Goldcorp GLAM IT Audit Controls
Denver Trimble User Conference

Chris Saari, Manager Compliance Land, RIM, Contracts

May 2, 2018

GOLDCORP

Goals:

- Understand the purpose of SOX and ITGCs
- Understand the control attributes for information security, change management, computer operations and program development
- Execute controls and appropriately document control performance evidence

Topics for Discussion

- What is SOX and ITGCs?
- Why are they important?
- Goldcorp's ITGCs:
  - Information Security
  - Change Management
  - Computer Operations
  - Program Development
- How to execute these controls?

What is SOX and ITGCs?

SOX and ITGCs

- Sarbanes-Oxley Act (SOX)
  - Legislation passed in 2002 by the US Congress
  - Protect shareholders and the general public from accounting errors and fraudulent practices
  - Administered by the US Securities and Exchange Commission (SEC)
  - Applies to all companies listed on the US stock exchange

- Information Technology General Controls (ITGCs)
  - Controls that apply to all systems components, processes and data for given organization or IT environment
  - To ensure the proper development and implementation of applications, integrity of programs, data files and computer operations

Why is SOX and ITGCs important?

Why is Sox Important? - Sarbanes Oxley Act – Key Sections

- Section 301
  - Audit committees of SEC registrants should be independent.
- Section 302
  - CEO and CFO to sign off on SEC filings attesting to their accuracy – greater accountability at the top.
  - **Penalties:** If certification is made and the reports are found to be financially unrepresentative, the CEO and CFO can be found criminally liable and face imprisonment of 10 to 20 years. In addition, civil penalties can include fines of up to $5 million.
- Section 404
  - **Management assessment** on the effectiveness of the internal controls structure and procedures for financial reporting.
  - **Auditor's attestation**
- Section 406
  - Sets forth ethics code and disclosure requirements for SEC registrants.

SOX Roles and Responsibilities - Independent review and governance

Process/Control Owners	External Audit	Internal Audit
• Understands and define risk associated with the business process or activity being performed, as well as related internal controls	• Required to be independent of the entity in both fact and appearance.	• Maintains dialogue with Management to obtain a thorough understanding of the control environment
• Takes ownership for defining and updating policies and procedures reflective of the process in place	• Required to be objective by applying professional scepticism to deliver an unbiased opinion on management's assertions regarding the effectiveness of internal controls surrounding financial reporting	• Performs operating effectiveness assessments
• Executes processes and control procedures in line with understanding of associated risk		• Report's findings from operating effectiveness assessments to management
• Identifies and communicate opportunities for improved efficiency or effectiveness		• Provides Management with feedback and recommendations to improve the control environment

Why are ITGCs important?

- ITGCs are the foundation upon which systems operate
- ITGCs help ensure the integrity, accuracy and completeness of data in the systems
- Without strong ITGCs, reliance upon IT-dependent controls and processes within a business process would be difficult
- ITGCs are pervasive across all business processes using IT systems
- Minimizes manual circumvention; consider restricted access
- Critical risks:
  - Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both.
  - Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or nonexistent transactions or inaccurate recording of transactions
  - Unauthorized changes to data in master files.
  - Unauthorized changes to systems or programs
  - Inappropriate manual intervention

Benefits of SOX Compliance and Information Technology General Controls

- A healthy control environment maximizes the value of a business

Financial Reporting Benefits	• Heightened credibility provided to all stakeholders, whether they be owners, employees, customers, lenders or vendors • Better information to manage the business • Reduced risk of errors or irregularities
Operational Benefits	• Clarity in the roles and responsibilities of both management and employees • Greater controls over the management of business growth • Reduced costs obtained from greater operating efficiency • Maximized operating performance
Regulatory Benefits	• Decreased risk of litigation or business disruption, thanks to the focus on compliance • Lowered risk of employee or customer litigation • Increased credibility with regulatory bodies • More credibility in contractual relationships with vendors and customers

Goldcorp's ITGCs - GLAM

GLAM – INFORMATION TECHNOLOGY GENERAL CONTROLS (ITGCs)
Upgrades for Argentina, Canada, Chile, Mexico, USA Closed sites

Information Security	• Ensure user access to GLAM is appropriately restricted
Program Change	• Requests for program technical/system upgrades and patches are appropriately considered, processed and tested.
Computer Operations	• Backups performed and any failures are investigated and resolved.
Program Development	• Requests for program development improvements are appropriately considered, processed, and tested.
Periodic Reviews	• Perform periodic user and IT application reviews ensuring segregation of duty - Reviewer, approver, and system change cannot be same person) • Global IT Help provides change management support for GLAM

GLAM = Goldcorp's Land Asset Management System

GLAM IT CONTROLS TRAINING FOR ALL JUSRISDICTIONS Q2 2018

INFORMATION SECURITY

IS-23 New User in GLAM

- *“When a new user requires access to GLAM, the manager from the site where access is required will send an email to the Manager Compliance, Land, RIM, Contracts to request access. When the vendor requires access to GLAM, the vendor will send an email to the Manager Compliance, Land, RIM, Contracts to request access. Once this email is received, the manager will open a Footprints ticket to document the request and also to request that IT provisions the access. The manager provides the approval while IT support team provisions the access and permissions.”*

- What auditors look for?
  - When was access granted?
  - Was access that was granted aligned with what was requested?
  - Who was the approver? Was the approver appropriate?
  - Was access granted after approval?

IS-02 Terminated Users

- *“When a user is terminated from Goldcorp or no longer requires access to the application the user’s manager or HR will submit a ticket request within Footprints for access to be changed to an inactive status, not removed. As the application is single sign on with Windows, IT support team will disable the network account upon receiving an IT ticket.”*

- What auditors look for?
  - When was the user terminated?
  - Was network/application account disabled or deleted on or before termination date?
  - Was the account accessed by the user after termination?

IS-25 GLAM USER REVIEW

- *“On a semi-annual basis, IT support team will generate the user list for GLAM and send it to the Manager Compliance, Land, RIM, Contracts for review. The user list will contain both the general users and the high privileged users who can add/change/delete data and users within the application. An IT ticket is created to track the approvals and any corrective actions. The manager will coordinate with the site managers to review the user list. If any corrective actions are noted, IT support team will implement the change.”*

- What auditors look for?
  - Is the review list complete and accurate?
  - Is the reviewer appropriate?
  - If corrective actions were noted, were they implemented on a timely manner?
  - Segregation of reviewer and implementer

IS-05 GLAM SINGLE SIGN ON VERIFICATION

- *“The application is authenticated against the network which is configured in accordance with Goldcorp's Global IT policies.”*

- What auditors look for?
  - Screenshot of application for single sign on ability

PROGRAM CHANGE

PC-29 VERIFICATION OF UAT/PROD ENVIRONMENTS

- *“The vendor - Trimble - hosts the development and testing environment while Goldcorp hosts their own testing and production environments which are segregated for changes to application.”*

- What auditors look for?
  - Screenshots of the different environments

PC-08 GLAM SYSTEM UPGRADES/PATCHES

- *“The vendor - Trimble - sends patch or version updates to the Manager Compliance, Land, RIM, Contracts for approval. Once approved, the manager will send the change request to the IT support team who will work with the vendor to conduct the application configuration changes. The vendor will develop the change and import the changes into a test environment where either the IT support team or the business will conduct testing. Once testing has been approved by IT, business owner and CAB, changes will be implemented to production by the vendor. The IT support team will create an IT ticket in Footprints to track the testing and approval evidence.”*

- What auditors look for?
  - Who developed the change? Who tested the change? Who implemented the change?
  - Is tested evidence retained?
  - Was approval granted prior to change being implemented into production?

PD-04 GLAM IT APPROVALS

- *“All projects (application development, acquisition and infrastructure) are approved by the business and IT sponsors prior to implementation. Evidence of approvals are maintained in an IT ticket in Footprints.”*

- What auditors look for?
  - A project change request is completed for major changes
  - Approval from the business and IT

PD-01 GLAM TESTING

- *“User Acceptance Testing (“UAT”) is performed and approved by business prior to migration to production.”*

- What auditors look for?
  - Was testing conducted for major application changes?
  - Was the change approved prior to implementing the change into production?

PD-05 – GLAM TESTING

- *“Defects are tracked and resolved prior to go-live where testing and approval evidence is maintained in an IT ticket in Footprints.”*

- What auditors look for?
  - If issues/problems occur during the project, how was is resolved?
  - Email evidence, testing evidence, etc.

GLAM DATABASE MANAGEMENT

CO-01 GLAM BACK UP

- *“Business critical applications, infrastructure, systems and data must be backed up daily (incremental/differential backups are acceptable). Full backups must be performed weekly at a minimum and when feasible prior to the implementation of any major changes in production environment. Storage and backup solutions are managed by the IT group that oversees the Markham data centre, which is operated by Goldcorp’s Infrastructure team.”*

- What auditors look for?
  - Screenshots of how the backups are conducted
  - The scheduled time for each backup

IS-06 (database)

- *“A user who requires direct access to the database for an in-scope application will create and IT ticket or request access by sending an email to the application owner. The application owner will provide the approval. Once approval is retrieved, the database infrastructure team will provision the access.”*

- What auditors look for?
  - When was access granted?
  - Was access that was granted aligned with what was requested?
  - Who was the approver? Was the approver appropriate?
  - Was access granted after approval?

IS-07 (database) USER TERMINATION

- *“When a user is terminated from Goldcorp or no longer requires access to the application, database and/or network, the user’s manager or HR will submit a ticket request within Footprints for access to be removed. As the database is single sign on with Windows, IT support team will disable the network account upon receiving an IT ticket.”*

- What auditors look for?
  - When was the user terminated?
  - Was network/application account disabled or deleted on or before termination date?
  - Was the account accessed by the user after termination?

IS-08 (database) – GLAM ADMIN ACCESS REVIEW

- *“Database infrastructure team and application owners access is monitored for appropriateness. Inappropriate access is removed or disabled, and access of terminated employees are removed.”*

- What auditors look for?
  - Who are the members in the database infrastructure team with system administrator access?
  - What type of access do they have?
  - Are they appropriate?

IS-09 (database) INTERNAL DATABASE REVIEW

- *“On a semi-annual basis, the database infrastructure team will generate the database user list for the in-scope application. The database infrastructure team will conduct the review with the application owner. If corrective actions are noted, changes are applied by the database infrastructure team. A Footprints ticket is created to track request and approval.”*

- What auditors look for?
  - Is the review list complete and accurate?
  - Is the reviewer appropriate?
  - If corrective actions were noted, were they implemented on a timely manner?
  - Segregation of reviewer and implementer

PC-03 (database) DATABASE CHANGES

- *“Database infrastructure changes consist of database or server updates and Microsoft patches. These changes will be initiated by the database infrastructure team and an IT ticket will be created. Infrastructure changes will first be approved by the Global infrastructure Manager and then go through CAB approval. Testing and approval evidence will be tracked in the IT ticket.”*

- What auditors look for?
  - Who developed the change? Who tested the change? Who implemented the change?
  - Is tested evidence retained?
  - Was approval granted prior to change being implemented into production?

IT NETWORK MANAGEMENT

IS-06 (network) USER ACCESS

- *“An IT ticket is created by the new user's manager to initiate the IT onboarding procedures. IT Helpdesk is responsible for adding new users to the network.”*

- What auditors look for?
  - When was access granted?
  - Was access that was granted aligned with what was requested?
  - Who was the approver? Was the approver appropriate?
  - Was access granted after approval?

IS-12 (network) TERMINATED USER

- *“The manager of the terminated user will submit and IT ticket to HR. Once received, IT helpdesk will disable the account on or before the termination date of the user.”*

- What auditors look for?
  - When was the user terminated?
  - Was network/application account disabled or deleted on or before termination date?
  - Was the account accessed by the user after termination?

IS-13 (network) NETWORK ADMINISTRATORS

- *“All Admin tier levels (Tier 1 to Tier 5 inclusive) are to use Active Roles Server for all AD account management activities. All admin tier levels are monitored for appropriateness. Inappropriate access is removed or disabled, and access of terminated employees are removed.”*

- What auditors look for?
  - Who are the members in the network infrastructure team with system administrator access?
  - What type of access do they have?
  - Are they appropriate?

IS-14 (network) NETWORK USER REVIEW INTERNAL

- *“On a monthly basis, an automatic IT ticket will be created to initiate the network user review process. The network infrastructure team will generate a user list from active directly through Active Role tool. Any users that have been inactive for 90 days will be highlighted. The user list will be sent to the IT Compliance team for review. Once review is conducted, the IT Compliance team will send the list back to the network infrastructure team to make the necessary changes if noted from the review.”*
- What auditors look for?
  - Is the review list complete and accurate?
  - Is the reviewer appropriate?
  - If corrective actions were noted, were they implemented on a timely manner?
  - Segregation of reviewer and implementer

IS-15 (network) DOMAIN ADMIN REVIEW

- *“On a monthly basis, there is also a domain admin review process where the network infrastructure team will generate this list. Then, the Global Infrastructure Manager will conduct the review. If any corrective actions are noted, the network infrastructure team will make the changes. An IT ticket is created to track the approval and review evidence.”*

- What auditors look for?
  - Is the review list complete and accurate?
  - Is the reviewer appropriate?
  - If corrective actions were noted, were they implemented on a timely manner?
  - Segregation of reviewer and implementer

IS-16 (network) INTERNAL AUTHORIZATIONS

- The network follows Goldcorp's IT policy for network passwords.
  - Enforce password history: 6
  - Max password age: 90 days
  - Min password age: 1 days
  - Min password length: 8 characters
  - Password must meet complexity requirements: Enabled
  - Store passwords using reversible encryption: Disabled
  - Account lockout duration: 30mins
  - Account lockout threshold: 5 invalid logon
  - Reset account lockout counter after: 30mins

What auditors look for?

- Does the network password parameters meet the IT policy?

PC-18 (network) INTERNAL TESTING

- *“Routine changes consists of specific changes pertaining to the network or database infrastructure. Network infrastructure team will initiate an IT ticket to track all the approvals and testing for evidence. Routine changes only require approval from the Global Infrastructure Manager prior to any changes being made. This change does not need to go through CAB approval.”*

- What auditors look for?
  - Who developed the change? Who tested the change? Who implemented the change?
  - Is tested evidence retained?
  - Was approval granted prior to change being implemented into production?

PC-19 (network) IT STANDARDS RETIRING DATABASE

- *“Standard changes consist of changes such as deleting/retiring a database. These changes will be initiated by the network infrastructure team where approval and testing evidence will be documented. the Global Infrastructure Manager will first provide the approval prior to going through the CAB approval process. The network infrastructure team will provision the change after approval is received from both the Global Infrastructure Manager and CAB approval.”*

- What auditors look for?
  - Who developed the change? Who tested the change? Who implemented the change?
  - Is tested evidence retained?
  - Was approval granted prior to change being implemented into production?

THANK YOU - ANY QUESTIONS?