

Terms and Terminology



Information Assurance (IA)

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Department of Defense (DoD)

The U.S. federal department charged with coordinating and supervising all agencies and functions of the government relating directly to national security and the United States armed forces.

DoD Directive 8500.1

Requires that "all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines" and tasks **DISA** to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA."

5





Terms and Terminology



DoD IA Controls

The Department of Defense Information Assurance (IA) program establishes a baseline set of controls to be applied to all DoD information systems. Each control is uniquely named and can be referenced, measured, and reported against throughout the life cycle of a DoD information system.

Security Readiness Review (SRR)

The audit performed at designated sites to review compliance with the **DISA STIGs**.

SRRAUDIT

The name assigned to the **SSR** audit process to validate compliance with the **DISA STIG**s.

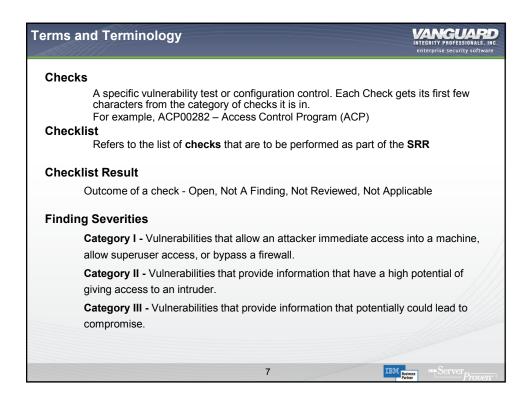
DHS

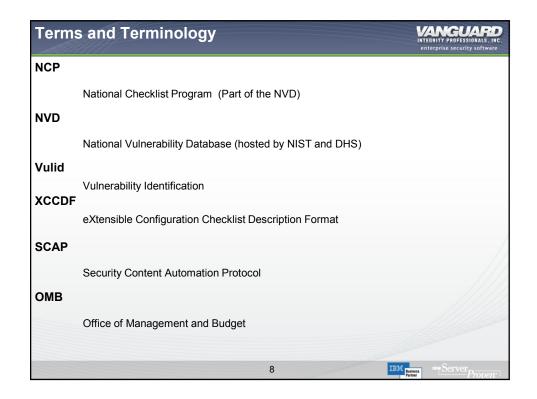
Department of Homeland Security

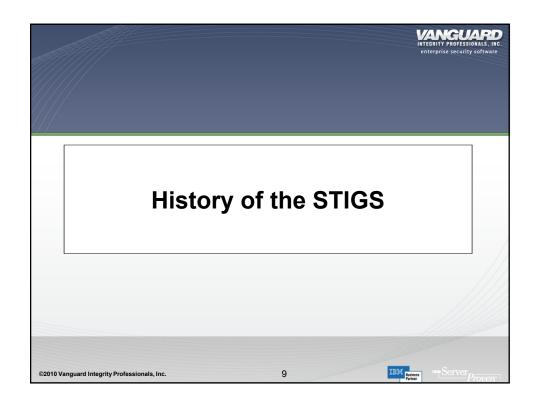


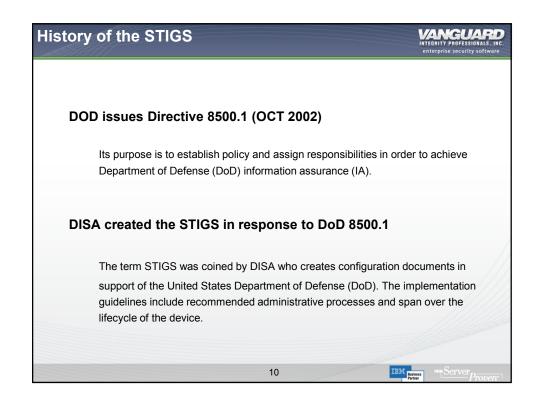


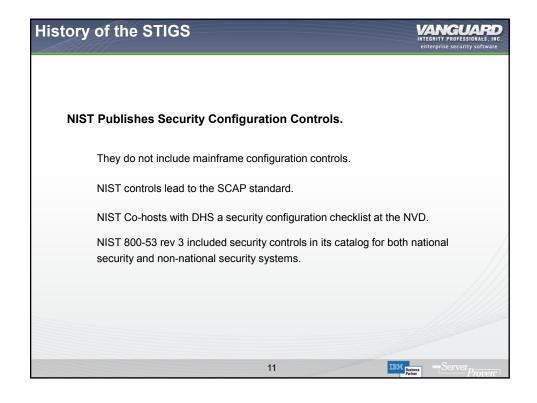
6

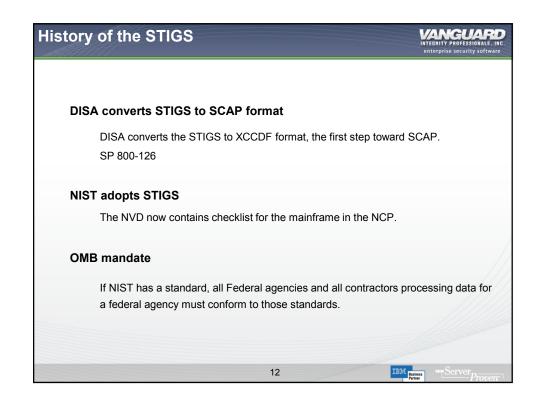


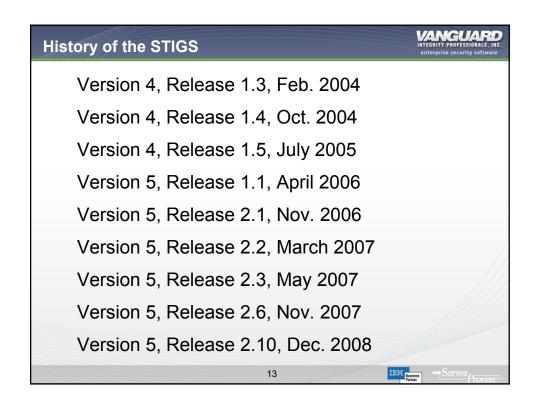


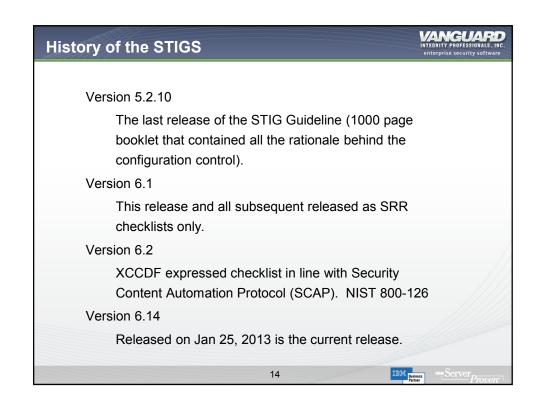




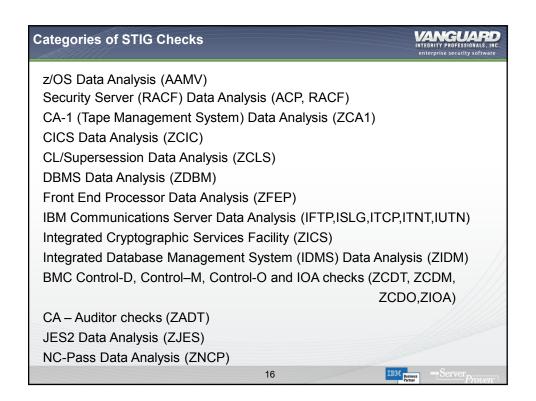


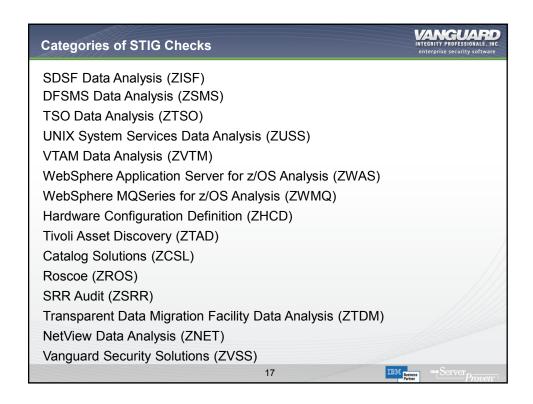


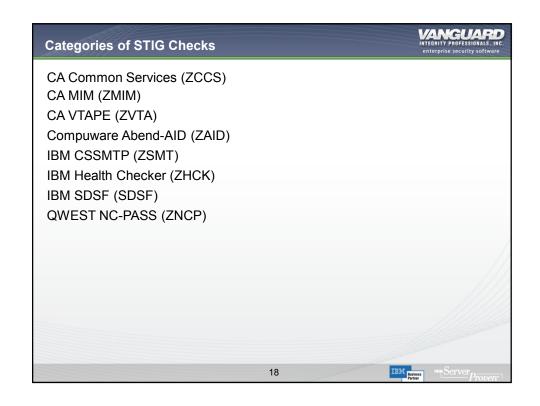


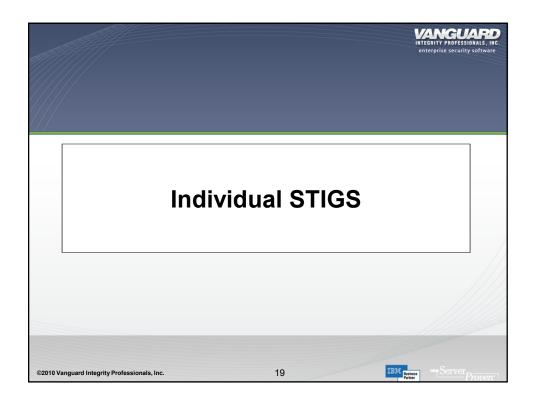


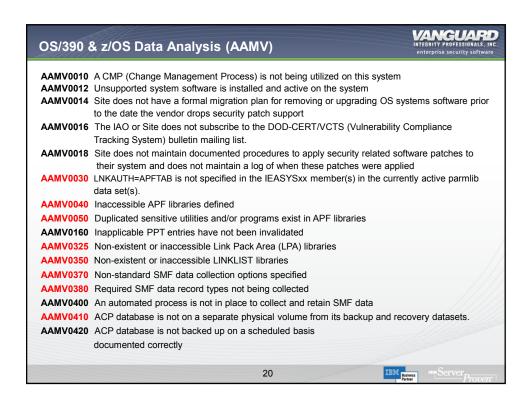


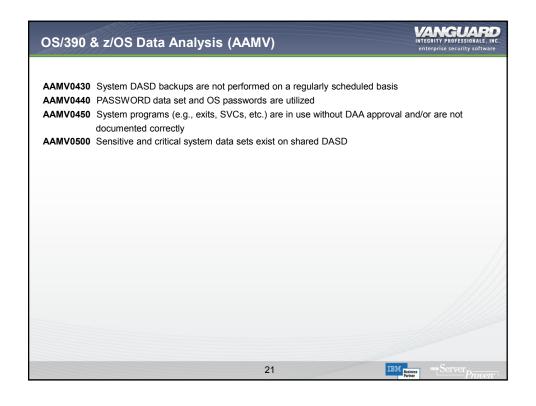


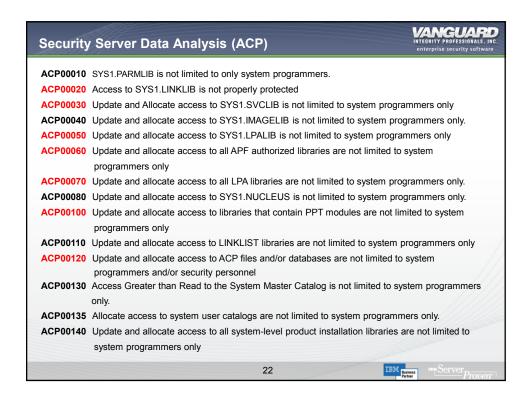




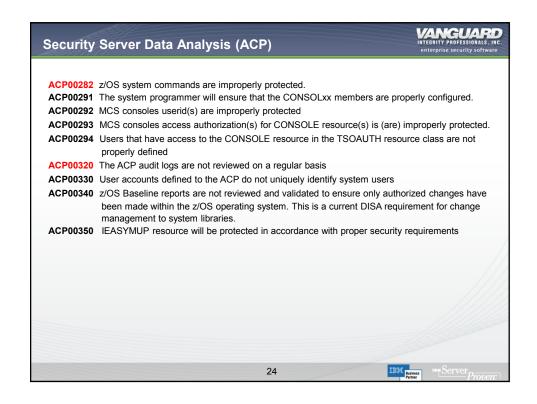


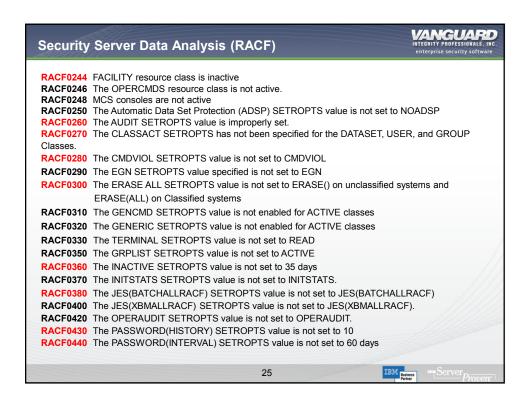


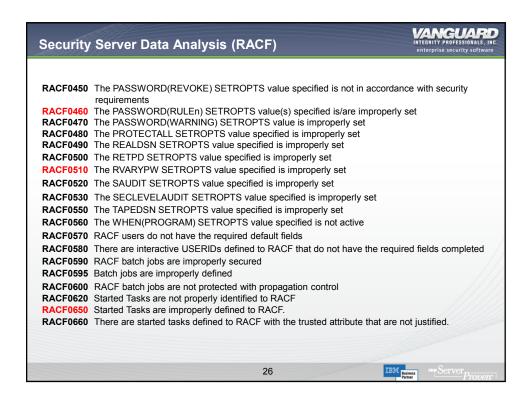


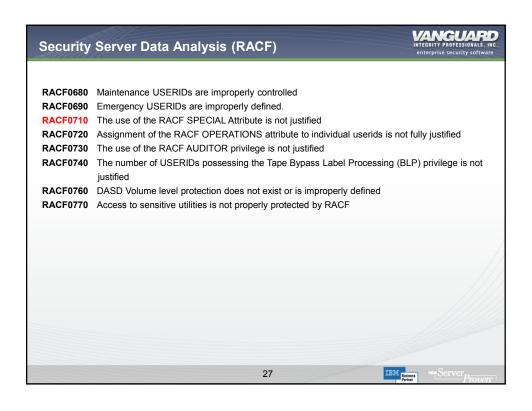


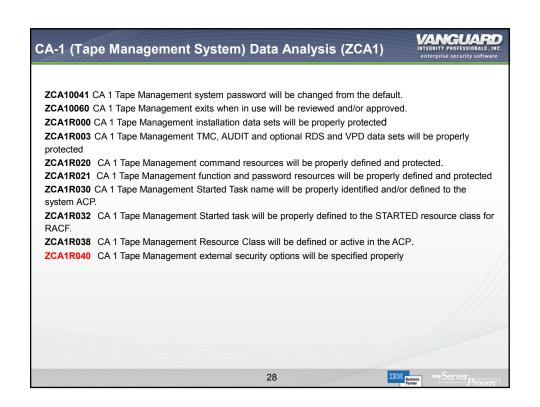
Security	Server Data Analysis (ACP)	VANGUARI INTEGRITY PROFESSIONALS, IN enterprise security software	
ACP00150	Update and allocate access to the JES2 System data sets (e.g., Spool, Checkpoint, and		
	Initialization parameters) are not limited to system programmers only		
ACP00170	Allocate access to SYS1.UADS is not limited to system programmers only and read and		
	update access is not limited to system programmer personnel and/or se	curity personnel	
ACP00180	Update and allocate access to SMF collection files (i.e., SYS1.MANx) are	e not limited to	
	system programmers and/or batch jobs that perform SMF dump process	sing.	
ACP00190	Update and allocate access to data sets used to backup and/or dump SN	MF collection files are	
	not limited to system programmers and/or batch jobs that perform SMF	dump processing.	
ACP00200	Access to SYSTEM DUMP data sets are not limited to system programmers only		
ACP00210	Update and allocate access to System backup files are not limited to system programmers and/or batch jobs that perform DASD backups.		
ACP00220	Access to SYS(x) TRACE is not limited to system programmers only		
ACP00230	Access to System page data sets (i.e., PLPA, COMMON, and LOCALx) are not limited to system programmers.		
ACP00240	Update and allocate access to Libraries containing EXIT modules are not limited to system programmers only		
ACP00250	Update and alter access to all system proclib datasets are limited to system programmers only		
ACP00260	Memory and privileged program dumps are not protected in accordance with proper security requirements		
ACP00270	Dynamic lists are not protected in accordance with proper security requir	rements.	
	23	BM Business Server	

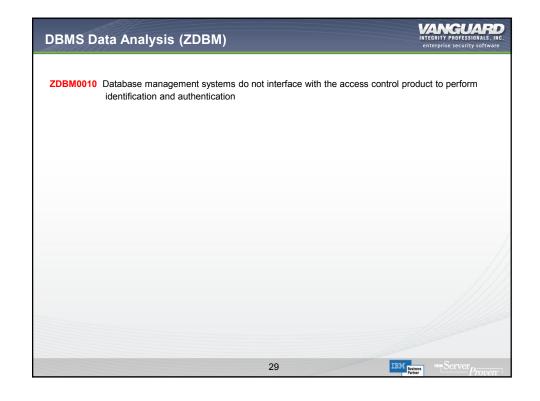


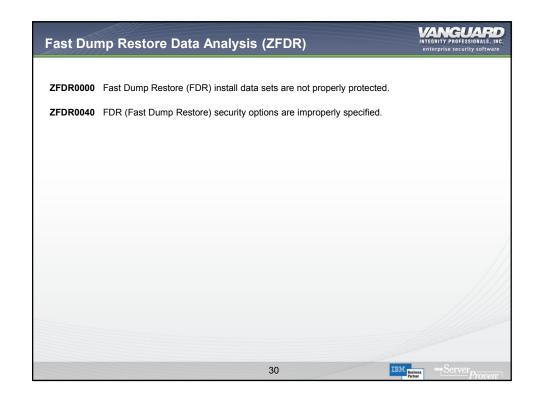






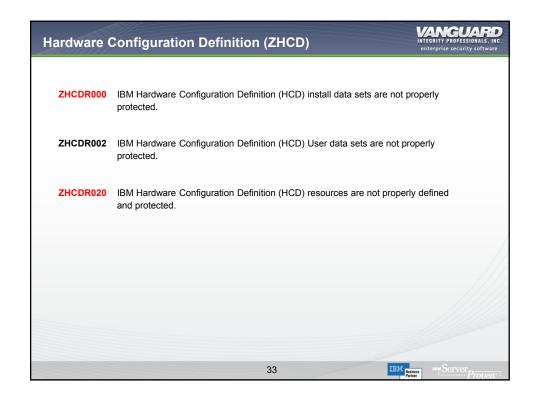


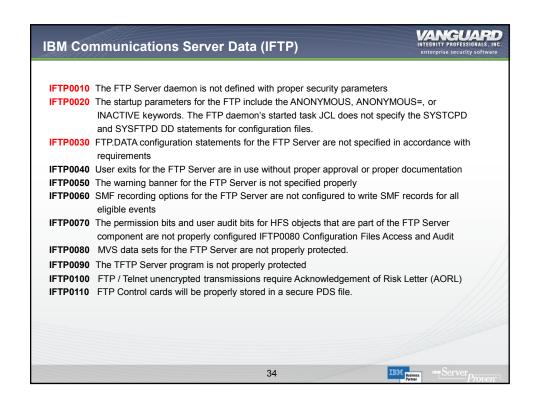


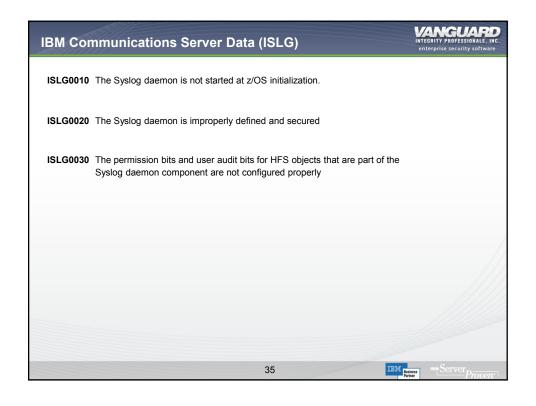


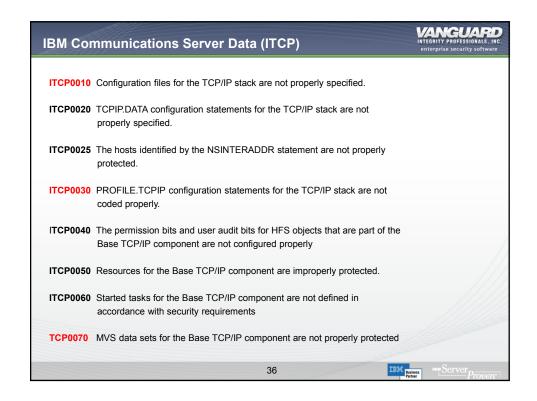
CICS Data	Analysis (ZCIC)	VANGUARD INTEGRITY PROFESSIONALS, INI enterprise security software
ZCIC0010	CICS system data sets are not properly protected	
ZCIC0020	Sensitive CICS transactions are not protected in accordance with security requirements.	
ZCIC0030	CICS System Initialization Table (SIT) parameter values are not specified in accordance with proper security requirements	
ZCIC0040	CICS region logonid(s) are not defined and/or controlled in accordance will requirements	th the security
ZCIC0041	CICS default logonid(s) are not defined and/or controlled in accordance with the security requirements	
ZCIC0042	CICS logonid(s) do not have time-out limit set to 15 minutes	
	External RACF Classes are not active for CICS transaction checking IBM CICS Transaction Server SPI command resources will be properly defined and	
ZCICR041	CICS regions are improperly protected to prevent unauthorized propagation userid	on of the region
	31 IBM	Server

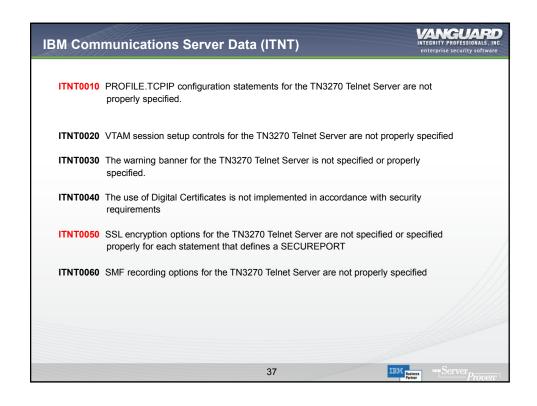
VANGUARD Front End Processor (FEP) Data Analysis (ZFEP) ZFEP0011 All hardware components of the FEPs are not placed in secure locations where they cannot be stolen, damaged, or disturbed ZFEP0012 Procedures are not in place to restrict access to FEP functions of the service subsystem from operator consoles (local and/or remote), and to restrict access to the diskette drive of the service subsystem. ZFEP0013 A documented procedure is not available instructing how to load and dump the FEP NCP (Network Control Program ZFEP0014 An active log is not available to keep track of all hardware upgrades and software changes made to the FEP (Front End Processor ZFEP0015 NCP Dataset Analysis ZFEP0015 NCP (Net Work Control Program) Data set access authorization does not restricts UPDATE and/or ALLOCATE access to appropriate personnel **ZFEP0016** A password control is not in place to restrict access to the service subsystem via the operator consoles (local and/or remote) and a key-lock switch is not used to protect the modem supporting the remote console of the service subsystem. 32

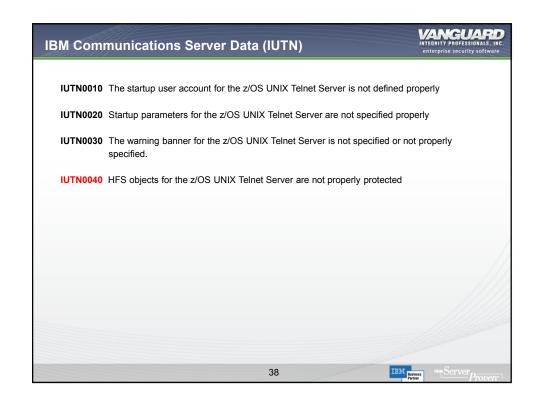


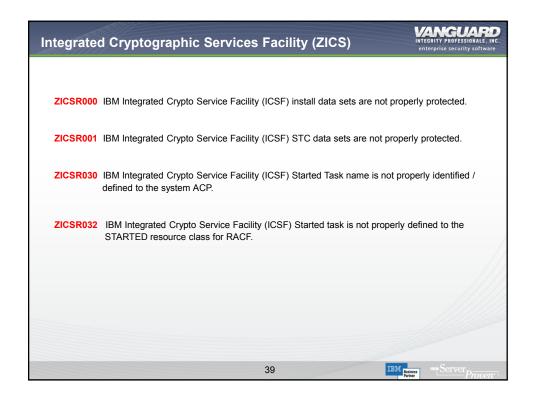


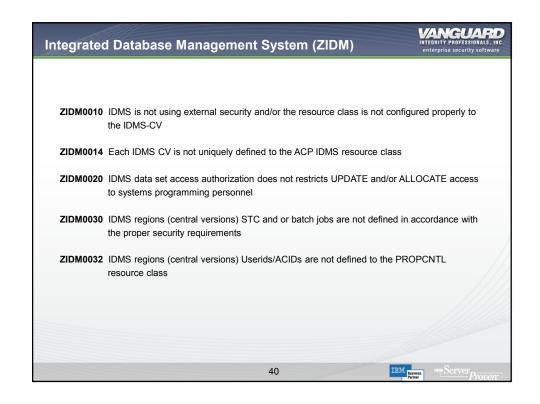


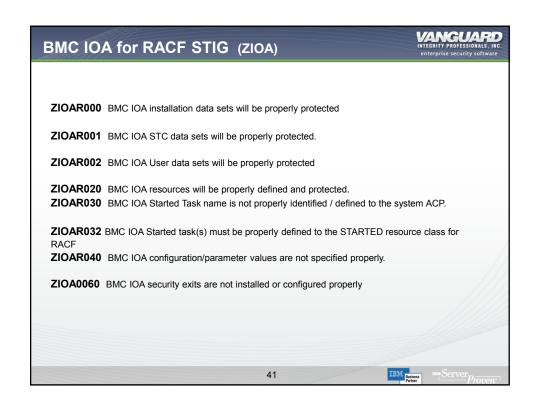


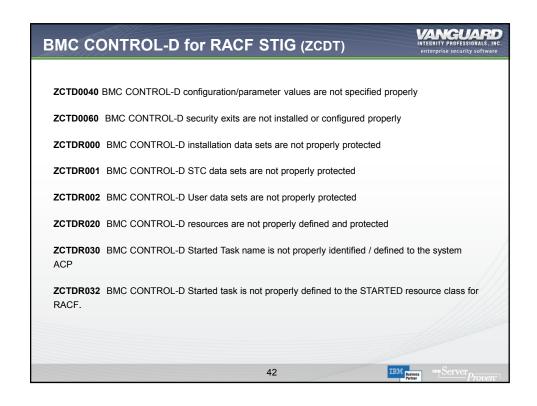












BMC CONTROL-O for RACF STIG (ZCTO)



ZCTO0040 BMC CONTROL-O configuration/parameter values are not specified properly.

ZCTO0041 BMC CONTROL-O configuration/parameter values are not specified properly.

ZCTO0060 BMC CONTROL-O security exits are not installed or configured properly

ZCTOR000 BMC CONTROL-O installation data sets are not properly protected

ZCTOR001 BMC CONTROL-O STC data sets are not properly protected

ZCTOR020 BMC CONTROL-O resources are not properly defined and protected.

ZCTOR030 BMC CONTROL-O Started Task name is not properly identified / defined to the system ACP.

ZCTOR032 BMC CONTROL-O Started task is not properly defined to the STARTED resource class for RACF.

43





BMC CONTROL-M for RACF STIG (ZCTM)



ZCTM0060 BMC CONTROL-M security exits are not installed or configured properly.

ZCTMR000 BMC CONTROL-M installation data sets are not properly protected.

ZCTMR001 BMC CONTROL-M STC data sets are not properly protected.

ZCTMR002 BMC CONTROL-M User data sets are not properly protected.

ZCTMR003 BMC CONTROL-M User/Application JCL data sets are not properly protected

ZCTMR020 BMC C0NTROL-M resources are not properly defined and protected.

ZCTMR030 BMC CONTROL-M Started Task name is not properly identified / defined to the system ACP.

ZCTMR032 BMC CONTROL-M Started task is not properly defined to the STARTED resource class for RACF.

ZCTMR040 BMC CONTROL-M configuration/parameter values are not specified properly

11





