RED RIVER COLLEGE
OF APPLIED ARTS, SCIENCE AND TECHNOLOGY

IT Security DACUM Workshop

Facilitated by Mike Stuhldreier & Gene Semchych

1-May-03

Manage Risk A	Classify data and assets A1	Assess threat, risk, and vulnerability A2	Work within scope of responsibility A3	Mitigate risk A4	Communicate Risk A5	Translate risk into business terms A6	Analyze risk A7
Apply Cryptography and Encryption B	Implement tools B1	Identify need B2	Establish standards B3	Test and verify encryption B4	Manage and distribute keys B5	Research techniques and products B6	Justify need B7
	Promote use of cryptography and encryption B8						
Communicate C	Write C1	Speak C2	Present C3	Communicate to a variety of audiences C4	Be concise C5	Seek and receive feedback C6	Listen C7
	Read C8	Filter information C9	Use meeting etiquette C10	Follow corporate communications plan C11	Communicate corporate values C12		
Display Positive Personal Attributes D	Demonstrate domain expertise D1	Demonstrate ethics D2	Focus on productivity D3	Problem solve D4	Be organized D5	Lead others D6	

Manage Security E	Write RFPs E1	Respond to RFPs E2	Evaluate RFPs E3	Develop and implement policies, procedures, and guidelines E4	Educate and train E5	Enforce policies and procedures E6	Evaluate and improve continuously E7
	Develop measurements E8	Record metrics E9	Implement security plan E10	Interface with human resouces E11			
Develop Security Architecture F	Map business to technology F1	Apply formal security models F2	Apply principles of common criteria F3	Design data separation F4	Interface and synchronize multiple DBMSs F5	Define and apply Guiding Principles F6	Define Zones of Operation F7
Be Professional G	Remain current G1	Negotiate G2	Think critically G3	Work in teams G4	Adapt G5	Network G6	Think outside the box G7
	Think strategically G8	Think globally G9	Function within a political environment G10	Apply business savvy G11	Multi-task G12	Train continuously G13	Maintain professional status G14
Manage Projects H	Develop timelines H1	Use tools H2	Plan H3	Budget H4	Monitor H5	Manage change H6	Manage project risk H7
	Evaluate H8	Set priorities H9	Manage team H10	Manage deliverables (Scope creep) H11	Enforce quality H12		
Manage Incidents I	Comply with laws, regulations, and protocols I1	Develop and implement forensic processes I2	Develop incident response capability I3	Liaise with external authorities I4	Develop and implement incident response methodology I5		

Manage People J	Create teams J1	Influence others J2	Delegate J3	Interview J4	Write job descriptions J5	Evaluate J6	Resolve disputes J7
	Identify training needs J8	Mentor J9	Hire and fire J10				
Develop Access Control Systems K	Define and determine access controls K1	Implement access controls K2	Monitor access controls K3	Enforce access controls K4	Select products and tools K5	Respond to violations K6	Define roles/ownership & rights K7
	Authorize users K8	Validate users K9	Manage users K10	Manage authentication and identificaton systems K11			
Apply Network Security L	Implement a secure IP network L1	Implement intrusion detection systems L2	Work with a variety of operating systems L3	Program firewalls L4	Manage/monitor traffic L5	Secure remote access L6	Manage certificates L7
	Audit passwords L8	Manage logs L9	Harden systems L10	Architect network solutions L11	Certify and accredit products L12	Implement anti-virus L13	Monitor Internet L14
	Monitor acceptable corporate use L15	Manage capacity L16	Build fault tolerance L17	Do penetration testing L18			
Apply Operations Security M	Ensure segregation of operational duties M1	Implement counter-measures M2	Define and implement operational procedures M3	Secure backup tapes M4	Process logs M5	Document exception handling M6	Implement and document change management process M7

	Apply and manage patches M8	Manage resources M9					
Manage Application Life Cycle Security N	Evaluate databases N1	Develop test plans N2	Ensure coding standards N3	Test for vulnerabilities N4	Monitor application use N5	Assess privacy impact N6	Audit development and application life cycles N7
Research and Experiement O	Establish test procedures O1	Test environments O2	Be an early adopter O3	Report findings O4	Find and disclose vulnerabilities O5	Be proactive O6	Test new technologies O7
	Collaborate with others O8						
Manage Physical Security P	Manage physical access controls P1	Test physical security P2	Contribute to design of physical environment P3	Monitor access P4	Work with facility security P5	Make recommendations (Insurance, product selection, business location, etc.) P6	Make recommendations for compliance enforcement P7
	Monitor breaches P8						
Contribute to DRP/BCP Plan Q	Test Q1	Design action plan Q2	Evaluate action plan Q3	Ensure compliance Q4	Perform business impact analysis Q5	Distinguish between DRP and BCP Q6	Manage crises Q7
	Plan for succession Q7	Manage availability Q8					