IT GRC & RISK MANAGEMENT

Greg Guracech
Craig Mancuso
Agenda

- Introductions
  - Creative Breakthroughs, Inc. (“CBI”)
  - Greg Guracech | Chief Operating Officer
    Creative Breakthroughs, Inc.
  - Craig Mancuso
    Vice President, Information Security and Risk Services
    Comerica Bank, Inc.

- Topical Overview
  - IT GRC
  - Examples

- Threats

- COBIT Framework

- Q&A
CBI Background

Established in 1991
Privately-Owned
Top Technical Expertise & Talent
Crain’s Cool Places to Work
Consultative/Advisory Approach
Active in Community
Greg Guracech

• Personal
  – Married 26 years with four kids (and a dog)
  – Sports Junkie
  – Passionate about music; play a few instruments
  – News junkie; love CNBC

• Career
  – Worked as a CFO at a Tier one auto supplier
  – Spent 8 years at PwC in the Advisory practice
Craig D. Mancuso - Curriculum Vitae

Comerica Bank (and predecessor), 1985 – present:

- Item Processing
- Software Development
- Telecommunications
- Program/Project Management
- Technology Support
- Bank Acquisition – Operational Consolidation
- Contract Management
- Corporate Communications
- Regulatory Agency Liaison (Operations)
- Audit Management
- Compliance Management
- Risk Management (Focus on technology risk)

BC 1975 – 1985:

San Diego Trust & Savings Bank (San Diego), United Savings Bank (San Francisco)
More about Craig

• Single
• One boy: (He's been to college)

• Play violin, viola and cello (It's good to be indispensable!)

• Movie buff (Way movie buff!)

• Huge fan of British crime dramas (I ♥ Helen Mirren)
TOPICAL OVERVIEW
What is IT GRC

IT GRC is:
• IT Governance, IT Risk, IT Compliance
• They are three distinct disciplines
• Best when managed coherently
  • Creates efficiencies
  • Provides a holistic view of the IT environment
  • Helps to ensure accountability
• Should be aligned with a company’s overall Risk Management program

A Forrester survey asked corporate America their view on IT GRC. The response was wide and varied:
• It demonstrated the lack of clarity
• By default it demonstrated a lack of leadership in the space at corporate America
IT Governance

• The act of establishing IT decision structure, process, and communication in support of business objectives and tracking progress against fulfilling business obligations effectively and consistently.

• Requirements
  – Appropriate governance structure
    • Cross section of departmental leaders
    • “Tone from the Top”
  – Ensure that appropriate processes are in place to:
    • Guarantee consistency and transparency
    • Approve investments
  – Proper communication cadence
  – Accountability to measure IT outcomes
IT Risk

• A coordinated set of activities to not only manage adverse impacts of IT on business operations but to also realize the opportunities that IT brings to increase business value.

• Requirements
  – Disciplined Operational approach to:
    • Identifying and prioritizing risks
    • Incident response planning
    • Disaster recovery
  – Technology
    • Assess the agility of the organization
    • Architecture sustainability and effectiveness
  – Partnering
    • Evaluation of third party partners
    • Vendor management
IT Compliance

• A process of establishing controls within the IT environment and managing the implementation of those controls.

• Objectives
  – Corporate Compliance
    • Security and Privacy
    • Human Resources
  – Best Practice
    • Establishing a compliance framework
    • Sustainability
  – Legal and Regulatory Compliance
    • Regulations (Industry & Global)
    • Laws (Local & Global)
Making IT GRC Work

Understand dependencies and provide a common approach

Unify controls for IT Risk and Compliance

Enable IT Governance by establishing accountability

Align technology and process for efficiency and consistency
Opportunities and Results

“However beautiful the strategy, you should occasionally look at the results.”

- Winston Churchill

“The pessimist sees difficulty in every opportunity. The optimist sees the opportunity in every difficulty.”

- Winston Churchill
Successes of IT GRC

- Enhancing IT governance capabilities
  - Building a framework to measure

- Helping mitigate IT threats more effectively
  - Identifying internal and external threats

- Establishing protocols to deal with the threats
  - Incident response team
  - Risk assessment

- Simplifying the regulatory compliance requirements

- Training
  - Making compliance a part of everyone’s DNA
  - Continuous updates and participation

- Building discipline around control issues (Lifecycle of an issue)
## Lifecycle of a Control Issue

**Four Phases**

- **Issue Discovery; Issue Analysis; Design & Execution; Test and Close**

<table>
<thead>
<tr>
<th>Time</th>
<th>Task</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Issue Discovery; Typically 3 to 5 Days</strong></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>IT Audit Performs Internal Examination</td>
<td>IT Audit performs internal examination (typically 3 to 5 days)</td>
</tr>
<tr>
<td></td>
<td>IT Audit, Client, IT GRC</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>IT Audit Prepares Preliminary Control Deficiency Report</td>
<td>IT Audit prepares preliminary control deficiency report (typically 1-2 days)</td>
</tr>
<tr>
<td></td>
<td>IT Audit, Client, IT GRC</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Revenue Deficiency Report</td>
<td>Revenue deficiency report is prepared (typically 1-2 days)</td>
</tr>
<tr>
<td></td>
<td>Client, IT GRC, IT Audit</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Departmental Contact Provides Preliminary Response</td>
<td>Departmental contact provides preliminary response (typically 1-2 days)</td>
</tr>
<tr>
<td></td>
<td>Client, IT GRC, IT Audit</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>IT Audit Prepares Draft Audit Report and Sends to Client</td>
<td>IT Audit prepares draft audit report and sends it to the client (typically 1-2 days)</td>
</tr>
<tr>
<td></td>
<td>IT Audit, Client, IT GRC</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Draft Report Meeting Chaired by IT Audit</td>
<td>Draft report meeting chaired by IT Audit (typically 1-2 days)</td>
</tr>
<tr>
<td></td>
<td>IT Audit, Client, IT GRC</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Client Provides Concurring Response</td>
<td>Client provides concurring response (typically 1-2 days)</td>
</tr>
<tr>
<td></td>
<td>Client, IT GRC, IT Audit</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Publish Issue Control Deficiency Report</td>
<td>Publish issue control deficiency report (typically 1-2 days)</td>
</tr>
<tr>
<td></td>
<td>IT Audit, Client, IT GRC, IT Audit Committee</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Control Issue Entered Into Issue Track</td>
<td>Control issue entered into issue track (typically 1-2 days)</td>
</tr>
<tr>
<td></td>
<td>IT Audit, IT GRC, Client</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Issue Analysis; 30 to 50 Days</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>11</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>12</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>13</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
**Lifecycle of a Control Issue**

- **Four Phases**
  - Issue Discovery; Issue Analysis; Design & Execution; Test and Close

<table>
<thead>
<tr>
<th>Time</th>
<th>Task</th>
<th>Task</th>
<th>RASC</th>
<th>Start Date</th>
<th>Planned Completion Date</th>
<th>Actual Completion Date</th>
<th>Milestone</th>
<th>Complete</th>
<th>Time Estimate</th>
<th>Input Documents</th>
<th>Output Documents</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Discovery (Phase I of the Control Issue Response Document)</td>
<td>Coordinator, Owner, IT GRC, IT Audit</td>
<td>Coordinator, Owner, IT GRC, IT Audit</td>
<td>See Notes</td>
<td>Audit Control Deficiency Report Examination Summary/Notes</td>
<td>Gap Analysis/Scope Statement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Submit Gap Analysis/Scope Statement to IT GRC</td>
<td>IT GRC, IT Audit, Owner, Coordinator</td>
<td>Y</td>
<td>1 Week</td>
<td>Gap Analysis/Scope Statement</td>
<td>IT GRC will submit the Gap Analysis/Scope Statement document to IT GRC. IT GRC will submit the Gap Analysis/Scope Statement document to IT Audit for review and phase completion.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Develop Work Plan (Phase II of the Control Issue Response Document)</td>
<td>Coordinator, Owner, IT GRC</td>
<td>Coordinator, Owner, IT GRC</td>
<td>See Notes</td>
<td>Gap Analysis/Scope Statement</td>
<td>Work Plan with High Level Milestones</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Submit Work Plan to IT Audit</td>
<td>IT GRC, Owner, IT Audit, Coordinator</td>
<td>Y</td>
<td>1 Week</td>
<td>Work Plan with High Level Milestones</td>
<td>On behalf of the Issue Owner, IT GRC will submit the Work Plan document to IT Audit for review and phase completion.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Execution of Work Plan</td>
<td>Coordinator, Owner, IT GRC</td>
<td>Coordinator, Owner, IT GRC</td>
<td>See Notes</td>
<td>Work Plan with High Level Milestones</td>
<td>Deliberable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Identify Evidence Requirements</td>
<td>Coordinator, Owner, IT GRC, IT Audit</td>
<td>Coordinator, Owner, IT GRC, IT Audit</td>
<td>3 Days</td>
<td>Gap Analysis/Scope Statement/Work Plan</td>
<td>Evidence Package Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Produce Evidence Package Requirements</td>
<td>Coordinator, Owner, IT GRC</td>
<td>Coordinator, Owner, IT GRC</td>
<td>See Notes</td>
<td>Evidence Package Requirements</td>
<td>Evidence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Conduct Solution Compliance Review</td>
<td>IT GRC, Owner, Coordinator</td>
<td>IT GRC, Owner, Coordinator</td>
<td>1 Week</td>
<td>Evidence</td>
<td>IT GRC will conduct a review of the evidence package and check for accuracy and completion.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Prepare Closure Package</td>
<td>IT GRC, Owner, Coordinator</td>
<td>IT GRC, Owner, Coordinator</td>
<td>1 - 2 Weeks</td>
<td>Evidence</td>
<td>Closure Package</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>IT GRC Internal Quality Review</td>
<td>IT GRC, Owner, Coordinator</td>
<td>IT GRC, Owner, Coordinator</td>
<td>3 Days</td>
<td>Closure Package</td>
<td>IT GRC will perform an internal peer review of the closure package to ensure accuracy and completion.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Submit Issue for Closure</td>
<td>IT GRC, IT Audit, Owner, Coordinator</td>
<td>Y</td>
<td>1 Day</td>
<td>Closure Package</td>
<td>IT GRC will submit the Issue/Closure Worksheet to IT Audit for consideration for closure.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>IT Audit Analysis</td>
<td>IT Audit, IT GRC, Owner, Coordinator</td>
<td>Y</td>
<td>1 - 2 Weeks</td>
<td>Closure Package</td>
<td>Test Target Date</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Issue Closed by IT Audit</td>
<td>IT Audit, IT GRC, Owner, Coordinator</td>
<td>Y</td>
<td>~10 Days</td>
<td>Email Confirmation</td>
<td>Closure of the open control issue.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Time:
  - Typically 25 - 30 Business Days
  - Determined by the Project Work Plan

- Task Description:
  - The task includes a specific, measurable objective or result of the component defined by a personal plan. Based on information derived from the issue analysis, consider the following at a minimum:
    - 1. Determine existing process procedures (e.g. - see there any existing procedures or processes that would be impacted by or could possibly be modified to address this issue?)
    - 2. Discuss and explore possible dependencies - see there any existing processes and/or procedures that could impact or be impacted by this issue?
    - 3. Determine if any new technologies may be required to support the remediation of the control issue. The new technology could be a requirement of the solution.
    - 4. Discuss technology allocation and requirements - determine if new technology is needed to support remediation. In some instances, it may require new technology or new procedures that would either be dependent on or would provide support for the resolution of the issue.
    - 5. Brainstorm allocation and requirements - reference a single requirement of line and resource allocation needed for remediation - IT GRC, determining the required resources needed to support remediation. IT GRC will present the required resources needed for remediation.
    - 6. Brainstorm classification and requirements - determine if any new technology or new processes that would provide support for the remediation of the control issue. It may require new technology or new procedures that would either be dependent on or would provide support for the resolution of the control issue. This phase allows IT GRC to identify any additional specific remediation requirements that are unique to this control issue.

- Input Documents:
  - Gap Analysis/Scope Statement
  - Audit Control Deficiency Report Examination Summary/Notes

- Output Documents:
  - Evidence Package Requirements
  - Evidence
Challenges of IT GRC

Tone from the Top
- Not always a priority at some companies
- Permeates to all levels

Coordination among IT departments
- Disparate skill set level
- Resistance to change
- Accountability

Integration into the Corporate Risk Profile

Disconnect between management and subordinates

Lack of framework adoption

Prioritizing control risk

Developing a risk profile

Adhoc processes embedded in the organization overtime that have become protocol
Challenges of IT GRC (cont.)

Employee movement within the organization
- Keeping all previous permissions
- Lack of knowledge transfer when moving on

Building a structured approach to manage threats
- Identifying threats
- Responding to breach’s (incident response)

Regulators
- Federal Financial Institutions Examination Council (FFIEC)
- State/local
Figure 1—Three Lines of Defense: Risk Identification and Assessment, Risk Management, and Risk Monitoring

**First Line of Defense: Risk Identification and Assessment**
- **Responsibility:** Business operations perform day-to-day risk management activity.
- **Function:** An established risk and control environment

**Second Line of Defense: Risk Management**
- **Responsibility:** Oversight functions, such as finance, human resources, quality assurance and risk management, define policy and provide assurance.
- **Function:** Strategic management, policy and procedure setting, functional oversight

**Third Line of Defense: Risk Monitoring**
- **Responsibility:** Independent assurance includes internal audit, external audit and other independent assurance providers, and offers independent challenges to the levels of assurance provided by business operations and oversight functions.
- **Function:** Provides independent challenge and assurance
Data Loss Prevention - Identify Policies for Deployment

Key considerations:
- How are current security policies handled?
- What data do you want to protect first?
- How can this data be detected?
- How is this data used?
- Where is the source of this data?
- What constitutes a violation?
- What do you consider a severe violation?

Process
- Examine current policies
- Identify critical data to protect
- Prioritize business impact
- Agree on top 2-3 policies
- Discuss data structure and location
- Discuss levels of violation
Data Loss Prevention

**DISCOVER**
- Find data wherever it is stored
- Create inventory of sensitive data
- Manage data clean up

**MONITOR**
- Understand how data is being used
- Understand content and context
- Gain enterprise-wide visibility

**PROTECT**
- Gain visibility into policy violations
- Proactively secure data
- Prevent confidential data loss

**MANAGE**
- Define unified policy across enterprise
- RemEDIATE and report on incidents
- Detect content accurately
Characteristics of Successful DLP Programs

- Executive Level Involvement
- Dedicated Experienced Resources
- Prioritized Approach
- Business Owner Involvement
- Trained Incident Response Team
- Employee Education
Building a Comprehensive DLP Program

Continuous Risk Reduction and Program Maturity

Policy and Protection
Remediation
Metrics
Employee Awareness

Security Governance Program
Incident Remediation

Key considerations:

- Which incident response structure do you want to use?
- Who are your IRT members?
- What is the incident workflow?
- How will the incidents be remediated?
- How will you manage incident load?

Process

- Discuss options
- Agree on incident approach and process
- Identify IRT
- Assign tasks
Workflow Response Structure

**Fan-out**

Escalation Team

- HR
- Legal
- BU A

HR Policy Violation

Suspected Theft

Broken Business Process

First Responders

**Fan-in**

Escalation Team

- Critical Incidents

First Responders

- BU A
- Legal
- BU B
Goal: Establish procedures for responding to incidents.
Data Scanning

Key considerations:
- Which scan approach will you use?
- What are the highest risk storage areas?
- Where do you want to start?
- How will you identify data owners?

Process
- Discuss scanning approach
- Discuss data
- Compile a list of targets and prioritize
- Assign tasks
Data Scanning Strategies

Data Clean-up

Find & clean up exposed sensitive data

• Broadest file server coverage
• Distributed laptops and desktops
• All SQL databases natively
• Major document repositories
• Key email servers
• Internal and external web sites

Data Inventory

Create inventory of sensitive data

• Fastest way to inventory data
• High performance, parallel scans
• Most flexible deployment options
Endpoint Protection Strategy

Key considerations:
- Who has access to highly sensitive data?
- Who are the “at-risk” employees or groups?
- Do you want to block or enable user justification at the Endpoint

Process
- Discuss considerations
- List and prioritize deployment targets
- Prioritize use cases
- Assign tasks
Goal: Recommend an Endpoint protection strategy

- **Laptop Theft**
  - Customer List

- **Wrongly Stored Data**
  - PCI Data

- **Removable Media**
  - Product Diagrams

- **Mobile Networks**
  - Customer List

- **Print/Fax**
  - Price Lists

- **Copy/Paste**
  - Social Security or Credit Card Numbers
Metrics and Reporting

**Risk Reduction**

- % decline in incidents
  - by policy and business unit
  - across all business units
  - due to broken business processes
- Top violating business units or senders
- Number of incidents per policy
- % of incidents of "High" severity

**Operational**

- % false positives for each policy
- % of exit points covered
- % of repositories covered
- Average duration time incidents spend as “new”
Metrics and Reporting

Key considerations:

- What are the key metrics that will prove most useful?
- What reports should be generated?
- Who should receive them?
- When should they be sent?
Asset Management Scorecard

Our analysis of the current state of key aspects of the Asset Management Program. Scoring is based on analytics applied during the assessment, review of existing documentation, interviews with program users, key stakeholders, industry best practices, and personal observations.

<table>
<thead>
<tr>
<th>1.0 IT Asset Management Process</th>
<th>Misaligned</th>
<th>Fully Aligned</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Asset Planning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2 Asset Procurement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3 Asset Deployment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.4 Asset Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5 Asset Support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.6 Asset Disposition</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Key Recurring Themes and Observations

- Current inefficiencies, gaps and manual processes force employees to spend a lot of effort to carry out their day-to-day tasks, leaving them with little time or energy to work towards process improvement or innovation – working hard, not working smart.

- There is heavy reliance on manual processes throughout the different phases of the asset life cycle.

- Accurate fixed asset record keeping is made nearly impossible given existing practices.

- Software lifecycle management falls short of industry best practice and puts the company at significant risk of unnecessary spend and vulnerable to audit.

- Corporate strategic initiatives are not consistently coordinated or communicated down the chain – currently decentralized.

- Progress has been made with the implementation of the consumption model and tracking of resource utilization/labor.
Employee Communication

Goal: Determine employee communication needs

- Messaging Campaign
- Violation Notifications
- Training/Awareness
  - Incident Response Team
  - Business Unit Leaders
  - Employee
COBIT brings together the **five principles** that allow the enterprise to build an effective **governance** and **management** framework based on a holistic set of **seven enablers** that optimises **information** and **technology** investment and use for the benefit of stakeholders.
Governance (and Management) in COBIT

- **Governance** ensures that enterprise objectives are achieved by *evaluating* stakeholder needs, conditions and options; setting *direction* through prioritisation and decision making; and *monitoring* performance, compliance and progress against agreed direction and objectives (*EDM*).

- **Management** plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives (*PBRM*).

- Exercising governance and management effectively in practice requires appropriately using all enablers. The COBIT process reference model allows us to focus easily on the relevant enterprise activities.
Governance in COBIT

• The COBIT process reference model subdivides the IT-related practices and activities of the enterprise into two main areas—governance and management—with management further divided into domains of processes.

• The GOVERNANCE domain contains five governance processes; within each process, evaluate, direct and monitor (EDM) practices are defined:
  1. Ensure governance framework setting and maintenance
  2. Ensure benefits delivery
  3. Ensure risk optimization
  4. Ensure resource optimization
  5. Ensure stakeholder transparency

• The four MANAGEMENT domains are in line with the responsibility areas of plan, build, run and monitor (PBRM).
COBIT domains:
- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

The domains sub sections narrow in on key aspects of proper structure:
- Controls are mapped to the framework
- GAPs can be identified and dealt with in a strategic and tactical fashion
COBIT Domains

Source: COBIT® 5, figure 16. © 2012 ISACA® All rights reserved.
Summary

• The COBIT framework includes the necessary guidance to support enterprise GRC objectives and supporting activities:
  – Governance activities related to GEIT (5 processes)
  – Risk management process—and supporting guidance for risk management across the GEIT space
  – Compliance—a specific focus on compliance activities within the framework and how they fit within the complete enterprise picture

• Inclusion of GRC arrangements within the business framework for GEIT helps enterprises to avoid the main issue with GRC arrangements—silos of activity!
INTEGRATING WITH ENTERPRISE RISK MANAGEMENT
Characteristics of Enterprise Risk Management

Enterprise risk management encompasses:

- Aligning risk appetite and strategy
- Enhancing business planning and forecasting
- Enhancing risk response decisions
- Reducing operational surprises and losses
- Identifying and managing cross-enterprise risks
- Providing integrated responses to multiple risks
- Seizing opportunities
- Improving deployment of capital and measurement of business performance
Summary

- Strategize
- Plan
- Execute
- Monitor
- Oversight

*These all sound so simple but in reality it takes a tremendous disciplined commitment to build and maintain a best in class ITGRC organization.*
Q & A

Gregory Guracech
Chief Operating Officer
gguracech@cbihome.com
586.321.6113

Craig Mancuso
Vice President, Information Security and Risk Services
Comerica Bank, Inc.
cdmancuso@comerica.com
248.371.6729
THANK YOU!