ACADEMY FOR COOPERATIVE MANAGEMENT RESEARCH AND TRAINING
(ACMART)
Website : wbacmart.com

Training Programme on "Risk Management In Banks"
(Particularly under Internet Banking and ATM Operations with Special Emphasis on Information / Cyber Security)
Day – to Day Schedule

Day	Session	Subject	Topic	Resource Person
First		**Registration & Inauguration**		
	I	**Introduction to Risk Management In Banks**	Identifying and assessing the potential risk in the banking business	
			Conventional Risks - *Credit Risk, Liquidity Risk, Market Risk or Systematic Risk, Interest Rate Risk, Earning Risk, Solvency or Default Risk*	
			Developing and executing an action plan to deal with and manage these activities that incur potential losses	
			Continuously reviewing and reporting the risk management practices after they have been put into action/operation.	
			Cyber Risks and Conventional Risks Vs. Cyber Risks	
	II	**Computer / Cyber Insecurity**	Meaning and Definition of Information Security	
			Pillars of Information Security	
			Software and Hardware Security	
			Network Security	
			Internet Crimes & Causes for Internet Crimes	
			User failures	
			Bank failures and Initiatives	
	III	**Necessity of Cyber Security in Banking Sector**	Increasing uses of digital money	
			Data breaches	
			Losing time and money	
			Private / personal data in the wrong hands	
	IV	**The Evolving Cyber Threat Landscape**	Account Takeovers	
			Payment Systems	
			ATM Skimming	
			Pont of sale Terminal	
			Internet Banking Frauds	
			Mobile Banking Exploitation	

Second Day	**I**	**Critical Components of Information / Cyber Security**	*Policies and procedures, Risk Assessment, Inventory and information/data classification, Defining roles and responsibilities, Access Control, Information security and information asset life-cycle, Personnel security, Physical security, User Training and Awareness, Incident management, Application Control and Security, Migration controls, Implementation of new technologies, Encryption, Data security*	
	II	**Critical Components of Information / Cyber Security (Contd....)**	*Vulnerability Assessment, Establishing on-going security monitoring processes, Security measures against Malware, Patch Management, Change Management, Audit trail, Information security reporting and metrics, Information security and Critical service providers/vendors, Network Security, Remote Access, Distributed Denial of service attacks(DDoS/DoS), Implementation of ISO 27001 Information Security Management System, Wireless Security, Business Continuity Considerations, Information security assurance*	
	III	**Security Threats and Security Measures with regard to Delivery Channels**	ATM related measures Card based online transactions/E-Commerce Phone Banking	
			Customer awareness / Education in Cyber Securities	
	IV	**Security Threats and Security Measures with regard to Delivery Channels (Contd.....)**	Mobile Banking Debit Card Security Measures Anti-skimming Measures Internet banking – Safety features	
Third Day	**I**	**Technology Options for Cyber Security**	AI and machine learning Technical integration Merging existing and new technologies Flexible endpoint solutions Virtualization Cloud Computing Multiprotocol Label Switching (MPLS)	
	II	**Emerging Technologies**	Hardware authentication User-behaviour analytics Data loss prevention	

			Endpoint detection and response	
			Remote browser	
			Deception	
		Future technologies	Single Photon Generation	
			Privacy Homomorphism	
	III	**IT Risk Management & Formulation of IT Security Policy**	Risk assessment - Risk identification, Risk evaluation, Risk Mitigation	
			Risk communication	
			Risk monitoring and review	
			IT Security Policy	
	IV	**Sum up, Feedback, Evaluation and Valediction**		

Session Timings

First : 10.00 a.m. to 11.30 a.m Second : 11.45 a.m. to 1.15 p.m. Third : 2.15 p.m. to 3.30 p.m. Fourth : 3.45 p.m. to 5.00 p.m.

Tea Break : 11.30 a.m. to 11.45 a.m. and 3.30 p.m. to 3.45 p.m. Lunch Break : 1.15 p.m. to 2.15 p.m.