日本ＩＴガバナンス協会

Monitoring of Internal Control Systems and IT

Governance Challenges in a Cloud Computing World

Everett C. Johnson, CPA

Deloitte LLP, Partner (retired)

Past International President - ITGI and ISACA

日本ＩＴガバナンス協会

Agenda

- Monitoring Defined
- Basic COSO Concepts
- Effects of IT on Monitoring
- IT Governance Challenges and Cloud Computing
- ISACA Publication on Monitoring

日本ＩＴガバナンス協会

Monitoring within the COSO Framework

ITGI Japan

日本ＩＴガバナンス協会

Definition of Monitoring

- Monitoring consists of the processes, procedures, tools and activities that an enterprise puts in place to ensure that internal control continues to operate effectively.

ITGI Japan

日本ＩＴガバナンス協会

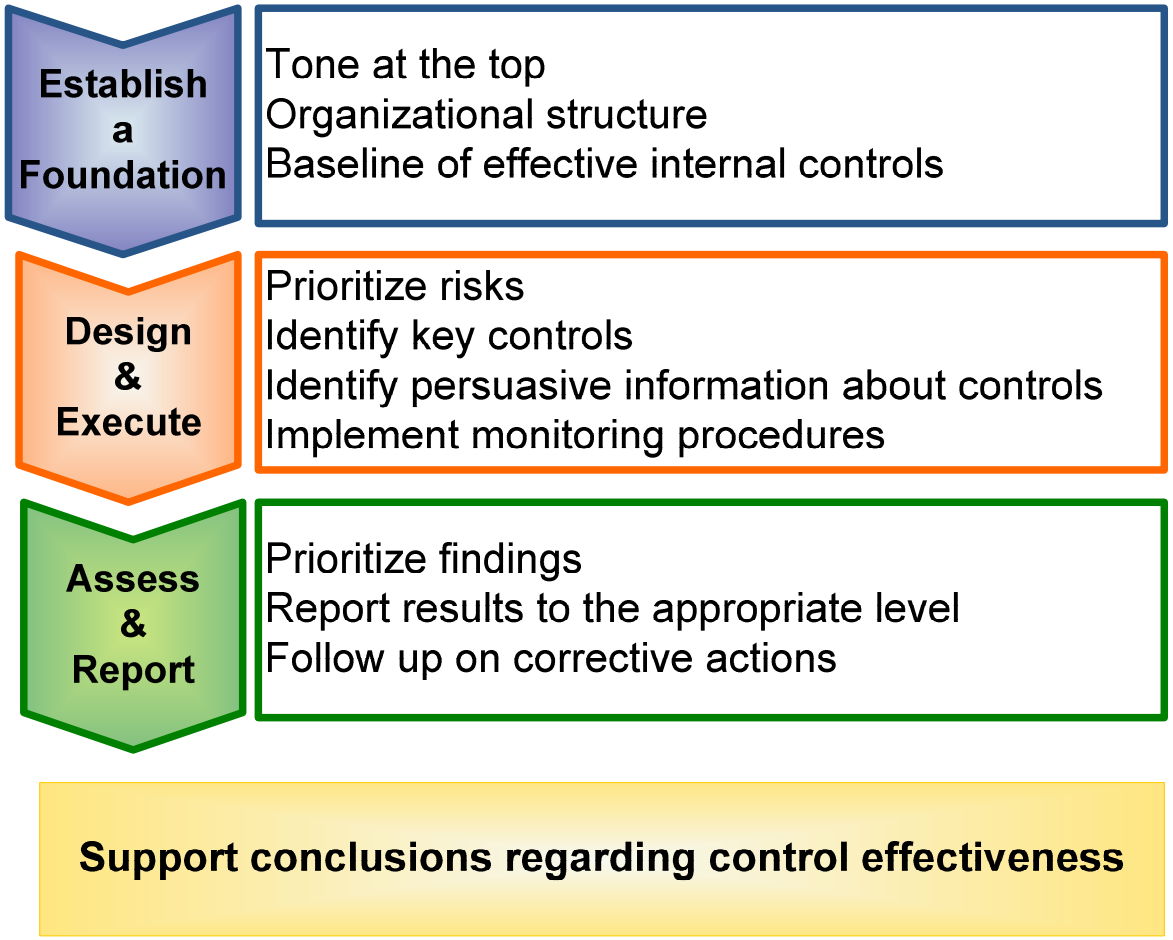
COSO Monitoring

- Focuses on the **monitoring of controls**
- Includes monitoring of controls over
  - Reliability of financial reporting
  - Effectiveness and efficiency of operations
  - Compliance with applicable laws and regulations
- Does **not** include monitoring of performance efficiencies and operational metrics, unless they provide evidence of control effectiveness

ITGI Japan

日本ＩＴガバナンス協会

COSO Model for Monitoring



ITGI Japan
日本ＩＴガバナンス協会

Agenda

- Monitoring Defined
- Basic COSO Concepts
- Effects of IT on Monitoring
- IT Governance Challenges and Cloud Computing
- ISACA's Publication on Monitoring

ITGI Japan

日本ＩＴガバナンス協会

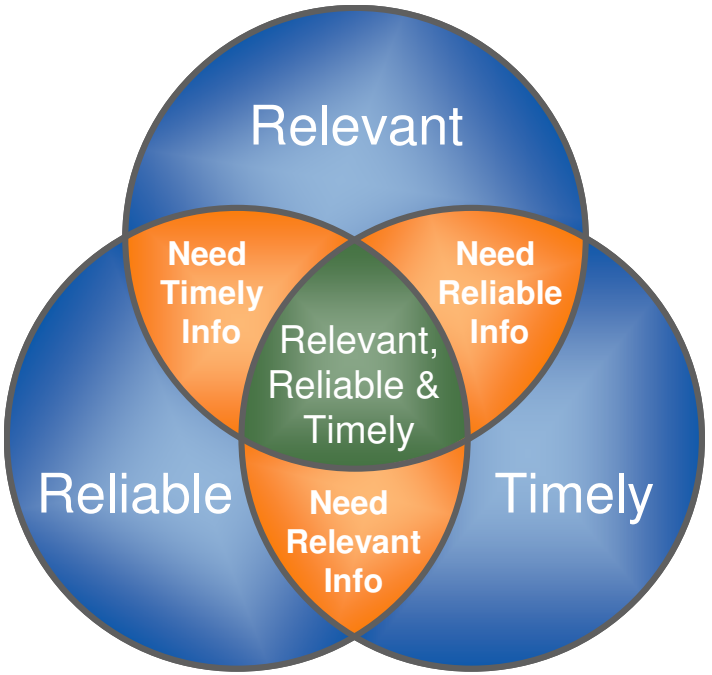
Key Controls

- Provide support for a reasonable conclusion about the entire internal control system's ability to achieve the underlying objectives
- Often have one or more of the following characteristics:
  - Their failure could materially affect the objectives for which the evaluator is responsible
  - Their failure might not be detected in a timely manner by other controls
  - Their operation might prevent or detect other control failures before they become material to the enterprise's objectives

日本ＩＴガバナンス協会

Elements of Persuasive Information

- Persuasive information:
  - Suitable (quality)
    - Relevant:
      - » Direct
      - » Indirect
    - Reliable
      - » Accurate
      - » Verifiable
      - » Objective
    - Timely
  - Sufficient (quantity)



ITGI Japan

日本ＩＴガバナンス協会

Basic COSO Concepts

- Types of Information
  - **Direct information** substantiates the operation of controls.
  - **Indirect information** *may* indicate a change or failure in the operation of controls or measurement of a business process.

- Types of Monitoring
  - **Ongoing monitoring** monitors the effectiveness of internal control in the ordinary course of operations.
  - **Separate evaluations** are designed to evaluate processes and controls periodically and are not ingrained in the routine operations of the enterprise.

日本ＩＴガバナンス協会

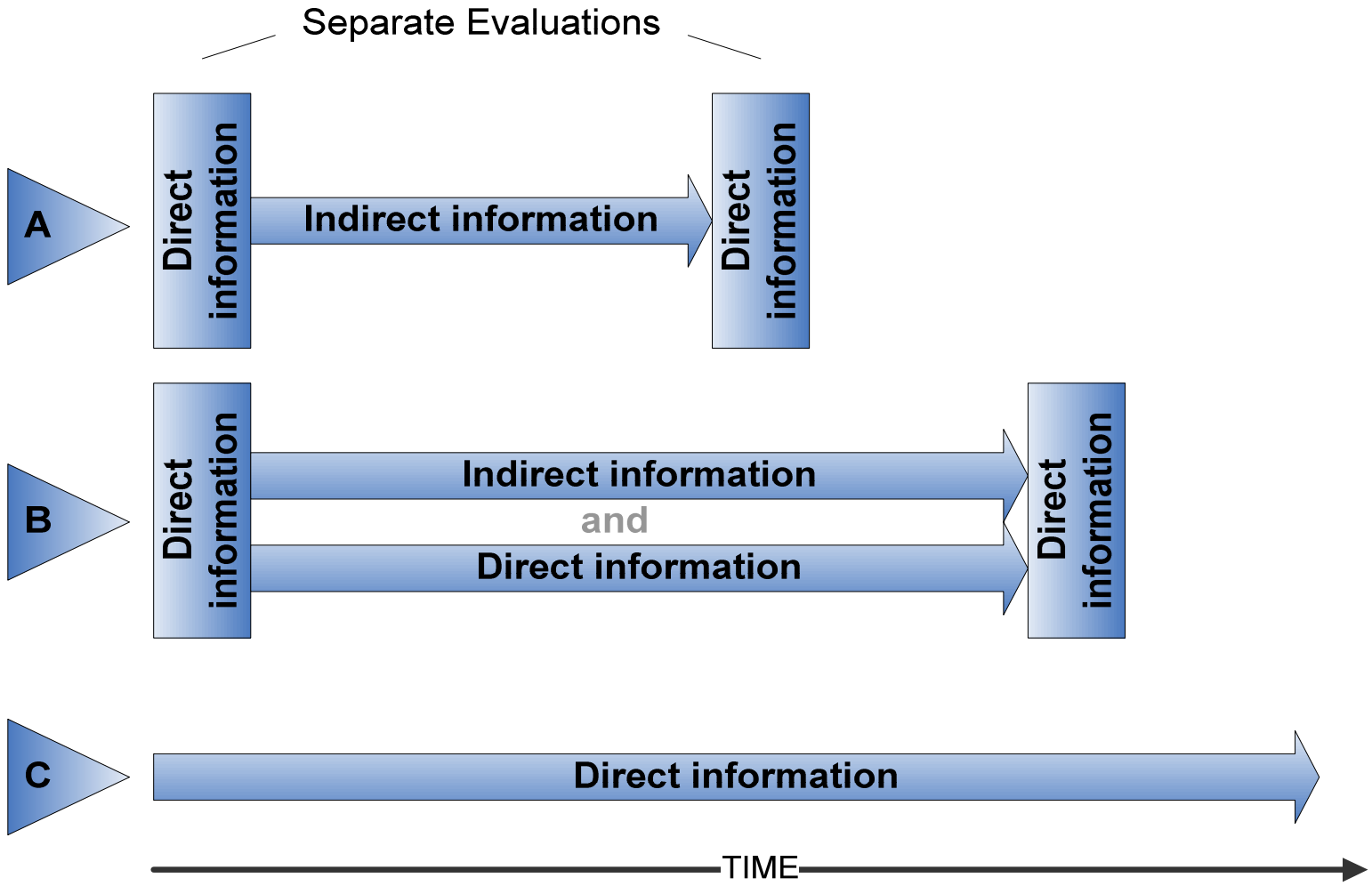
Achieving the Right Balance

	Direct Information	Indirect Information
Ongoing monitoring	• Typically most persuasive • Especially valuable in high-risk areas	• Can enhance monitoring efficiency • Provides support to direct information
Separate evaluation	• Primarily used to revalidate conclusions reached through ongoing monitoring	• Typically least persuasive • Can help scope other separate evaluation procedures

ITGI Japan

日本ＩＴガバナンス協会

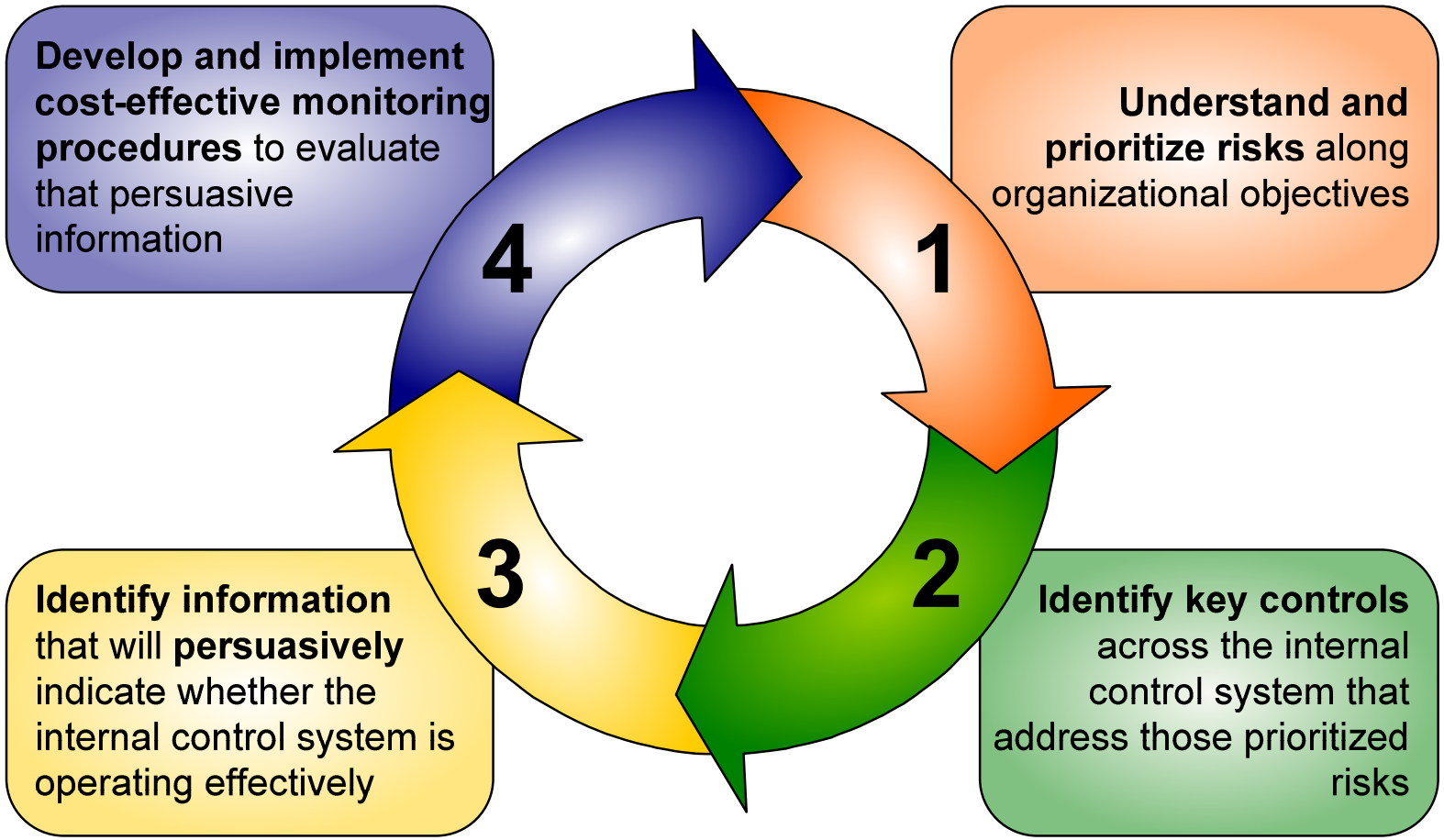
Achieving the Right Balance



ITGI Japan

日本ＩＴガバナンス協会

Design and Execute



ITGI Japan
日本ＩＴガバナンス協会

Identifying a Monitoring Activity

- What is the key control to be monitored?
- What information indicates control effectiveness?
- What is the monitoring process?

ITGI Japan
日本ＩＴガバナンス協会

Bottom-line Benefits of Monitoring

- Ensures that **internal controls** continue to operate effectively
- Provides **timely evidence** of changes that have occurred within internal controls
- Facilitates remediation **before** adverse consequences occur
- **Reduce effort and cost** of GRC

日本ＩＴガバナンス協会

Agenda

- Monitoring Defined
- Basic COSO Concepts
- Effects of IT on Monitoring
- IT Governance Challenges and Cloud Computing
- ISACA's Publication on Monitoring

ITGI Japan

日本ＩＴガバナンス協会

IT and Monitoring

- Monitoring of controls:
  - Application controls
    - IT-dependent manual controls
    - Automated controls
  - IT general controls

- Automating the monitoring process:
  - Controls monitoring
  - Reporting and follow-up

ITGI Japan

日本ＩＴガバナンス協会

Key Concepts for Monitoring and IT

1. If key controls are automated, relevant underlying IT general controls usually need to be monitored.
2. If key controls are manual, but depend on information produced by IT, they are usually dependent on selected IT general controls, which also may need to be monitored.
3. The risk assessment process and the availability of computerized information drive which IT and manual controls will be monitored.
4. Information needed for monitoring may be available only from an IT process.
5. Monitoring of IT controls and automated monitoring often can be leveraged to address multiple monitoring objectives.
6. IT facilitates a repetitive, and often a continuous, monitoring process.

日本ＩＴガバナンス協会

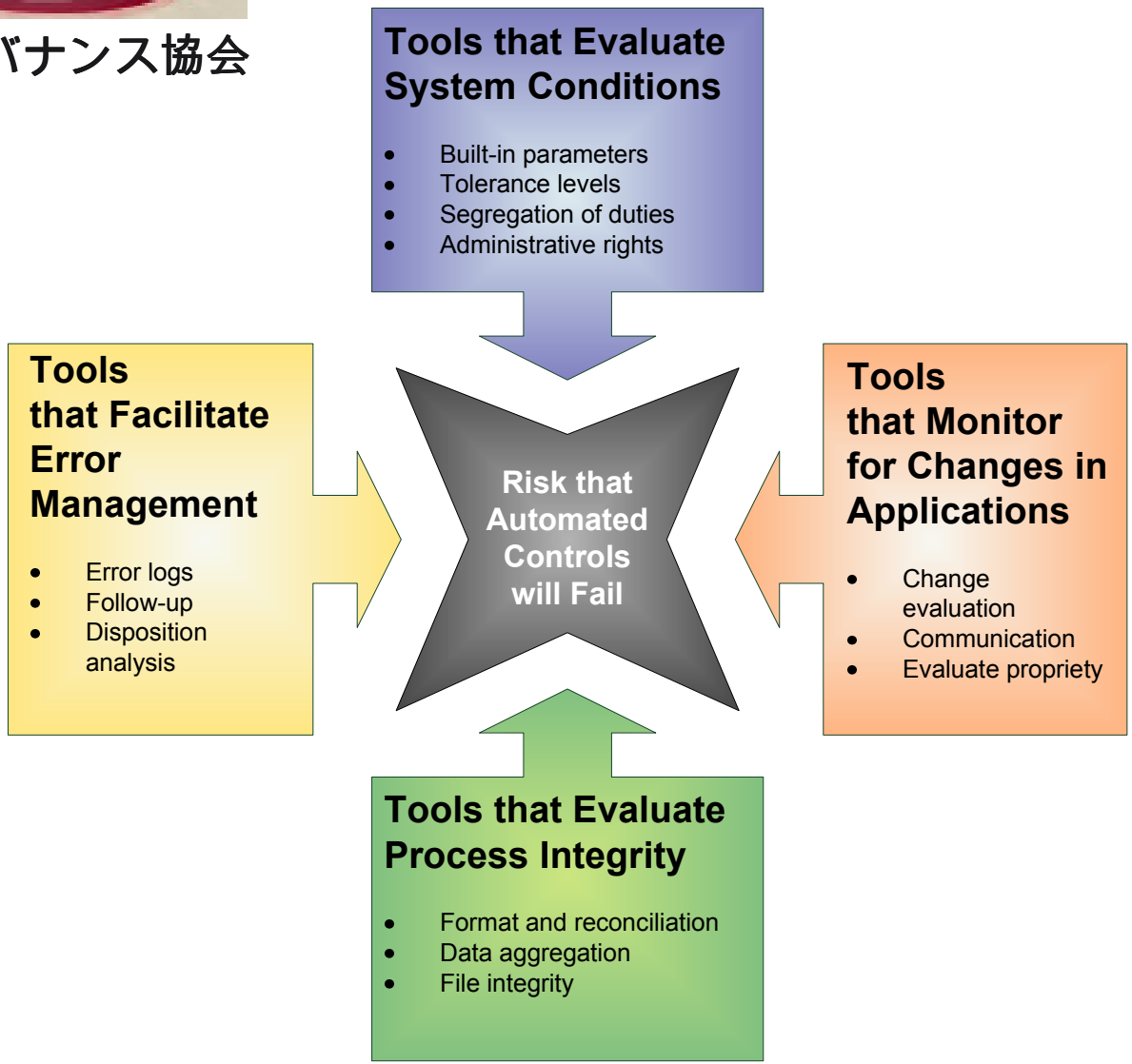
Benefits of IT Monitoring

- Earlier identification of problems
- Timelier corrective action
- Increased leverage
- Increased consistency

ITGI Japan

日本ＩＴガバナンス協会

Monitoring Tools



ITGI Japan
日本ＩＴガバナンス協会

Benefits of Automating the Monitoring Process

- Opportunities that are not feasible manually
  - Integration across systems and geographies
  - Evaluation of system conditions
- Further improvement
  - Effectiveness
  - Efficiency
  - Timeliness
- Leverage of existing investment in systems and data

日本ＩＴガバナンス協会

Agenda

- Monitoring Defined
- Basic COSO Concepts
- Effects of IT on Monitoring
- IT Governance Challenges and Cloud Computing
- ISACA's Publication on Monitoring

日本ＩＴガバナンス協会

IT Governance Challenges and Cloud Computing

- Relationship of Monitoring and IT Governance
  - Integration of monitoring and risk assessment
  - Monitoring of some IT controls
  - Monitoring of the monitoring program
- Cloud Computing Challenges
  - Getting behind the “cloud”
  - Contract provisions for monitoring, auditing and reporting
  - Availability of an audit report on service organization controls
- New reporting on service organization controls

日本ＩＴガバナンス協会

Reporting on Service Organization Controls "The End of SAS 70"

- USA audit standard SAS No. 70
  - Became a defacto global standard
  - Internal controls over financial reporting
  - No accepted criteria for reporting on controls
  - Auditor-to-auditor communication
- New international standard ISAE 3402 and USA standard SSAE 16
  - Cloud computing and outsourcing elevated the need for a new standard
- Two new supporting guides for two types of detailed reports
  - Service organization controls (SOC-1) related to financial reporting
  - Service organization controls (SOC-2) related to security, availability, processing integrity, confidentiality and privacy
- Promotion of a third type of report
  - Short-form general-use report on service organization controls (SOC-3) related to security, availability, processing integrity, confidentiality and privacy
- Helps service organizations demonstrate reliability and trust

ITGI Japan

日本ＩＴガバナンス協会

Contents of a SOC-2 Report on a Cloud Computing Provider

- Report on controls related to one or more of the following
  - Security, availability, processing integrity, confidentiality and/or privacy
  - Based on AICPA/CICA Trust Services Principles and Criteria developed internationally
  - Can cover a period of time, such as 6 months or 1 year
- Contains
  - Cloud computing provider's description of its system and infrastructure
  - All the criteria, for the principle(s) selected (such as security), and a listing of controls designed to meet those criteria
  - A description of changes to the system and controls during the period
  - An assertion by cloud computing management about the description and the controls
  - The auditor's report and opinion on the fairness of presentation of the description and whether the controls are suitably designed to meet the criteria and operated effectively
  - Details of the testing performed by the auditor
- Comments
  - SOC-1 and SOC-2 use is restricted to customers, regulators, auditors, etc.
  - May contain too much detail for some purposes
  - SOC-3 may be better in some situations:
    - Short-form report
    - Doesn't include details of controls or tests
    - Intended for general use (not restricted)

日本ＩＴガバナンス協会

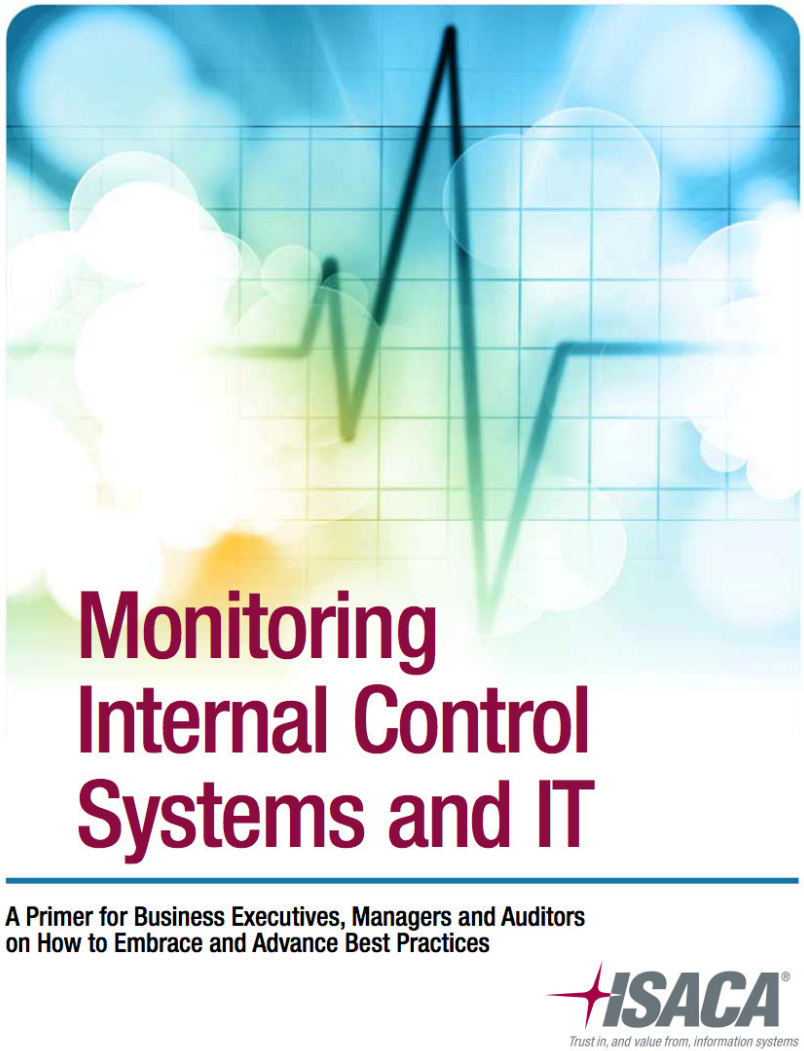
Agenda

- Monitoring Defined
- Basic COSO Concepts
- Effects of IT on Monitoring
- IT Governance Challenges and Cloud Computing
- ISACA's Publication on Monitoring

ITGI Japan

日本ＩＴガバナンス協会

New ISACA Publication



日本ＩＴガバナンス協会

Publication Audience

- IT/assurance practitioners
- Audit/security practitioners
- Compliance practitioners
- IT and User Managers
- Executives responsible for IT governance

日本ＩＴガバナンス協会

Publication Overview

- **Overview of the Use of Internal Controls and Monitoring**
- **Foundational Concepts and Principles of Monitoring**
- **How to Design and Execute an IT Monitoring Process**
- **How to Automate Monitoring of Controls to Increase Efficiency and Effectiveness**
- **Other Important Considerations**
- Appendices

ITGI Japan

日本ＩＴガバナンス協会

Session Summary

- Monitoring Defined
- Basic COSO Concepts
- Effects of IT on Monitoring
- IT Governance Challenges and Cloud Computing
- ISACA's Publication on Monitoring

日本ＩＴガバナンス協会

Thank you!

ありがとう