

AS/400 Control Matrix

Business Process: _____

Program Section	Specific Control Objectives	Risk Effect(s)	Audit Tests Performed	Results	Workpaper
	Access methods should be limited to methods established by system administrators	<ul style="list-style-type: none"> Users may gain access to the system by unauthorized means 	<ul style="list-style-type: none"> Determine the access methods (LAN, Citrix, dial-up...) Evaluate the controls used to gain access 	<ul style="list-style-type: none"> 	
	Only management approved, authorized users should have access to the system	<ul style="list-style-type: none"> Unauthorized users may obtain access to the system 	<ul style="list-style-type: none"> Document the process of adding new users to the system Obtain a list of new users on the system and trace to authorization requests 	<ul style="list-style-type: none"> 	
	Terminated users are promptly removed from the system	<ul style="list-style-type: none"> Unauthorized users may obtain access to the system 	<ul style="list-style-type: none"> Obtain either an employee list or a list of terminated employees and reconcile to user list Determine if users have been removed or passwords set to *NONE 	<ul style="list-style-type: none"> 	

Program Section	Specific Control Objectives	Risk Effect(s)	Audit Tests Performed	Results	Workpaper
	Manufacturer supplied user profiles' passwords should be changed or set to *NONE	<ul style="list-style-type: none"> Unauthorized access could be gained by using published password names 	<ul style="list-style-type: none"> Display all users on the system by user and group profiles (user profile query): DSPAUTUSR (*PRINT) – or to file Ensure the following names have been set to *NONE or have been changed from original installation passwords: QLPAUTO, QLPINSTALL, QSPL, QRJE, QFNC, QGATE, QPGMR, QSRVBAS, QSRV, QSYS, QDOC, QDBSHR, QDFTOWN, QUSER, QSPLJOB, QSNADS, QDSNX Ensure passwords have been changed for the following names: QSECOFR, and QSYSOPR. 	<ul style="list-style-type: none"> 	
	High level security profiles should be limited to a select group of key users	<ul style="list-style-type: none"> Inappropriate access to high security level profiles provides users with excessive system access 	<ul style="list-style-type: none"> Examine the user profile query to determine allocation of special authorities: QSECOFR, *ALLOBJ, *SECADM, *SAVSYS, *JOBCTL, *SERVICE, *SPLCTL, AND *AUDIT 	<ul style="list-style-type: none"> 	

Program Section	Specific Control Objectives	Risk Effect(s)	Audit Tests Performed	Results	Workpaper
	Use of sensitive commands should be limited to select group of key users	<ul style="list-style-type: none"> Inappropriate access to sensitive commands provides users with excessive system access 	Print out all users who have object authority to the following list of sensitive commands using DSPOBJAUT OBJ(QSYS/command) OBJTYPE(*CMD) OUTPUT(*PRINT) ADDAUTLE CHGAUTLE CHGDTA CHGNETA CHGOBJOWN CHGSYSVAL CHGUSRPRF CRTAUTHLR CRTAUTL CRTUSRPRF DLTAUTHLR DLTAUTL DLTUSRPRF EDTAUTL EDTOBJAUT GRTOBJAUT GRTUSRAUT PWRDWNSYS SBMRMTCMD STRDFU STRPDM STRREXPRC STRSEU STRSST TRFCTL UPDDTA	<ul style="list-style-type: none"> 	

Program Section	Specific Control Objectives	Risk Effect(s)	Audit Tests Performed	Results	Workpaper
	System parameters should be set to match the AS/400 standards established by BHBSS	<ul style="list-style-type: none"> Users could gain unauthorized access to information assets 	<ul style="list-style-type: none"> Have the system administrator print the system parameters listing: DSPNETA OUTPUT (*PRINT) Reconcile system parameters to BHBSS's AS/400 standards 		
	Programs should not be able to adopt and give authority to users who should not have such authority.	<ul style="list-style-type: none"> Unauthorized users will have more authority to change system values and user profiles 	<ul style="list-style-type: none"> Generate a list of programs that adopt powerful user capabilities: DSPPGMADP USRPRF (name of profile) 	<ul style="list-style-type: none"> 	
	Audit logs should activated and reviewed regularly to insure the system has not been accessed by inappropriate users	<ul style="list-style-type: none"> Unauthorized users could gain access to the system and go undetected if the audit logs are not reviewed Under-auditing may lead to a lack of security. Over-auditing may lead to a lack of system performance 	<ul style="list-style-type: none"> Interview the security administrator to determine the review procedure and frequency of the audit logs Determine the types of security related activities the system is monitoring: DPSYSVAL SYSVAL (QAUDLVL) Suggested values: *AUTFAIL, *PGMFAIL, * SECURITY Avoid: *PGMADP, *SPLFDTA 	<ul style="list-style-type: none"> 	
	Auditing should be activated on appropriate levels.	<ul style="list-style-type: none"> Unauthorized access may go undetected. 	<ul style="list-style-type: none"> Determine the value of auditing control: DPSYSVAL SYSVAL (QAUDCTL) 	<ul style="list-style-type: none"> 	
	Users should review the use of their usernames and report attempts at inappropriate access	<ul style="list-style-type: none"> Unauthorized access using an established user profile could go undetected 	<ul style="list-style-type: none"> Determine the value of display user sign-on information: DPSYSVAL SYSVAL (QDSPGNINF) (1 = Display, 0 = No Display) 	<ul style="list-style-type: none"> 	

Program Section	Specific Control Objectives	Risk Effect(s)	Audit Tests Performed	Results	Workpaper
	User inactivity on the system should be limited	<ul style="list-style-type: none"> Systems that are open and inactive provide unauthorized users the ability to gain access without signing on to a system 	<ul style="list-style-type: none"> Determine the value of the inactive interval: DSPSYSVAL SYSVAL (QINACTITV) Value should be 30 minutes or less Determine the value of the inactive command: DSPSYSVAL SYSVAL (QINACTMSGQ) Recommended value: *DSCJOB 	<ul style="list-style-type: none"> 	
	Users should sign on at only one device. If users require more than one session, this can be overridden in their user profile.	<ul style="list-style-type: none"> Unauthorized access by an inappropriately obtained username would be prevented 	<ul style="list-style-type: none"> Determine the value for limiting device sessions: DSPSYSVAL SYSVAL (QLMTDEVSSN) 0 = More than one; 1 = One device 	<ul style="list-style-type: none"> 	
	Data required to validate a user should only be available on the server	<ul style="list-style-type: none"> User validation information may be removed from the client workstation and used to obtain access to the server 	<ul style="list-style-type: none"> Determine the value of the retain server security data system value: DSPSYSVAL SYSVAL (QRETSVRSEC) 0 (Recommended) = off; 1 = on 	<ul style="list-style-type: none"> 	
	Verification of remote users should be performed	<ul style="list-style-type: none"> Unauthorized users may gain access to information on other servers without proper verification 	<ul style="list-style-type: none"> Determine the value for remote sign-on control: DSPSYSVAL SYSVAL (QRMTSIGN) Recommended value: *FRCSIGNON 	<ul style="list-style-type: none"> 	
	Each person authorized to use the system should have their own user profile assigned to them and usernames should not be shared.	<ul style="list-style-type: none"> Shared or group usernames leads to the inability to monitor and track the use of usernames and user authorities. 	<ul style="list-style-type: none"> Interview the security administrator to determine if group usernames are being used. Examine a list of usernames to look for group usernames 	<ul style="list-style-type: none"> 	

Program Section	Specific Control Objectives	Risk Effect(s)	Audit Tests Performed	Results	Workpaper
	Initial passwords should be established by appropriate security personnel, be different than the username, and be difficult to guess	<ul style="list-style-type: none"> Improper access to initial password establishment and weak initial passwords can lead to unauthorized access 	<ul style="list-style-type: none"> Using system values, determine who has the authority to create new users and assign new passwords Interview the person responsible for setting initial passwords and determine the methodology used 	<ul style="list-style-type: none"> 	
	All user profiles should be members of at least one group for the purpose of owning objects and simplifying authorization to objects. Users should generally not own objects. Note that objects created in Shared Folders default to ownership by the individual who creates them regardless of membership in a group. Manual ownership change is required.	<ul style="list-style-type: none"> Creating individual profiles makes administration of users difficult Allowing individuals to own objects makes removing user profiles difficult. 	<ul style="list-style-type: none"> Review users membership to groups 	<ul style="list-style-type: none"> 	
	Application system software (e.g. JD Edwards, ASI, Software 2000) should not be run with a user profile with *ALLOBJ authority in order to manage the application and/or application objects. It is also a common practice for these applications to have a user profile that owns all objects related to the processing of the application. Use of these user profiles should be restricted through the Password =*None (no sign-on capability) except on a very limited basis where required	<ul style="list-style-type: none"> Programs could have too much system access and improperly provide that system access to users User profiles for programs provide access to system capabilities and should not be available as logons 	<ul style="list-style-type: none"> Review user profiles for application system software and determine authority Determine the passwords for these user profiles 	<ul style="list-style-type: none"> 	

Program Section	Specific Control Objectives	Risk Effect(s)	Audit Tests Performed	Results	Workpaper
	Vendors system access should be limited including only special situational use of the security officer or the security administrator profiles.	<ul style="list-style-type: none"> Vendors with significant access may gain access to confidential data 	<ul style="list-style-type: none"> Determine if vendors have accessed the system. Examine the user profiles used by vendors Determine if the vendor ID's were appropriate 	<ul style="list-style-type: none"> 	
	Vendor contracts should contain clauses that require vendors to adhere to established best practices, policies and procedures that maybe monitored and violations or non-compliance leading to potential termination of contract	<ul style="list-style-type: none"> Contracts without specific clauses for policy adherence and monitoring leave the company little recourse in the event of a loss of data 	<ul style="list-style-type: none"> Determine if vendors have accessed the system. Obtain a copy of vendor contracts Review vendor contracts for clauses that require policy adherence and monitoring with repercussions to include potential termination of contracts 	<ul style="list-style-type: none"> 	
	Vendor profiles should be disabled after contracts are completed or terminated	<ul style="list-style-type: none"> Vendor profiles that are not disabled are entry points for unauthorized access to information 	<ul style="list-style-type: none"> Determine if vendors have used the system Review vendor profiles and determine if these profiles have been disabled or deleted 	<ul style="list-style-type: none"> 	
	Automatic sign-on from workstations should be disabled	<ul style="list-style-type: none"> Automatic sign-ons allow users to access the system without using a username or password 	<ul style="list-style-type: none"> Observe users accessing the system to determine if automatic sign-ons are enabled 	<ul style="list-style-type: none"> 	
6220	Access to hubs, switches, and routers should be limited to approved personnel	<ul style="list-style-type: none"> Unauthorized access to hubs, switches, and routers provides is an opportunity for unauthorized access to information or accidental damage 	<ul style="list-style-type: none"> Examine the location, security, and environmental protection of hubs, switches, and routers 	<ul style="list-style-type: none"> 	

Program Section	Specific Control Objectives	Risk Effect(s)	Audit Tests Performed	Results	Workpaper
	Double redundancy of key infrastructure equipment should be in place to reduce or eliminate downtime. Servers should have a minimum of RAID-5 fail-over, but mirroring is preferred.	<ul style="list-style-type: none"> Significant downtime may lead to loss of critical information 	<ul style="list-style-type: none"> Examine and determine if double redundancy exists for key infrastructure components 	<ul style="list-style-type: none"> 	
	Operating systems should be using a supported version with all appropriate system patches installed	<ul style="list-style-type: none"> Technical support may not be available for systems Unauthorized users may be able to exploit published security weaknesses 	<ul style="list-style-type: none"> Determine the operating system version and if it is being supported Determine the version of patches installed and the latest version available and reconcile the results 	<ul style="list-style-type: none"> 	
	Physical access to the master console should be limited to authorized users	<ul style="list-style-type: none"> Unauthorized users can gain access to the system because users do not need a password to obtain access to the system at the master console 	<ul style="list-style-type: none"> Review physical access to the master console 	<ul style="list-style-type: none"> 	
	Access to AS/400 key should be limited	<ul style="list-style-type: none"> Access to the AS/400 key may provide complete system access 	<ul style="list-style-type: none"> Ensure the security key is set to "Secure" or "Auto" and stored in a secure location with the backup key in a separate secure location 	<ul style="list-style-type: none"> 	
	The computer room should have adequate environmental safeguards to ensure systems are free of physical danger	<ul style="list-style-type: none"> Information assets may be lost if computers are exposed to physical danger 	<ul style="list-style-type: none"> Perform the server room checklist 	<ul style="list-style-type: none"> 	<ul style="list-style-type: none">
	Adequate backup procedures should be in place and performed to ensure recovery of information assets.	<ul style="list-style-type: none"> Information assets could be lost due to system failure or natural disaster 	<ul style="list-style-type: none"> Obtain a copy of the backup policies and procedures Obtain a copy of the backup tape log and trace tapes to the log 	<ul style="list-style-type: none"> 	

Program Section	Specific Control Objectives	Risk Effect(s)	Audit Tests Performed	Results	Workpaper
	On-site storage tapes are secure	<ul style="list-style-type: none"> Information assets could be lost due to negligence, misappropriation or natural disaster 	<ul style="list-style-type: none"> Observe the storage location of the on-site backup tapes 	<ul style="list-style-type: none"> 	
	Backup tapes are taken to a secure off-site location at least one-mile from the facility on a weekly basis	<ul style="list-style-type: none"> Information assets could be lost due to natural disaster 	<ul style="list-style-type: none"> Determine the process and frequency of backups to be rotated to an off-site storage facility. Determine the location and adequacy of the off-site location 	<ul style="list-style-type: none"> 	
	Backup tapes should be properly rotated to ensure compliance with Document Retention Policy	<ul style="list-style-type: none"> Documents may be destroyed before the required date – company may be liable for obstruction Documents are kept longer than required – company records may provide basis for legal actions 	<ul style="list-style-type: none"> Determine the backup file rotation Determine the information contained on the backup tapes Compare to Document Retention Policy 	<ul style="list-style-type: none"> 	
	The facility should be able to restore processing in the event of a hardware system failure within a reasonable period of time	<ul style="list-style-type: none"> Inability to quickly restore system processing could lead to a disruption of normal business processes 	<ul style="list-style-type: none"> Evaluate the plans and procedures for restoring operations in the event of a hardware failure Determine the fail-safe capabilities of the hardware 	<ul style="list-style-type: none"> 	

Program Section	Specific Control Objectives	Risk Effect(s)	Audit Tests Performed	Results	Workpaper
	<p>The facility should have an adequate disaster recovery plan to restore processing in the event of a disaster</p>	<ul style="list-style-type: none"> A significant disruption of business operations may occur in the event of a disaster 	<ul style="list-style-type: none"> Obtain a copy of the disaster recovery plan Review the disaster recovery plan for adequacy, timeliness, and scope Determine if a copy of the plan is stored off-site with the backup tapes Determine if the plan has been tested within the previous twelve (12) months 	<ul style="list-style-type: none"> 	