The GAIT Series from the IIA and How it Impacts Internal Auditors

Dallas Chapter of the IIA

August 7, 2008

Edward L. Hill
Managing Director
Protiviti

Today's Agenda

- The Who, What, and Why of GAIT
  - GAIT Evolution, Principles, and Methodology
  - GAIT for SOX IT Scoping
  - GAIT Deficiency Evaluation (not discussed today) CEM1
  - GAIT- for IT and Business Risks
- Applying GAIT to an Environmental Audit
- Lessons Learned
- Conclusion

Slide 2

CEM1 Can we not have a few slides on this? It was listed in the description you'd sent to me so I suspect the expectation is there for this on some level.

Clint McPherson, 8/5/2008

What is GAIT?

Guide to the **A**ssessment of **IT** General Controls Scope Based on Risk

- A series of principles and methodologies for top-down, risk-based scoping of IT general controls

Why Was GAIT Formed?

- Lack of established guidance (inconsistency and subjectivity, reliance on checklists, etc.)
- Originally Generally Applied IT Principles
- Most pressing need was rationalization of SOX practices - so the first GAIT addressed SOX compliance
- Significant compliance and audit costs
- Need for better overall scoping frameworks

Who Developed GAIT for SOX scoping?

protiviti®
Independent Risk Consulting

Core Team

- Ed Hill, Protiviti
- Gene Kim, Tripwire
- Steve Mar, Microsoft
- Norman Marks, Business Objects
- Heriot Prentice, The IIA
- Fawn Weaver, Intel

Advisory Board

- CPA Firms – Big Four, Mid-sized Firms
- SEC Registrants
- Regulators

What is GAIT for SOX scoping?

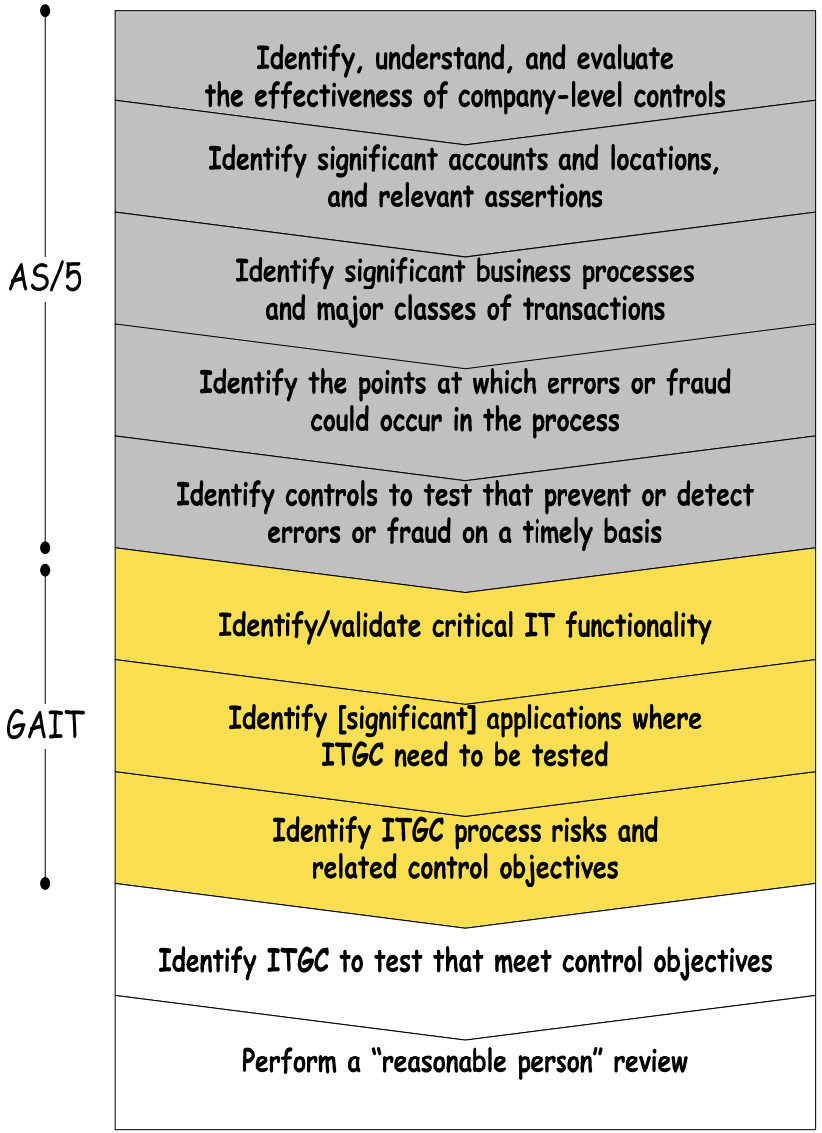
- GAIT is a reasoned thinking process that *continues* the top-down and risk-based approach in AS/5 to assess risk in ITGC
- It helps identify risk in IT processes that could affect critical functionality needed to prevent/detect material errors
- Control objectives are identified in GAIT, but not specific key controls

How Does GAIT for SOX Scoping Work?

- The GAIT document has two main parts
  - The Four Principles
  - Methodology for GAIT implementation
- Overall theory
- Practical Approach

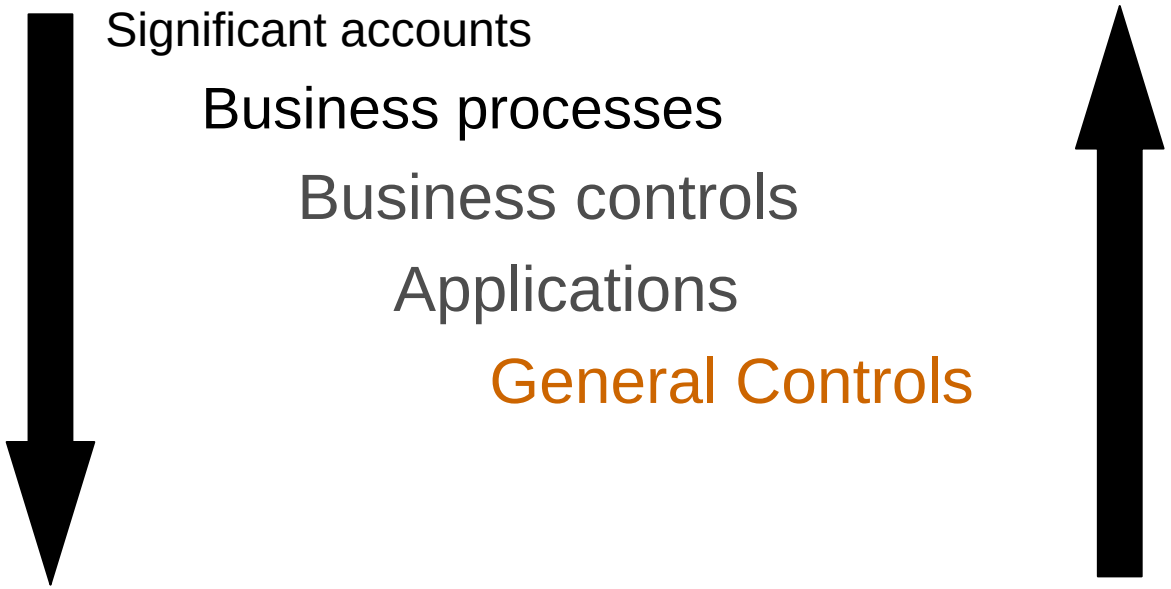
Overall GAIT Scoping

Top-Down
Risk-Based



Overall GAIT Scoping, cont'd

RISK of material misstatement/fraud to financial statements & disclosures



Scope according to RISK of material misstatement/fraud.

IT Risk Assessment and Scoping

STEP 1: validate understanding

- Significant accounts
  - Business processes
    - Business controls
      - Applications

STEP 2: perform risk assessment at each layer

IT Process Controls:

Change Mgt, Operations, Security

- ➢Application
- ➢Database
- ➢Operating System
- ➢Network

STEP 3: **Conclude:** is it REASONABLY POSSIBLE a failure in this IT Process area could impact application controls & result in a material misstatement?

Risk is not eliminated; is it reduced to a REASONABLE level.

GAIT Principle 1

The identification of risks and related controls in IT business processes should be a continuation of the top-down and risk-based approach used to identify significant accounts, risks to those accounts, and key controls in the business processes.

GAIT Principle 2

The IT general control process risks that need to be identified are those that affect critical IT functionality in financially significant applications and related data.

Financially Significant - Definition

- Application: contains functionality relied upon to assure the integrity of the financial reporting process.
  - Should that functionality not function consistently and correctly, there is at least a reasonable possibility of a material misstatement that would not be prevented or detected.

- Data: data that, if affected by unauthorized change that bypasses normal application controls (i.e., as a result of an ITGC failure), is at least reasonably likely to result in a material misstatement that would not be prevented or detected.

GAIT Principle 3

The IT general control process risks that need to be identified exist in processes and at various IT layers:

- Application program code,
- Databases,
- Operating systems, and
- Network.

GAIT Principle 4

Risks in IT general control processes are mitigated by the achievement of IT control objectives, not individual controls.

Summary

- Consider whether the failure is at least reasonably likely to have such an effect

- Use common sense, grounded in reality

GAIT for IT and Business Risk

protiviti®
Independent Risk Consulting

What it is intended to be:

- Methodology for identifying *all* the key controls critical to achieving business goals and objectives
- Identifies the critical aspects of information technology essential to the management and mitigation of business risk
- The critical IT functionalities and the risks to them should be considered when planning audit work.

Who should use this guidance?

Primarily for internal auditing practitioners:

- Those who run such functions within organizations (Chief Audit Executives, or “CAE’s”) or leaders of internal audit service providers, and
- Those who are responsible specifically for the auditing of information technology (IT auditors)
- Also used by IT governance and security managers, or those who are charged with designing and managing information technology risks within their organizations.

Principles

- **Principle 1**: *The failure of technology is only a risk that needs to be assessed, managed, and audited if it represents a risk to the business.*

- **Principle 2**: *Key controls should be identified as the result of a top-down assessment of business risk, risk tolerance, and the controls- including automated controls and IT general controls- required to manage or mitigate business risk*

Principles

- **Principle 3**: *Business risks are mitigated by a combination of manual and automated key controls. To assess the system of internal control to manage or mitigate business risks, key automated controls need to be assessed.*

- **Principle 4**: *IT general controls may be relied upon to provide assurance of the continued and proper operation of automated key controls.*

Identification of key ITGC's

- **Principle 4a:** *The IT general control process risks that need to be identified are those that affect critical IT functionality in significant applications and related data.*

- ***Principle 4b:*** *The IT general control process risks that need to be identified exist in processes and at various IT layers: the application program code, databases, operating systems, and network.*

- ***Principle 4c:*** *Risks in IT general control processes are mitigated by the achievement of IT control objectives, not individual controls.*

Key control types

- Manual controls (e.g., the performance of a physical inventory)
- Fully automated controls (e.g., matching or updating accounts in the general ledger)
- Partly automated, or “hybrid controls”, where an otherwise manual control relies on application functionality.
  - If an error in that functionality would not be detected, the entire control would be ineffective.

Top-Down Methodology

1. Identify the business objectives for which the controls are to be assessed

2. Identify the key controls within business processes required to provide reasonable assurance that the business objectives will be achieved

3. Identify the critical IT functionality relied upon, from among the key business controls

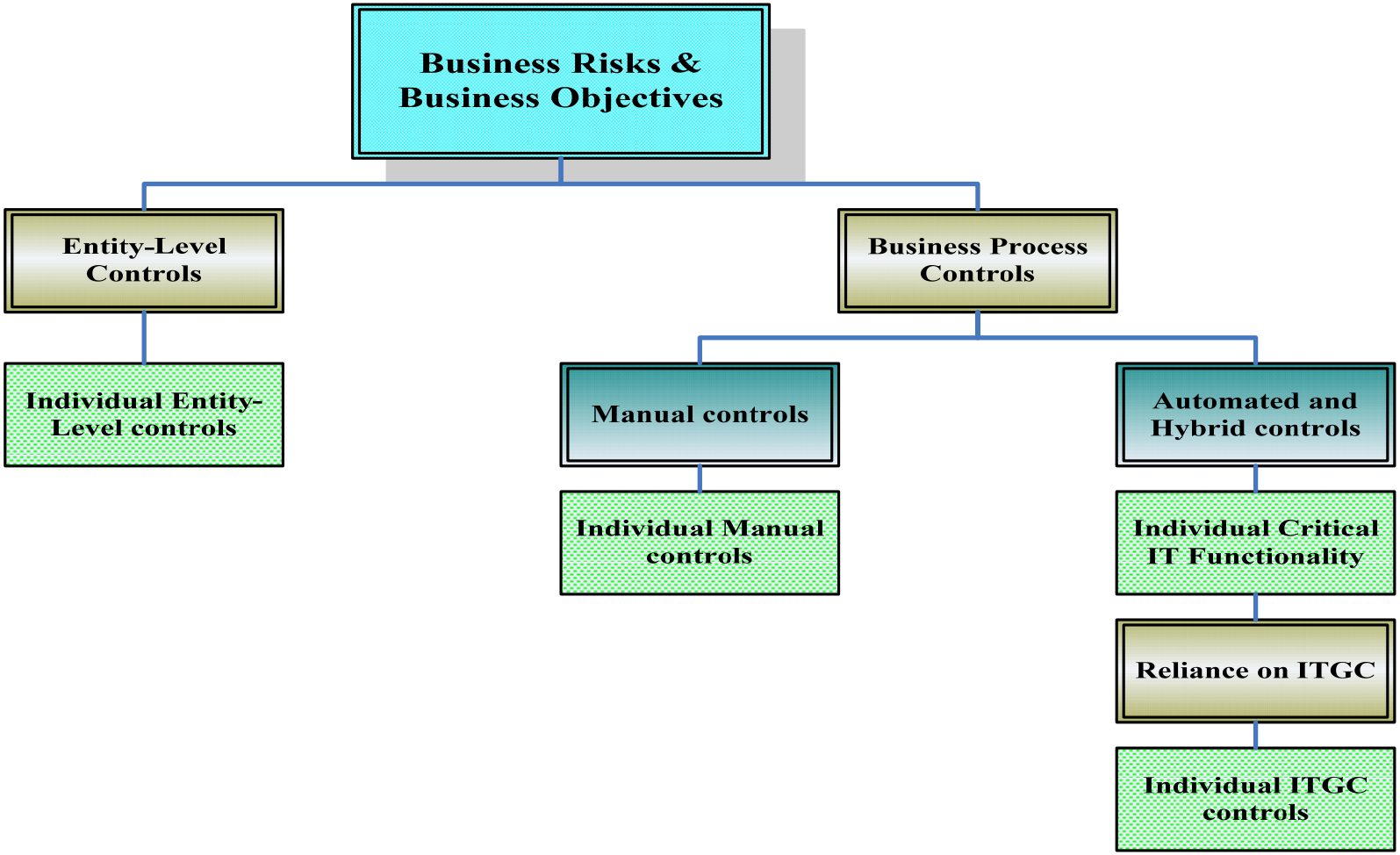
4. Identify the [significant] applications where ITGC need to be tested.

5. Identify ITGC process risks and related control objectives

6. Identify the ITGC to test that meet control objectives

Top-Down Methodology (cont'd)

7. Perform a "reasonable person," holistic review of all the key controls identified



Top-Down Methodology (cont'd)

protiviti®
Independent Risk Consulting

8. Determine the scope of the review

- A complete business audit (some might consider this an 'integrated' audit) of all the risks
  - The auditor should decide whether to perform the assessment in a single project, or split among multiple projects that may be performed at different times
  - If the assessment will be split among multiple projects, the auditor should determine how the combined assessment will be made and reported, as well as how the results of individual projects will be assessed and reported

Top-Down Methodology (cont'd)

8. Determine the scope of the review
   - An audit that is limited in scope to only selected key controls
     - The limited scope should be clearly identified and communicated both prior to work starting and also in the audit report
     - Keep in mind that the assessment of any control deficiencies may be more difficult without understanding the effectiveness of all related controls, and whether the impact of any deficiencies may be mitigated by other key controls that were not assessed
   - A consulting project, rather than an assurance project, designed to add value by improving the effectiveness of the system of internal control

Closing Summary

- GAIT for IT and Business Risk addresses how IT risk and controls should be addressed in consideration of the overall business use of technology
- There is a top-down approach to determining what technology risks and controls are important to the achievement of business goals and objectives
- Technology risks only matter when viewed in the broader business risk context

Case Study

Audit of Environmental Compliance Management Process Using GAIT

1. Business Objectives

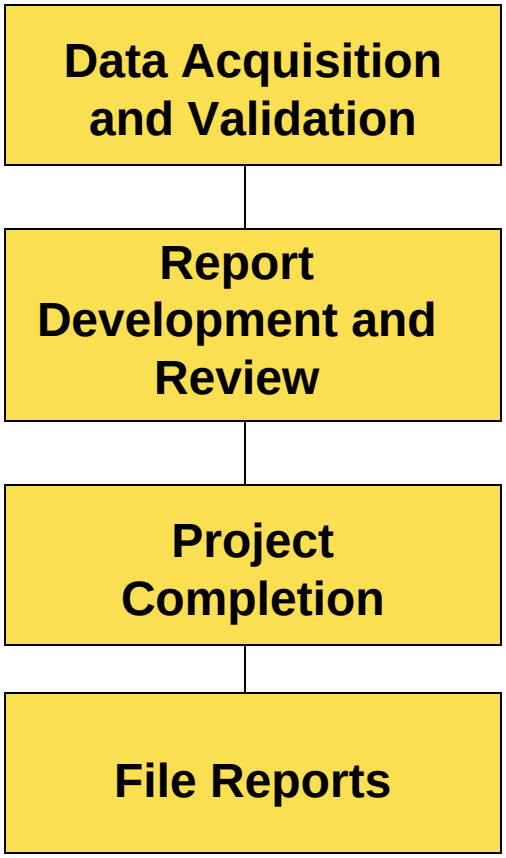
- Business Process: Manage Environmental Legal Compliance (e.g., the production of required federal and state governmental reporting for manufacturing facilities)
  - Business Objective: File complete and accurate annual reports required under the U.S. Superfund Amendment Reauthorization Act (SARA) Title III, Section 313 and 40 CFR 370/372
  - COSO Objective: Manage Regulatory / Legal Risk

Business Risks

- Key Business Risk: Under-reporting releases of hazardous chemicals and emissions
  - Fines and penalties ranging up to $37,000 per incident, per day

- Other Risks:
  - Failure to comply with laws and regulations
  - Access to information may not be based on business need
  - Reputation risk / negative media exposure
  - 3rd party risk – relying on vendor for maintaining and hosting IT system

Process Overview for the Environmental Management Process (EMP)



- Flowcharted the EMP
  - EMP includes 13 distinct steps
- System supporting the process is called “Ops Environmental System” or OES
  - Collect, calculate and analyze purchases and uses of hazardous chemicals
  - Prepare and submit reports in compliance with U.S. and state regulations
- OES hosted by 3rd party provider (called Trusty Tech or “TT”) but owned by company

So … we only have a certain number of audit hours …

What is critical to review?

Why??

2. Key Controls in the Business Process to Achieve Business Objectives

A = Timeliness

B = Completeness

C = Accuracy

Key Controls	A	B	C
1. Calendar-based reminders to users prompting input of critical data (automated)	X	X	
2. Entry and edit of chemical purchases, usages, losses, releases, etc. (hybrid)			X
3. Comparison of current results (post-calculation) to previous results (automated)		X	X
4. Final review of reports including support data (hybrid – heavy dependence) (note: “precision”)		X	X
5. e-Filing of regulatory reports	X		

3. Critical IT Functionality Relied Upon from Among the Key Business Controls

Key Controls	Related IT Functionality
1. Calendar reminders to users (automated)	Programmed routine including user notification
2. Entry and edit of chemical purchases (hybrid)	Programmed edits against tables (range check; chemical types; etc.)
3. Comparison of current results to previous results (automated)	Calculate quantities not accounted for, and compare to thresholds and priors
4. Final review of report including support (hybrid)	Select transactions, format, and print user reports
5. e-Filing of regulatory reports	Select, format, & transmit

4. The Applications Where IT General Controls Need to be Tested

- "Ops Environmental System" or OES

- Hosted and operated by Trusty Tech Co. on our behalf
  - Desire to audit may result in "push back" by TT to internal auditors
    - Contractual terms and conditions; SLAs
    - Consideration of SAS-70s

- Out of Scope for Planning (will revisit this decision later in the process):
  - Purchasing system – reviewed separately w/Dept. audit
  - Material receiving system – reviewed separately in plants
  - Excel spreadsheets (accumulate purchases) – minor role

5. IT General Control Process Risks and Related Control Objectives

Key Controls	Related Risks	Control Objectives
1. Calendar reminders	•Overdue tasks not flagged or referred to users for follow-up	•Controls ensure that all tasks have assigned due dates and users
2. Entry/edit of purchases, receipts, etc.	•Incorrect quantities, chemical types, etc. entered by users	•Controls ensure that data entered conforms to business rules (e.g. format); errors are rejected
3. Comparison of results (period to period; similar facilities; threshold comparisons, etc.)	•Calculated results may be out of line but not identified; regulatory thresholds may be inaccurate for comparison purposes	•Controls ensure calculations & transaction summarization is performed accurately and results appropriately displayed to users for review

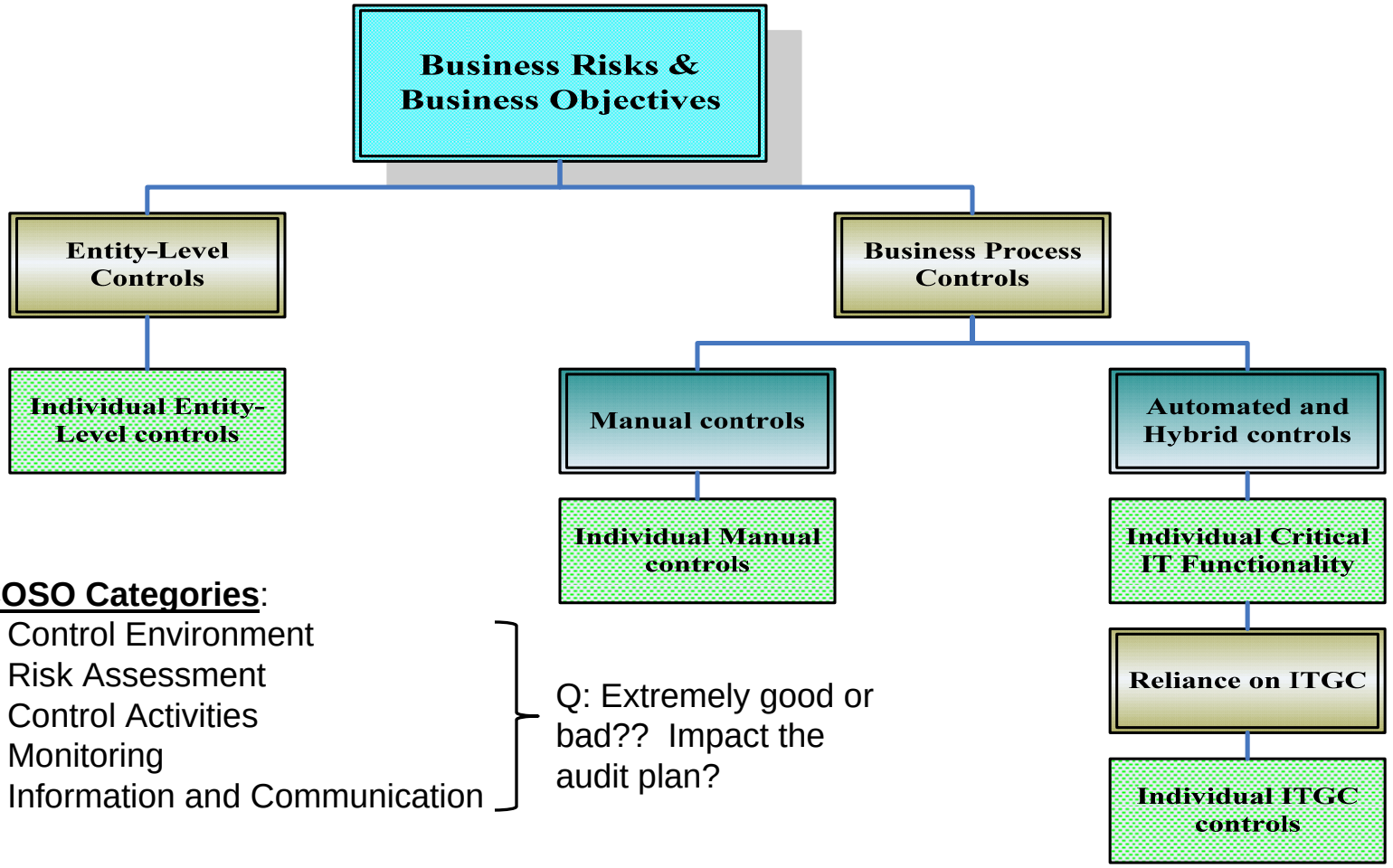
5. IT General Control Process Risks and Related Control Objectives, Cont'd

Key Controls	Related Risks	Control Objectives
4. Final review of report	•Reports produced by OES system may contain calculation errors or other inaccuracies	•Controls ensure that transactions are summarized, and calculations are performed accurately and consistently
5. e-Filing of reports	•Reports may be transmitted using wrong template (federal, state); may be transmitted late; may not identify missing delivery acknowledgements	•Controls ensure that proper template is selected and used •Controls ensure report delivery is timely and evidence of receipt is obtained from regulator

6. IT General Controls to Test, That Meet the Control Objectives

Control Objectives	IT General Controls (Examples)
•Controls ensure that all tasks have assigned due dates and users	•Application and Database security – table update functionality •Change control – application code
•Controls ensure that data entered conforms to business rules (e.g. format); errors are rejected	•Application and Database security – input transactions •Change control – application code – edit rules and error identification
•Controls ensure calculations and summarizations are correctly performed and results appropriately displayed to users for review	•Change control – application code – critical calculations and report format •Application, Database & OS security – display and modify results

7. Perform a "reasonable person," holistic review of all the key controls identified



COSO Categories:

- Control Environment
- Risk Assessment
- Control Activities
- Monitoring
- Information and Communication

Q: Extremely good or bad?? Impact the audit plan?

8. Scope of the Review – Integrated Audit – Coverage of All Business Risks

Now that the detailed scoping for this project is finished ….

- Am I covering each of the business risks?
- Do I need to reference and rely upon something that is out of scope, so management understands what I did NOT do?
  - Example: Purchasing system covered in another audit
- Am I planning to rely on the IT general controls?
  - Would a reasonable person with this same information come to the same conclusions?
  - Can I really conclude the way I did?

Scope Change Needed

- What if some plants may not have migrated to the new OES system?
  - Continuing to operate on spreadsheets
  - Much higher risk of error in this environment
  - Complex calculations and logic require explanation and documentation
  - Change control and security needed
- Must decide: expand the scope, or exclude from scope and explain in final audit report
  - Impact on assurance I can give?

Conclusions and Lessons Learned

- GAIT useful for scoping SOX 404 and any IT audit work
- GAIT results in the ability to do less test work overall
  - However, the work that is completed is clearly targeted to cover the key business risks

Now, let's look at how to write up our findings …..

Conclusions and Lessons Learned, Cont'd

- Improved audit comment wording helps to connect to things management cares about:
  - "We noted poor change control procedures and were unable to obtain comfort that all changes were authorized and tested as required"

    -- vs. --

  - "Poor change control practices introduced the risk of unauthorized or untested changes to key data such as annual threshold amounts for toxic chemical releases. Given the level of precision applied to reviewing the final report downstream, it is unlikely management would detect such errors. Our testing disclosed numerous "break/fix" changes had been made to code or data without supervisory review and approval or notifying the users."

Conclusions and Lessons Learned, Cont'd

- Linking finding to business risk makes it real:
  - "We noted that system edits did not ensure user input was in the proper format or that non-allowable materials were rejected from further processing"

  -- vs. --

  - "Edit routines for user input were not properly designed to ensure only designated chemical types could be entered into the "Product_Type_User" table in the Oracle database. We noted eight products had been entered incorrectly, which resulted in the OES system adding the related transaction quantities to the "Miscellaneous" default category in error. Because the final report review process was being conducted at a very high level, these errors were not detected and the final report contained a minor level of misstatement"

More Information . . .

- **GAIT Resources**
  www.theiia.org
- **Questions? Ask Dr. GAIT**
  drgait@theiia.org
- **Edward Hill**
  edward.hill@protiviti.com

protiviti®
Independent Risk Consulting

Know Risk.
Know Reward.