Title	Control Number	Control Detail / Description	Control Attributes	Control Frequency	Risk	Control Name	Process
ITAS	ITAS-001	Application user access is approved by management before access is granted	A. User's access request was approved by appropriate management. B. Access was approved prior to access being provisioned. C. Access provisioned was consistent with access approved.	Many times per day	High	IT Application Security	New User Provisioning Review
ITAS	ITAS-002	Application user access is revoked upon employment termination or contract/vendor termination	A. User has been promptly deleted or disabled (within 5 business days of termination). B. Documentation exists and Management submitted the termination request (i.e. through email or appropriate request forms).	Many times per day	High	IT Application Security	Termination Requests
ITAS	ITAS-003	Application passwords are configured according to company policy	A. Obtain management's review of the password parameters and verify agree to company's password policy or there is an approved policy exception: - password minimum length (8), - complexity (enabled), - expiration (90 days), - account lockout (5), - password history (8). B. Verify that default passwords are changed to adhere to Brinks password policy. C. Determine the completeness and accuracy of the report utilized to perform the review. D. Verify that any corrections to the password is performed within 10 business days. If Additional time is required, a policy exception form must be filed and approved. E. Verify an appropriate risk assessment was performed for any parameters not in compliance with company's password policy or approved policy exception. F. Verify that the review was done within 120 days of the year-end.	Ad-hoc	High	IT Application Security	Password Requirement
ITAS	ITAS-004	All Application accounts (excluding read-only) and associated privileges for Key Financial Applications are reviewed on a quarterly basis. Modification/removal requests are made and confirmed in 10 business days	A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate personnel with proper segregation of duties enforced. -Managers or delegates performing reviews. -Privileged/administrative accounts are reviewed for appropriateness. -Reviewers are not performing self reviews (including service/shared/system accounts). B. Determine whether all users were reviewed (excluding read-only). C. Determine whether the user report was generated within the quarter of review. D. Modification/removal requests are made and confirmed in 10 business days. E. Determine the completeness and accuracy of the user report utilized to perform the review. F. Inappropriate access identified as a result of the user access review is investigated to determine if unauthorized tasks or functions were performed. (Lookback procedure) (Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)). G. Determine if system/generic accounts are reviewed by a primary reviewer and includes a secondary reviewer if the primary reviewer knows the password to the system/generic account). H. Determine if system/generic accounts have a brief description of the account and who all knows the password to that account.	Quarterly	High	IT Application Security	User Access Reviews
ITBK	ITBK-001	Backups of GL systems/database(s) are configured to be backed up according to Brink's company policy, standard, or procedure. In an event of a key financial job failure, proper procedures are in place to ensure resolution. Failed jobs are resolved accordingly.	A. Backups are configured/scheduled according to Brink's Company policy, standard, or procedure. B. Full/Incremental backup occur for each in-scope system. C. Back-up job failures of the GL Systems/Databases are monitored and followed up to a resolution.	Daily/Weekly	Medium	IT Backup	Backups
ITDB	ITDB-003	Database passwords are configured according to company policy.	A. Obtain management's review of the password parameters and verify agree to company's password policy or there is an approved policy exception: - password minimum length (8), - complexity (enabled), - expiration (90 days), - account lockout (5), - password history (8). B. Verify that default passwords are changed to adhere to Brinks password policy. C. Determine the completeness and accuracy of the report utilized to perform the review. D. Verify that any corrections to the password is performed within 10 business days. If Additional time is required, a policy exception form must be filed and approved. E. Verify an appropriate risk assessment was performed for any parameters not in compliance with company's password policy or approved policy exception. F. Verify that the review was done within 120 days of the year-end.	Ad-hoc	High	IT Database	Password Requirement
ITDB	ITDB-004	All database accounts (excluding read-only) with access to Key Financial databases is reviewed on a quarterly basis by appropriate IT management or a qualified delegate. Modification/removal requests are made and confirmed in 10 business days	A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate personnel with proper segregation of duties enforced. -Managers or delegates performing reviews -Privileged/administrative accounts are reviewed for appropriateness -Reviewers are not performing self-reviews (including service/shared/system accounts) B. Determine whether all users were reviewed (excluding read-only accounts) C. Determine whether the user report was generated within the quarter of review D. Modification/removal requests are made and confirmed in 10 business days. E. Determine the completeness and accuracy of the user report utilized to perform the review. F. Inappropriate access identified as a result of the user access review is investigated to determine if unauthorized tasks or functions were performed. (Lookback procedure) (Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)). G. Determine if system/generic accounts are reviewed by a primary reviewer and includes a secondary reviewer if the primary reviewer knows the password to the system/generic account) H. Determine if system/generic accounts have a brief description of the account and who all knows the password to that account.	Quarterly	High	IT Database	User Access Reviews
ITNS	ITNS-002	(Global) Active Directory user access is revoked promptly (within 5 business days) of employment termination or contractor/vendor termination	A. User has been promptly deleted or disabled (within 5 business days of termination). B. Documentation exists and Management submitted the termination request (i.e. though email or appropriate request forms).	Many times per day	High	IT Network Security	Termination Requests
ITNS	ITNS-003	Active Directory passwords are configured according to company policy.	A. Obtain management's review of the password parameters and verify agree to company's password policy or there is an approved policy exception: - password minimum length (8), - complexity (enabled), - expiration (90 days), - account lockout (5), - password history (8). B. Verify that default passwords are changed to adhere to Brinks password policy. C. Determine the completeness and accuracy of the report utilized to perform the review. D. Verify that any corrections to the password is performed within 10 business days. If Additional time is required, a policy exception form must be filed and approved. E. Verify an appropriate risk assessment was performed for any parameters not in compliance with company's password policy or approved policy exception. F. Verify that the review was done within 120 days of the year-end	Ad-hoc	High	IT Network Security	Password Requirement
ITNS	ITNS-004	Active Directory domain-wide administrative security groups are reviewed on a quarterly basis by IT management or a qualified delegate. Modification/removal requests are made and confirmed in 10 business days.	A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate personnel with proper segregation of duties enforced. -Managers or delegates performing reviews. -Privileged/administrative accounts are reviewed for appropriateness. -Reviewers are not performing self reviews (including service/shared/system accounts). B. Determine whether all users were reviewed (excluding read-only accounts). C. Determine whether the user report was generated within the quarter of review. D. Modification/removal requests are made and confirmed in 10 business days. E. Determine the completeness and accuracy of the user report utilized to perform the review. F. Inappropriate access identified as a result of the user access review is investigated to determine if unauthorized tasks or functions were performed. (Lookback procedure). (Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)). G. Determine if system/generic accounts are reviewed by a primary reviewer and includes a secondary reviewer if the primary reviewer knows the password to the system/generic account). H. Determine if system/generic accounts have a brief description of the account and who all knows the password to that account.	Quarterly	High	IT Network Security	User Access Reviews
ITOS	ITOS-003	Operating system passwords are configured according to company policy.	A. Obtain management's review of the password parameters and verify agree to company's password policy or there is an approved policy exception: - password minimum length (8), - complexity (enabled), - expiration (90 days), - account lockout (5), - password history (8). B. Verify that default passwords are changed to adhere to Brinks password policy. C. Determine the completeness and accuracy of the report utilized to perform the review. D. Verify that any corrections to the password is performed within 10 business days. If Additional time is required, a policy exception form must be filed and approved. E. Verify an appropriate risk assessment was performed for any parameters not in compliance with company's password policy or approved policy exception. F. Verify that the review was done within 120 days of the year-end	Ad-hoc	Medium	IT Operating System	Password Requirement
ITOS	ITOS-004	Elevated/administrative User accounts (including system/generic accounts) and access rights to the operating system supporting key financial systems are reviewed quarterly. Modification/removal requests are made and confirmed in 10 business days.	A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate personnel with proper segregation of duties enforced. -Managers or delegates performing reviews. -Privileged/administrative accounts are reviewed for appropriateness. -Reviewers are not performing self reviews (including service/shared/system accounts). B. Determine whether all users were reviewed (excluding read-only accounts). C. Determine whether the user report was generated within the quarter of review D. Modification/removal requests are made and confirmed in 10 business days. E. Determine the completeness and accuracy of the user report utilized to perform the review. F. Inappropriate access identified as a result of the user access review is investigated to determine if unauthorized tasks or functions were performed. (Lookback procedure) (Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)). G. Determine if system/generic accounts are reviewed by a primary reviewer and includes a secondary reviewer if the primary reviewer knows the password to the system/generic account). H. Determine if system/generic accounts have a brief description of the account and who all knows the password to that account.	Quarterly	High	IT Operating System	User Access Reviews
ITAD	ITAD-001	Access to migrate changes to production envirnonments for key financial systems is restricted to personnel with non-development responsiblities	A. A comparison is performed between the system generated list of developers and system generated listing of migrators is not a member on the migrator list. B. Determine the completeness and accuracy of the report utilized to perform the review. C. Inappropriate access (developers having access to migrate code to production) identified as a result the comparison is investigated to determine if unauthorized tasks or changes were performed. (Lookback procedure) (Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)).	Ad-hoc	High	IT Application Development	Change Management (Access to Production)
ITAD	ITAD-001.1	(US Only) - On an Annual basis, IT Management will review the key configurations and security administrator access for the STAT tool.	A. Changes are tested successfully prior to being implemented into production. B. Authorized stakeholder commensurate with the entity's IT DOA approve the test results prior to implementation. (NOTE: Test results do not necessarily need separate "approval", but testing needs to be completed by appropriate personnel and completion should be documented.) C. Changes are approved prior to being implemented into production. D. The business/IT authorized user commensurate with the entity's IT DOA provides final approval to implement the change into production.	Annually	High	IT Application Development	Change Management (US Only)
ITAD	ITAD-002	Changes to Key Financial Applications and/or supporting infrastructure are properly tested and approved prior to being promoted to production (Changes include standard, emergency, and patching to all layers supporting Key Financial systems).	A. Determine change was authorized by the appropriate business owner. B. Determine change was tested (system, UAT) prior to moving into production and evidence of testing was maintained. C. Determine change was approved by appropriate management prior to it being promoted into production.	Daily (Determined by Total Population)	High	IT Application Development	Change Management
ITAS	ITAS-002.1	Reviews of terminated users with access to Key Financial Applications are performed by the last business day of the month	A. Determine whether the active application user report was generated by the last business day of the month. B. Terminated users on HR termination listing (of the same month) are crossed referenced to the active application user listing on a monthly basis. C. Inappropriate access identified as a result of the assessment is disabled immediately and is investigated to determine if unauthorized tasks or functions were performed (Lookback procedure). (Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)). D. Verify the review was performed within 10 business days. E. Determine the completeness and accuracy of the active application user and HR termination reports utilized to perform the assessment. (Include a screenshot of the query/parameters/process used to generate this listing. Include the time and date stamp of your computer screen is included in the screenshot.)			IT Application Security	Termination Requests
ITAD	ITAD-001.2	Access to migrate changes to all production environments (production servers and databases) for Key Financial systems is restricted to personnel with non-development responsibilities is reviewed bi-annually.	A. Access to production servers and databases is reviewed to determine if each account (including generic accounts) is a developer or has development capabilities. B. Determine the completeness and accuracy of the user report utilized to perform the review. C. Inappropriate access (developers having access to migrate code to production) identified as a result the comparison is investigated to determine if unauthorized tasks or changes were performed. (Lookback procedure (Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)).			IT Application Development	Change Management
ITNS	ITNS-002.1	(Global) Reviews of terminated users with access to AD are performed by the last business day of the month.	A. Determine whether the AD user report was generated by the last business day of the month. B. Terminated users on HR termination listing (of the same month) are crossed referenced to the AD user listing on a monthly basis. C. Inappropriate access identified as a result of the assessment is disabled immediately and is investigated to determine if unauthorized tasks or functions were performed (Lookback procedure). (Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)). D. Verify the review was performed within 10 business days. E. Determine the completeness and accuracy of the AD user and HR termination reports utilized to perform the assessment. (Include a screenshot of the query/parameters/process used to generate this listing. Include the time and date stamp of your computer screen is included in the screenshot.)			IT Network Security	Termination Requests
ITNS	ITNS-002.1	(US - Automated) The system is configured to revoke terminated user's AD access every 12 hours (Contingent upon the business process completion date) provided by Workday.	A. Obtain screenshot and evidence of configuration showing the tool is configured to disable an employee's AD access upon termination.			IT Network Security	Termination Requests
ITNS	ITNS-002.2	(US) A monthly termination report is automatically sent to (TBD) to determine if there exist any terminated employees whose Business Process approvals were completed after 5 days of their termination date. If so, an impact analysis is performed.	A. A monthly termination report is automatically sent to the appropriate personnel to determine if there exist any terminated employees who's Business Process approvals was completed after 5 days of their termination date. If so, an impact analysis is performed. B. Determine the impact analysis identified all terminated employees whose Business Process approvals were completed after 5 days of their termination date. C. Impact analysis was performed accurately. (lookback procedure) (Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)). D. Determine the completeness and accuracy of the HR user report utilized to perform the assessment. (Include a screenshot of the query/parameters/process used to generate this listing. Include the time and date stamp of your computer screen is included in the screenshot.).			IT Network Security	Termination Requests
ITJS	ITJS-001	All Application Accounts (excluding read-only) and associated privileges for key financial Jobs are reviewed on a quarterly basis. Modification/removal requests are made and confirmed in 10 business days.	A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate personnel with proper segregation of duties enforced. -Managers or delegates performing reviews. -Reviewers are not performing self-reviews (including service/shared/system accounts). -privileged/administrative accounts are reviewed for appropriateness. B. Determine whether all users were reviewed. C. Determine whether the user report was generated within the quarter of review. D. Modification/removal requests are made and confirmed in 10 business days. E. Determine the completeness and accuracy of the user report utilized to perform the review. F. Inappropriate access identified as a result of the user access review is investigated to determine if unauthorized tasks or functions were performed. (Lookback procedure). (Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)). G. Determine if system/generic accounts are reviewed by a primary reviewer and includes a secondary reviewer if the primary reviewer knows the password to the system/generic account). H. Determine if system/genic accounts have a brief description of the account and who all knows the password to that account. I. Roles and privileges that enables users to modify/delete/add jobs are reviewed.			IT Job Systems	Key Financial Job Systems
ITJS	ITJS-001.2	In an event of a key financial job failure, proper procedures are in place to ensure resolution. Failed jobs are resolved within 5 business days.	A. Job failures are monitored and followed up to resolution (within 5 business days).			IT Job Systems	Key Financial Job Systems