership Principles** • **Focus** on Public Good. • **Promote** Social Responsibilities. • **Enhance** Quality of Working Life. • **Support** Ethical Policies. • **Create** Growth Opportunities. • **Modify** Systems with Care. • **Steward** Systems in Infrastructure. **Compliance with the Code** • **Uphold** and **Promote** Principles. • **Address** Violations Seriously.	

Practical Tasks:

	Task	Description	Week
1	**Setup and Deploy a Firewall**	● Practice how firewall rules operate by configuring a basic firewall rule. ● Implement firewall rules, generate alerts based on detection rules.	Week 1
2	**Provide mentioned details about www.certifiedhacker.com website**	● What is the IP Address of this website ● What's the country name of its hosting server ● Is this website protected by any WAF or not? If yes, then mention its details. ● When will this website's domain registration expire? ● Which Company is managing its web hosting?	Week 2
	Using Ethical Hacking Methodology Create a malicious file and gain access of Windows Machine and produce following mentioned things as proof of access	● Screenshot of the compromised machine ● List of running services on compromised machine ● Download zipfldr.dll file to Kali Linux which is placed in C:\Winodws\System32 folder	
3	**Implement an ISMS using ISO 27001 Framework for a Small Business**	● Define the ISMS scope and why? ● List five risks and their mitigation strategies. ● Select ten Annex A controls. Why? ● Create bring your own device (BYOD) policy	Week 3
4	**Demonstrate a Social Engineering and Analyse**	● Demonstrate a Phishing Attack ● Analyse any Social Engineering Attack using any online portal	Week 4
5	**Task#1: Implement Firewalls rules to Block social media access**	● Create firewall rules that blocks user access on TikTok, Instagram, WhatsApp, Instagram, YouTube, and Discord by restricting all traffic to those platforms, ensuring controlled internet usage within the network.	Final Exam #1
	Task#2:	● IP Address of Machine	

	VAPT Task **Scan the complete network and find any Windows Server Machine then find vulnerability and compromise it.**	● List of Running Services and Open Ports ● Operating System Details ● Services Versions Info ● NetBIOS name of Computer ● Vulnerability code ● Vulnerability rating ● Collect hashed passwords of all users ● Clear all activity Logs	
	Task#3: Implement an ISMS using ISO 27001 Framework for an Organization	● Define the ISMS scope and why? ● Identify and deploy ISO27001 Annex A controls. Why? ● Create at least three policy ● Describe how e-banking applications secure credit card holder data, highlighting compliance with PCI-DSS standards and data protection practices. ● Create Statement of Applicability (SoA)	
6	**Task#1: Demonstrate various social engineering attacks and apply mitigation strategies using knowledge gained throughout the course.**	● Create a spear-phishing email and send it to a target user to simulate a real social engineering attack. ● Demonstrate credential harvesting by sending a phishing link (such as a social site login page) to steal user credentials. ● Use the knowledge gained throughout this course to identify, mitigate, and protect your organization from such social engineering attacks.	Final Exam #2
	Task#2: Implement an ISMS using ISO 27001 Framework for an Organization	● List assets, perform risks assessment and their mitigation strategies. ● Create Risk Treatment Plan RTP ● Handle non-conformities and ensure corrective actions are effectively implemented	
	Task#3 Conduct a vulnerability assessment to identify and mitigate vulnerabilities in your environment.	● Deploy a vulnerability scanning tool within your environment. ● Execute a vulnerability scan on a designated machine to uncover vulnerabilities. ● Analyze the scan results and recommend appropriate mitigation strategies for the identified	

		vulnerabilities. ● Prepare a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) report summarizing the activities and findings, tailored for an executive audience.	

Annexure-IV:

Workplace/Institute Ethics Guide

Work ethic is a standard of conduct and values for job performance. The modern definition of what constitutes good work ethics often varies. Different businesses have different expectations. Work ethic is a belief that hard work and diligence have a moral benefit and an inherent ability, virtue, or value to strengthen character and individual abilities. It is a set of values-centered on the importance of work and manifested by determination or desire to work hard.

The following ten work ethics are defined as essential for student success:

1. **Attendance:**
   Be at work every day possible, plan your absences don't abuse leave time. Be punctual every day.
2. **Character:**
   Honesty is the single most important factor having a direct bearing on the final success of an individual, corporation, or product. Complete assigned tasks correctly and promptly. Look to improve your skills.
3. **Team Work:**
   The ability to get along with others including those you don't necessarily like. The ability to carry your weight and help others who are struggling. Recognize when to speak up with an idea and when to compromise by blend ideas together.
4. **Appearance:**
   Dress for success set your best foot forward, personal hygiene, good manner, remember that the first impression of who you are can last a lifetime
5. **Attitude:**
   Listen to suggestions and be positive, accept responsibility. If you make a mistake, admit it. Values workplace safety rules and precautions for personal and co-worker safety. Avoids

unnecessary risks. Willing to learn new processes, systems, and procedures in light of changing responsibilities.

6. **Productivity:**

   Do the work correctly, quality and timelines are prized. Get along with fellows, cooperation is the key to productivity. Help out whenever asked, do extra without being asked. Take pride in your work, do things the best you know-how. Eagerly focuses energy on accomplishing tasks, also referred to as demonstrating ownership. Takes pride in work.

7. **Organizational Skills:**

   Make an effort to improve, learn ways to better yourself. Time management; utilize time and resources to get the most out of both. Take an appropriate approach to social interactions at work. Maintains focus on work responsibilities.

8. **Communication:**

   Written communication, being able to correctly write reports and memos. Verbal communications, being able to communicate one on one or to a group.

9. **Cooperation:**

   Follow institute rules and regulations, learn and follow expectations. Get along with fellows, cooperation is the key to productivity. Able to welcome and adapt to changing work situations and the application of new or different skills.

10. **Respect:**

    Work hard, work to the best of your ability. Carry out orders, do what's asked the first time. Show respect, accept, and acknowledge an individual's talents and knowledge. Respects diversity in the workplace, including showing due respect for different perspectives, opinions, and suggestions.