le Control Number	Control Detail / Description	Control Attributes A. User's access request was approved by appropriate management. B. Access was approved prior to access being provisioned.	Control Frequency	Risk Control Name	Process
S ITAS-001	Application user access is approved by management before access is granted	<ul><li>C. Access provisioned was consistent with access approved.</li><li>A. User has been promptly deleted or disabled (within 5 business days of termination).</li></ul>	Many times per day	High IT Application Security	New User Provisioning Review
AS ITAS-002	Application user access is revoked upon employment termination or contract/vendor 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
TAS ITAS-002		<ul> <li>A. Obtain management's review of the password parameters and verify agree to company's password policy or there is an approved policy exception:</li> <li>password minimum length (8),</li> <li>complexity (enabled),</li> <li>expiration (90 days),</li> <li>account lockout (5),</li> </ul>			
		<ul> <li>password history (8).</li> <li>B. Verify that default passwords are changed to adhere to Brinks password policy.</li> <li>C. Determine the completeness and accuracy of the report utilized to perform the review.</li> <li>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.</li> <li>E. Verify an appropriate risk assessment was performed for any parameters not in compliance with company's password policy or approved policy exception.</li> </ul>			
5 ITAS-003	Application passwords are configured according to company policy	F. Verify that the review was done within 120 days of the year-end.	Ad-hoc	High IT Application Security	Password Requirement
		<ul> <li>A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate personnel with proper segregation of duties enforced.</li> <li>-Managers or delegates performing reviews.</li> <li>-Privileged/administrative accounts are reviewed for appropriateness.</li> <li>-Reviewers are not performing self reviews (including service/shared/system accounts).</li> <li>B. Determine whether all users were reviewed (excluding read-only).</li> <li>C. Determine whether the user report was generated within the quarter of review.</li> <li>D. Modification/removal requests are made and confirmed in 10 business days.</li> <li>E. Determine the completeness and accuracy of the user report utilized to perform the review.</li> <li>F. Inappropriate access identified as a result of the user access review is investigated to determine if</li> </ul>			
		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)).			
	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	<ul><li>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).</li><li>H. Determine if system/generic accounts have a brief description of the account and who all knows the</li></ul>			
5 ITAS-004	Backups of CL systems (database(s) are configured to be backed up according to Brink's company	password to that account.	Quarterly	High IT Application Security	User Access Reviews
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.	<ul> <li>A. Backups are configured/scheduled according to Brink's Company policy, standard, or procedure.</li> <li>B. Full/Incremental backup occur for each in-scope system.</li> <li>C. Back-up job failures of the GL Systems/Databases are monitored and followed up to a resolution.</li> </ul>	Daily/Weekly	Medium IT Backup	Backups
		<ul> <li>A. Obtain management's review of the password parameters and verify agree to company's password policy or there is an approved policy exception: <ul> <li>password minimum length (8),</li> <li>complexity (enabled),</li> <li>expiration (90 days),</li> <li>account lockout (5),</li> <li>password history (8).</li> </ul> </li> <li>B. Verify that default passwords are changed to adhere to Brinks password policy.</li> <li>C. Determine the completeness and accuracy of the report utilized to perform the review.</li> <li>D. Verify that any corrections to the password is performed within 10 business days. If Additional time</li> </ul>			
		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			
3 ITDB-003	Database passwords are configured according to company policy.	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
		<ul> <li>A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate personnel with proper segregation of duties enforced.</li> <li>-Managers or delegates performing reviews</li> <li>-Privileged/administrative accounts are reviewed for appropriateness</li> <li>-Reviewers are not performing self-reviews (including service/shared/system accounts)</li> <li>B. Determine whether all users were reviewed (excluding read-only accounts)</li> <li>C. Determine whether the user report was generated within the quarter of review</li> <li>D. Modification/removal requests are made and confirmed in 10 business days.</li> <li>E. Determine the completeness and accuracy of the user report utilized to perform the review.</li> <li>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)</li> <li>(Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)).</li> <li>G. Determine if system/generic accounts are reviewed by a primary reviewer and includes a secondary</li> </ul>			
B 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	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-002	(Global) Active Directory user access is revoked promptly (within 5 business days) of employment termination or contractor/vendor termination	<ul> <li>A. User has been promptly deleted or disabled (within 5 business days of termination).</li> <li>B. Documentation exists and Management submitted the termination request (i.e. though email or appropriate request forms).</li> </ul>	Many times per day	High IT Network Security	Termination Requests
		<ul> <li>policy or there is an approved policy exception:</li> <li>password minimum length (8),</li> <li>complexity (enabled),</li> <li>expiration (90 days),</li> <li>account lockout (5),</li> <li>password history (8).</li> </ul>			
ITNS-003	Active Directory passwords are configured according to company policy.	<ul> <li>B. Verify that default passwords are changed to adhere to Brinks password policy.</li> <li>C. Determine the completeness and accuracy of the report utilized to perform the review.</li> <li>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.</li> <li>E. Verify an appropriate risk assessment was performed for any parameters not in compliance with company's password policy or approved policy exception.</li> <li>F. Verify that the review was done within 120 days of the year-end</li> </ul>	Ad-hoc	High IT Network Security	Password Requirement
ITNS-003	Active Directory passwords are configured according to company policy.	<ul> <li>C. Determine the completeness and accuracy of the report utilized to perform the review.</li> <li>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.</li> <li>E. Verify an appropriate risk assessment was performed for any parameters not in compliance with company's password policy or approved policy exception.</li> <li>F. Verify that the review was done within 120 days of the year-end</li> <li>A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate personnel with proper segregation of duties enforced.</li> <li>-Managers or delegates performing reviews.</li> <li>-Privileged/administrative accounts are reviewed for appropriateness.</li> <li>-Reviewers are not performing self reviews (including service/shared/system accounts).</li> <li>B. Determine whether all users were reviewed (excluding read-only accounts).</li> <li>C. Determine whether the user report was generated within the quarter of review.</li> <li>D. Modification/removal requests are made and confirmed in 10 business days.</li> <li>E. Determine the completeness and accuracy of the user report utilized to perform the review.</li> <li>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).</li> <li>(Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)).</li> </ul>		High IT Network Security	Password Requirement
	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	<ul> <li>C. Determine the completeness and accuracy of the report utilized to perform the review.</li> <li>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.</li> <li>E. Verify an appropriate risk assessment was performed for any parameters not in compliance with company's password policy or approved policy exception.</li> <li>F. Verify that the review was done within 120 days of the year-end</li> <li>A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate personnel with proper segregation of duties enforced.</li> <li>-Managers or delegates performing reviews.</li> <li>-Privileged/administrative accounts are reviewed for appropriateness.</li> <li>-Reviewers are not performing self reviews (including service/shared/system accounts).</li> <li>B. Determine whether all users were reviewed (excluding read-only accounts).</li> <li>C. Determine the completeness and accuracy of the user report utilized to perform the review.</li> <li>F. Inappropriate access identified as a result of the user report utilized to perform the review.</li> <li>F. Inappropriate access identified as a result of the user serview is investigated to determine if unauthorized tasks or functions were performed. (Lookback procedure).</li> <li>(Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)).</li> <li>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).</li> <li>H. Determine if system/generic accounts have a brief description of the account and who all knows the</li> </ul>	Ad-hoc		
	Active Directory domain-wide administrative security groups are reviewed on a quarterly basis by IT	<ul> <li>C. Determine the completeness and accuracy of the report utilized to perform the review.</li> <li>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.</li> <li>E. Verify an appropriate risk assessment was performed for any parameters not in compliance with company's password policy or approved policy exception.</li> <li>F. Verify that the review was done within 120 days of the year-end</li> <li>A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate personnel with proper segregation of duties enforced.</li> <li>-Managers or delegates performing reviews.</li> <li>-Privileged/administrative accounts are reviewed for appropriateness.</li> <li>-Reviewers are not performing self reviews (including service/shared/system accounts).</li> <li>C. Determine whether all users were reviewed (excluding read-only accounts).</li> <li>C. Determine whether all users were reviewed (excluding read-only accounts).</li> <li>C. Determine whether all users were reviewed (excluding read-only accounts).</li> <li>C. Determine whether all users were reviewed (excluding read-only accounts).</li> <li>E. Determine the completeness and accuracy of the user access review is investigated to determine if unauthorized tasks or functions were performed. (Lookback procedure).</li> <li>(Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)).</li> <li>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).</li> <li>H. Determine if system/generic accounts have a brief description of the account and who all knows the password to that account.</li> <li>A. Obtain management's review of the password parameters and verify agree to company's password</li></ul>	Ad-hoc	High       IT Network Security         High       IT Network Security	Password Requirement
5 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	<ul> <li>C. Determine the completeness and accuracy of the report utilized to perform the review.</li> <li>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.</li> <li>E. Verify an appropriate risk assessment was performed for any parameters not in compliance with company's password policy or approved policy exception.</li> <li>F. Verify that the review was done within 120 days of the year-end</li> <li>A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate personnel with proper segregation of duties enforced.</li> <li>-Managers or delegates performing reviews.</li> <li>-Privileged/administrative accounts are reviewed for appropriateness.</li> <li>-Reviewers are not performing self reviews (including service/shared/system accounts).</li> <li>B. Determine whether all users were reviewed (excluding read-only accounts).</li> <li>C. Determine whether the user report was generated within the quarter of review.</li> <li>D. Modification/removal requests are made and confirmed in 10 business days.</li> <li>E. Determine the completeness and accuracy of the user access review is investigated to determine if unauthorized tasks or functions were performed. (Lookback procedure).</li> <li>(Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)).</li> <li>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).</li> <li>A. Obtain management's review of the password parameters and verify agree to company's password policy or there is an approved policy exception:         <ul> <li>password to that account.</li> </ul> </li> <li>A. Obtain management's review of the password parameters and verify agree to company's password policy or</li></ul>	Ad-hoc		
5 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.	<ul> <li>C. Determine the completeness and accuracy of the report utilized to perform the review.</li> <li>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.</li> <li>E. Verify an appropriate risk assessment was performed for any parameters not in compliance with company's password policy or approved policy exception.</li> <li>F. Verify that the review was done within 120 days of the year-end</li> <li>A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate personnel with proper segregation of duties enforced.</li> <li>-Managers or delegates performing reviews.</li> <li>-Privileged/administrative accounts are reviewed for appropriateness.</li> <li>-Reviewers are not performing self reviews (including service/shared/system accounts).</li> <li>C. Determine whether all user report was generated within the quarter of review.</li> <li>D. Modification/removal requests are made and confirmed in 10 business days.</li> <li>E. Determine the completeness and accuracy of the user report utilized to perform the review.</li> <li>F. Inappropriate access identified as a result of the user report utilized to perform the review.</li> <li>F. Inappropriate access identified as a reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure).</li> <li>(Note: Log-in monitoring activities are reviewed for a primary reviewer and includes a secondary reviewer if the primary reviewer knows the password to the system/generic account.</li> <li>A. Obtain management's review of the password parameters and verify agree to company's password policy or there is an approved policy exception:         <ul> <li>password history (8).</li> <li>account lockourt (5).</li> <li>password bistory (8).</li> <li>Sverify that default passwords are changed to adhere to Brinks password policy.</li> <li>Determine the completeness and accuracy of the</li></ul></li></ul>	Ad-hoc	High IT Network Security	User Access Reviews
ITOS-003	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.	<ul> <li>C. Determine the completeness and accuracy of the report utilized to perform the review.</li> <li>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.</li> <li>E. Verify an appropriate risk assessment was performed for any parameters not in compliance with company's password policy or approved policy exception.</li> <li>F. Verify that the review was done within 120 days of the year-end</li> <li>A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate personnel with proper segregation of duties enforced.</li> <li>Managers or delegates performing reviews.</li> <li>Privileged/administrative accounts are reviewed for appropriateness.</li> <li>Reviewers are not performing self reviews (including service/shared/system accounts).</li> <li>B. Determine whether all users were reviewed (excluding read-only accounts).</li> <li>C. Determine whether all users are made and confirmed in 10 business days.</li> <li>E. Determine the completeness and accuracy of the user report utilized to perform the review.</li> <li>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).</li> <li>(Note: Log in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure) documentation).</li> <li>G. Determine if system/genetic accounts are reviewed by apirany reviewer and includes a secondary reviewer if the primary reviewer if the password bothe account.</li> <li>A. Obtain management's review of the password parameters and verify agree to company's password policy or there is an approved policy exception:         <ul> <li>password bits (9).</li> <li>account lockout (5).</li> <li>password bits (9).</li> <li>password bits (9).</li> <li>pactivity (190 days).</li> <li>account lockout (5</li></ul></li></ul>	Ad-hoc Quarterly Ad-hoc	High IT Network Security	User Access Reviews
ITOS-003	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.	<ul> <li>C. Determine the completeness and accuracy of the report utilized to perform the review.</li> <li>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.</li> <li>F. Verify that the review was done within 120 days of the year-end</li> <li>A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate personal with proper segregation of duties enforced.</li> <li>Managers or delegates performing reviews.</li> <li>Privileged/administrative accounts are reviewed for appropriateness.</li> <li>Reviewers are not performing services of the user report utilized to perform the review.</li> <li>D. Determine whether a review of an accuracy of the user report utilized to perform the review.</li> <li>D. Determine whether the user report was generated within the quarter of review.</li> <li>D. Determine whether the user report was generated within the quarter of review.</li> <li>D. Determine whether the user report was generated within the quarter of review.</li> <li>D. Determine whether the user report was generated within the quarter of review.</li> <li>D. Determine whether the user cocounts are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure).</li> <li>(Note: Log in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation).</li> <li>D. Determine fly system/generic accounts are reviewed by a primary reviewer and includes a secondary.</li> <li>P. Determine fly system/generic accounts are reviewed by a primary reviewer and includes a secondary.</li> <li>P. Determine fly system/generic accounts are reviewed by a primary reviewer and includes a secondary.</li> <li>P. Determine fly system/generic accounts are reviewed by a primary reviewer a</li></ul>	Ad-hoc Ad-hoc	High IT Network Security Medium IT Operating System	User Access Reviews Password Requirement
5 ITOS-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.	<ul> <li>L certain the completeness and accuracy of the report utilized to perform the review.</li> <li>J verify that any corrections to the password is performed think in the use of the performed that in the performance of the performance of the performance accuracy.</li> <li>Performed the performing the performing the performed that in the quarter of review.</li> <li>Performed the performance are reviewed (performed that in the quarter of review.</li> <li>Performed the performance are reviewed (performed that in the quarter of review.</li> <li>Performed the completeness are reviewed for anormal in 10 business days.</li> <li>Performed the completeness are reviewed for anormal in the perform the review.</li> <li>Performed the completeness are reviewed for anormal the performation.</li> <li>Performed the completeness are reviewed for anormal that any performed the performation.</li> <li>Performed the performance the performation.</li> <li>Performed the performance the performance of the performed the performation.</li> <li>Performance the performance t</li></ul>	Ad-hoc Ad-hoc	High IT Network Security Medium IT Operating System	User Access Reviews  Password Requirement User Access Reviews
5 ITOS-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.         Operating system passwords are configured according to company policy.         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.         Access to migrate changes to production envirnonments for key financial systems is restricted to	<ul> <li>Letermine the completeness and accuracy of the report utilized to perform the review.</li> <li>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.</li> <li>Verify that perform the review was done within 120 days of the year-end</li> <li>A Determine whether a review of all access (accluding read-only accounts) was performed by appropriate performing self reviews (including service/shared/system accounts).</li> <li>Perfleged/administrative accounts are reviewed for appropriate-personal within proper segregation of duries enforced.</li> <li>Monager: or delegates performing reviews.</li> <li>Perileged/administrative accounts are reviewed for appropriate-personal within the review.</li> <li>Determine whether that users were reviewed (accuding read-only accounts).</li> <li>Determine the user report was generated within the quarter of review.</li> <li>Modification/reviewa (accusation of duries enforced</li></ul>	Ad-hoc Quarterly Quarterly Quarterly	High IT Network Security Medium IT Operating System High IT Operating System	User Access Reviews Password Requirement
5 ITNS-004 ITOS-003	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.         Operating system passwords are configured according to company policy.         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.         Access to migrate changes to production environments for key financial systems is restricted to personnel with non-development responsibilities         (US Only) - On an Annual basis, IT Management will review the key configurations and security	<ul> <li>Letermine the completeness and accuracy of the report utilized to perform the review.</li> <li>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.</li> <li>Verify an appropriate risk assessment was performed for any parameters not in compliance with ompany's password policy or approved policy exception.</li> <li>Verify that the review was done within 120 days of the year-end</li> <li>A betermine whether a review of all access (excluding read only accounts) was performed by appropriate personnel with proper segregation of duties enforced.</li> <li>Manages or delegates performing reviews.</li> <li>Herineages or delegates performing reviews.</li> <li>Determine whether all uses were reviewed (excluding read only accounts).</li> <li>Determine whether all uses were reviewed (excluding read only accounts).</li> <li>Determine whether all uses were and accuracy of the user report utilized to perform the review.</li> <li>Indepropriate cases identified as reviewed (excluding read only accounts).</li> <li>Determine whother all uses were access reviewed by a primary reviewer and includes a secondary reviewer if the primary reviewer knows the password to the system/generic accounts.</li> <li>Determine if system/generic accounts hare reviewed (excluding read only account and who all knows the password to the account.</li> <li>Determine if system/generic accounts hare reviewed within 10 business days. If Additional time is a specific performed review.</li> <li>Determine if system/generic accounts hare a brief description of the account and who all knows the password to the account.</li> <li>Determine if system/generic accounts hare a brief description of the cacount and who all knows the password to inter access description gate access description access interview.</li> <li>Determine if a capproved policy exception:</li> <li>Serving ad</li></ul>	Ad-hoc Ad-hoc Ad-hoc Ad-hoc	High IT Network Security I Operating System I Groperating System I Grope	User Access Reviews Password Requirement User Access Reviews User Access Reviews Change Management (Access to Production
5 ITNS-004 5 ITOS-003	Active Directory domain-wide administrative security groups are reviewed on a quarterly basis by IT management or a quarterly basis by IT management will review the key configurations and security administrative User accounts (including system/generic accounts) and access rights to the personnel with non-development responsibilities         Access to migrate changes to production environments for key financial systems is restricted to personnel with non-development responsibilities         (US Only) - On an Annual basis, IT Management will review the key configurations and security administrative access for the STAT tool.         Changes to Key Financial Applications and/or supporting infrastructure are properly tested and	<ul> <li>C. Determine the completeness and accuracy of the regort utilication perform the review.</li> <li>V. Verify that arguing exception form must be filed and approved.</li> <li>Verify an appropriate risk ascessment was performed within 10 business days. If Additional time is realized, a policy exception form must be filed and approved.</li> <li>Verify that properties risk ascessment was performed or any parameters not in compliance with company's password policy or approved policy exception.</li> <li>Verify that the review was done within 120 days of the year-and</li> <li>A. Determine whether a review of all access (adualing read-only accounts) was performed by appropriate provides.</li> <li>Performation with proper service dynamic grad-only accounts.</li> <li>Determine whether all users were reviewed for allops read-only accounts.</li> <li>Determine whether the allows were reviewed for allops and this the password bases.</li> <li>Determine whether the allows were reviewed for allops with integrorize access were within the review.</li> <li>Determine whether the allows were reviewed for allops with histoprofite access within the review.</li> <li>Determine whether the user report was generaled within 10 business days.</li> <li>Determine the review of the user report was generaled within 20 days.</li> <li>Determine the review of the user versive of rail uses with insportate access within the review.</li> <li>Determine the review of the password parameters and werely agree to company's password policy or there is an approved policy exception.</li> <li>Determine the review of all access (excluding read-only accounts).</li> <li>Determine the review of all access (excluding read-only accounts).</li> <li>Determine the review of all access (excluding read-only accounts).</li> <li>Determine the review of all access (excluding read-only accounts).</li> <li>Perform the review of all access (excluding read-only accounts).</li> <li>Deter</li></ul>	Ad-hoc Quarterly Ad-hoc Ad-hoc Ad-hoc Annually Annually	High IT Network Security I Operating System I Groperating System I Grope	User Access Reviews Password Requirement User Access Reviews User Access Reviews Change Management (Access to Product)
5 ITNS-004 5 ITOS-003 5 ITOS-003	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.         Operating system passwords are configured according to company policy.         Operating system passwords are configured according to company policy.         Eventer(/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.         Access to migrate changes to production environonments for key financial systems is restricted to personnel with non-development responsibilities:         (US Only) - On an Annual basis, IT Management will review the key configurations and security administrator access for the STAT tool.         Changes to Key Financial Applications and/or supporting infrastructure are properly tested and approved prior to being provide to the STAT tool.	<ul> <li>L. Determine the completeness and accuracy of the report utilized to perform the review.</li> <li>V. Verify that argorithm form must be filed and approved.</li> <li>V. Verify an appropriate scale access of the second accuracy of th</li></ul>	Ad-hoc Quarterly Ad-hoc Ad-hoc Ad-hoc Annually Annually	Nedium   IT Network Security   High   IT Operating System	User Access Reviews Password Requirement User Access Reviews User Access Reviews Change Management (Access to Producti Change Management (US Only)
ITNS-004 ITOS-003 ITOS-003 ITAD-001.1	Active Directory domain-wide administrative security groups are reviewed on a quarterly basis by T         management or a qualified delegate. Modification/removal requests are made and confirmed in 10         business days.         Operating system passwords are configured according to company policy.         Deprating system passwords are configured according to company policy.         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.         Access to migrate changes to production environments for key financial systems is restricted to personnel with non-decedopment responsibilities         UUS Only - On an Annual basis, IT Management will review the key configurations and security administrator access for the STAT tool.         Changes to key Financial systems).         Elevated supporting key Financial systems).         Elevated supporting key Financial systems).	<ul> <li>C. Detrimine the completeness and accuracy of the report utilized to perform the review.</li> <li>V. Verify has apporten its is asserved is performed within 10 business days. If Additional time is required, a policy acception form must be filed and approved.</li> <li>V. Verify that the review was done within 12 diays of the year-and</li> <li>A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate generation of utilizes (access verify shared) (see the review).</li> <li>A. Determine whether a review of all access (excluding read-only accounts).</li> <li>Determine whether a the event was accounted on the period on the accounts.</li> <li>Determine whether all uses were reviewed for all period on the accounts.</li> <li>Determine whether all uses were reviewed for all period on the accounts.</li> <li>Determine whether the all uses were reviewed for all period on the account of the access vertices is a reviewed for all users were access vertices is access access within the quarter of reviews.</li> <li>Determine whether the all uses were reviewed for all uses with inappropriate access within the vertices.</li> <li>Determine whether the uses report was generated within the quarter of reviews.</li> <li>Determine the more access and the set of the set or whether appropriate access within the vertices.</li> <li>Determine the provided (please set he lobback procedure documentation).</li> <li>Determine the provided parameters and whether all uses were reviewed of all access vertices in any performation access and the provided (please set he lobback procedure documentation).</li> <li>Determine the provided parameters and whether an evene of all parameters and whether a review of all access (excluding read-only acceuts).</li> <li>Despont the accounts.</li> <li>Determine the completeness and accuracy of the report utilized to perform the review.</li> <li>Despont the accounts.</li> <li>Determine th</li></ul>	Ad-hoc Quarterly Ad-hoc Ad-hoc Ad-hoc Annually Annually	High IT Application Development High IT Application Development High IT Application Development	User Access Reviews Password Requirement User Access Reviews User Access Reviews User Access Reviews Change Management (Access to Producti Change Management (US Only) Change Management

		(Global) Reviews of terminated users with access to AD are performed by the last business day of the	<ul> <li>A. Determine whether the AD user report was generated by the last business day of the month.</li> <li>B. Terminated users on HR termination listing (of the same month) are crossed referenced to the AD user listing on a monthly basis.</li> <li>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).</li> <li>(Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)).</li> <li>D. Verify the review was performed within 10 business days.</li> <li>E. Determine the completeness and accuracy of the AD user and HR termination reports utilized to generate this</li> </ul>		
ITNS	ITNS-002.1	month.	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.	<ul> <li>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.</li> <li>B. Determine the impact analysis identified all terminated employees whose Business Process approvals were completed after 5 days of their termination date.</li> <li>C. Impact analysis was performed accurately. (lookback procedure)</li> <li>(Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)).</li> <li>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.).</li> </ul>	IT Network Security	Termination Requests
	11113-002.2	termination date. If so, an impact analysis is performed.	and date stamp of your computer screen is included in the screen shot.j.	Thetwork Security	
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.	<ul> <li>A. Determine whether a review of all access (excluding read-only accounts) was performed by appropriate personnel with proper segregation of duties enforced.</li> <li>-Managers or delegates performing reviews.</li> <li>-Reviewers are not performing self-reviews (including service/shared/system accounts).</li> <li>-privileged/administrative accounts are reviewed for appropriateness.</li> <li>B. Determine whether all users were reviewed.</li> <li>C. Determine whether the user report was generated within the quarter of review.</li> <li>D. Modification/removal requests are made and confirmed in 10 business days.</li> <li>E. Determine the completeness and accuracy of the user report utilized to perform the review.</li> <li>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).</li> <li>(Note: Log-in monitoring activities are reviewed for all users with inappropriate access within the evidence provided (please see the lookback procedure documentation)).</li> <li>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 and who all knows the password to that account.</li> <li>I. Roles and privileges that enables users to modify/delete/add jobs are reviewed.</li> </ul>	IT Job Systems	Key Financial Job Systems
SLTI	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
1135	1130 001.2		A see faile to the montered and followed up to resolution (within 5 business days).	11 305 5y3tems	Key manadrisos systems