ARCHITECTURE FOR A DISTRIBUTED ADAPTABLE AUDITABLE FINANCIAL REPORTING AND MANAGEMENT OVERSIGHT SYSTEM

Pre-defense: Kevin M. Burns

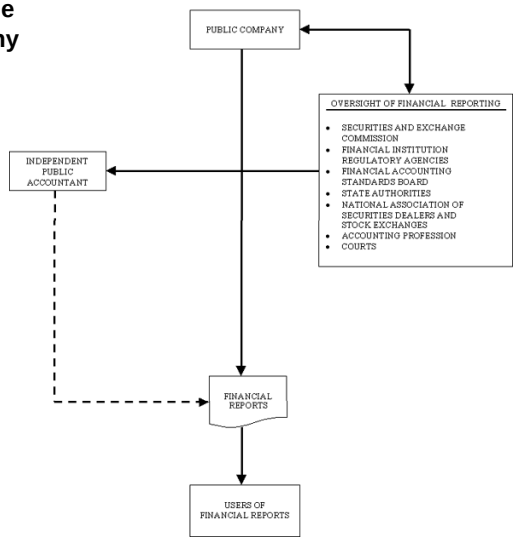
Motivation

- Integration of heterogeneous data and applications during a public company's financial close is a key challenge faced by most Finance departments.
- SEC has accelerated periodic report filing dates and disclosures on a graduated scale from 2002 thru 2005
- The public company is required, per the Sarbanes-Oxley Act (SOX) of 2002, to provide confidence in any financial statements released to the public through internal controls
  - ❖ Accountability
  - ❖ Controlled processes
  - ❖ Auditability
- PCAOB recognizes Information Technology plays a large role in enabling Internal Controls
- Regulation and Standards are evolving; therefore, people and systems must be adaptable to changes

Background

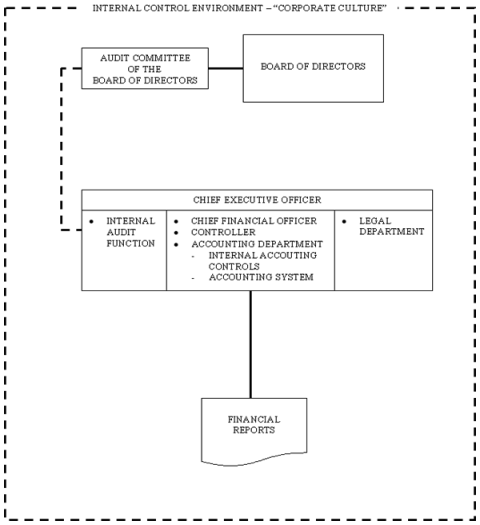
The Public Company

Financial Reporting in the Public Company



The Public Company

Internal Controls



Current Regulations

Regulatory Authorities

- **Securities and Exchange Commission**
  - Securities Act of 1933 and the Securities Exchange Act of 1934
    - Division of Corporation Finance
  - Investment Company Act of 1940
  - **Acceleration of Periodic Report Filing Dates and Disclosures (2002)**
  - **Sarbanes-Oxley Act 2002**
    - **Public Company Accounting Oversight Board (PCAOB)**
    - **COSO's "Internal Control – Integrated Framework"**

Acceleration of Periodic Report Filing Dates and Disclosures (2002)

For Fiscal Years Ending On or After	Form 10-K Deadline	Form 10-Q Deadline
December 15, 2002	90 days after fiscal year end	45 days after fiscal quarter end
December 15, 2003	75 days after fiscal year end	45 days after fiscal quarter end
December 15, 2004	60 days after fiscal year end	40 days after fiscal quarter end
December 15, 2005	60 days after fiscal year end	35 days after fiscal quarter end

Sarbanes-Oxley Act 2002

SEC Chairman William Donaldson -

- *"Simply complying with the rules is not enough. They should, as I have said before, make this approach part of their companies' DNA. For companies that take this approach, most of their major concerns about compliance disappear. Moreover, if companies view the new laws as opportunities – opportunities to improve internal controls, improve the performance of the board, and improve their public reporting – they will ultimately be better run, more transparent, and therefore more attractive to investors. "*
- *"A strong central focus of the Sarbanes-Oxley Act is to enhance the integrity of the audit process and the reliability of audit reports on issuers' financial statements. As discussed below, the Commission has taken the actions directed by the Act and, when appropriate, pursued additional measures with the goal of restoring public confidence in the independence and performance of auditors of public companies' financial statements. "*

Sarbanes-Oxley Act 2002

- Section 3: Commission Rules and Enforcement.
- Section 302: Corporate Responsibility For Financial Reports.
- Section 404: Management Assessment Of Internal Controls.
  - **COSO's "Internal Control – Integrated Framework"**
- Section 409: Real Time Disclosure.
- Section 802: Records Retention.
- Section 906: Certification.

Public Company Accounting Oversight Board

- **PCAOB Auditing Standard No. 2**
  - Requirements for auditors to understand the flow of transactions, including how transactions are initiated, authorized, recorded, processed and reported
  - *"The audit of internal control over financial reporting and the audit of the company's financial statements are an integrated activity and are required by the (Sarbanes-Oxley) Act to be a single engagement."*
  - *"The nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting."*

COSO's "Internal Control – Integrated Framework"

Internal control is broadly defined as a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- ❖Reliability of financial reporting.
- Compliance with applicable laws and regulations.

COSO's "Internal Control – Integrated Framework"

Internal control consists of five interrelated components:

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

Information Technology Controls

- IT Governance Institute (ITGI)
  - **COBIT**
    - comprehensive framework for managing risk and control of IT, comprising four domains, 34 IT processes and 318 detailed control objectives
    - COBIT provides controls that address operational, financial reporting and compliance objectives
  - ❖ **IT Control Objectives For Sarbanes-Oxley**
- Other IT control guidelines, including ISO (International Organization for Standardization) 17799 and the Information Technology Infrastructure Library (ITIL), are two other guidelines that deal with information security but do not address specific all financial reporting objectives (i.e. application controls like completeness, accuracy and validity).

IT Control Objectives For Sarbanes-Oxley

- Combines COBIT, PCAOB Standard No. 2 and COSO

CoaT Areas/COSO Components

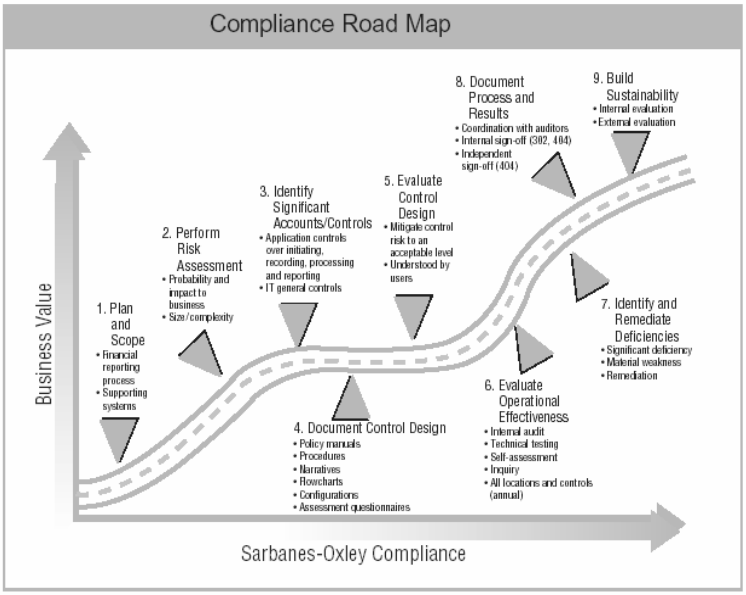
Company Level	Activity Level	CoaT Area	COSO Component: Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
Plan and Organize (IT Environment)							
●		IT strategic planning	●	●		●	●
●		Information architecture			●	●	
		Determine technological direction					
●		IT organization and relationships	●			●	
		Manage the IT investment					
●		Communication of management aims and direction	●			●	●
●		Management of human resources	●			●	
●		Compliance with external requirements				●	●
●		Assessment of risks		●			
		Manage projects					
●		Management of quality	●		●	●	●
Acquire and Implement (Program Development and Program Change)							
		Identify automated solutions					
	●	Acquire or develop application software			●		
	●	Acquire technology infrastructure			●		
	●	Develop and maintain policies and procedures			●	●	
	●	Install and test application software and technology infrastructure			●		
	●	Manage changes			●		●
Deliver and Support (Computer Operations and Access to Programs and Data)							
	●	Define and manage service levels	●		●		●
	●	Manage third-party services	●	●	●		●
●		Manage performance and capacity			●		●
		Ensure continuous service					
	●	Ensure systems security			●	●	●
		Identify and allocate costs					
●		Educate and train users	●			●	
		Assist and advise customers					
	●	Manage the configuration			●	●	
	●	Manage problems and incidents			●	●	●
	●	Manage data			●	●	
●		Manage facilities		●			
	●	Manage operations			●	●	
Monitor and Evaluate (IT Environment)							
●		Monitoring				●	●
●		Adequacy of internal controls					●
●		Independent assurance	●				●
●		Internal audit					●

COBIT and PCAOB Standard No. 2

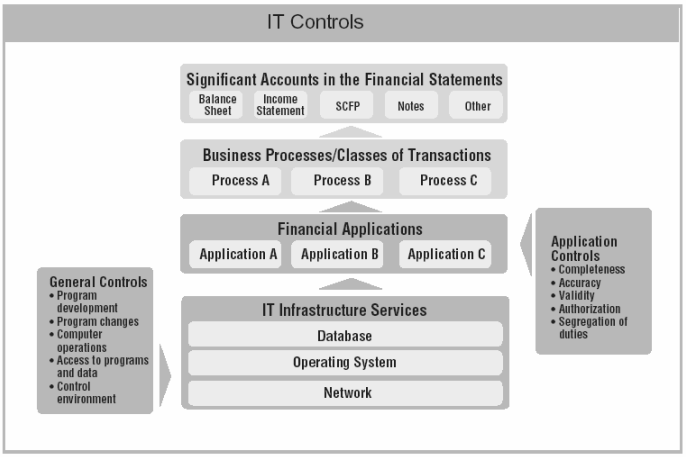
Control Processes

CoaT Control Objective Heading	PCAOB IT General Control Heading: Program Development	Program Changes	Computer Operations	Access to Programs and Data
1. Acquire or develop application software.	●	●	●	●
2. Acquire technology infrastructure.	●	●	●	
3. Develop and maintain policies and procedures.	●	●	●	●
4. Install and test application software and technology infrastructure.	●	●	●	●
5. Manage changes.		●		●
6. Define and manage service levels.	●	●	●	●
7. Manage third-party services.	●	●	●	●
8. Ensure systems security.			●	●
9. Manage the configuration.			●	●
10. Manage problems and incidents.			●	
11. Manage data.			●	●
12. Manage operations.			●	●

IT Control Objectives For Sarbanes-Oxley

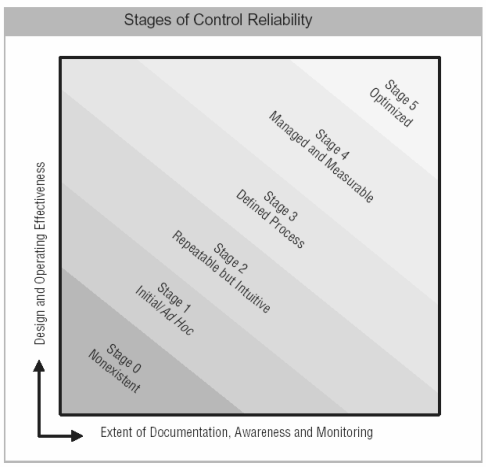


IT Control Objectives For Sarbanes-Oxley



IT Control Objectives For Sarbanes-Oxley

Financial Control Maturity Model



SOX-Section 404

	Stage 0 Non-existent	Stage 1 Initial/Ad Hoc	Stage 2 Repeatable & Intuitive	Stage 3 Defined Process	Stage 4 Managed & Measurable	Stage 5 Optimized
Characteristics	**NO control process or related procedures** Compliance challenge not understood or recognized	**Controls, policies, and procedures not in place** Compliance challenge recognized NO employee awareness of responsibilites	**Controls in place but not fully documented** Event and disclosure process in place NO ongoing control evaluations	**Controls in place and adequately documented** Ongoing evaluation and remediation of controls Broad employee awareness	**Initial use of technolgy to manage** Effectiveness of controls evaluated on a periodic basis Minimal event and disclosure process re-evaluations	**Technology leveraged to fullest extent** Enterprisewide control and risk program in place Self-assessment process to evaluate design and effectiveness of controls
Implications	NO capability to be in compliance	Insufficient controls and documentation to support attestation	Controls in place Documentation can not support attestation	**Sufficient documentation to support attestation with MAJOR on-going effort**	Lowered effort to maintain control documentation	**Reduced costs, improved decision making and internal resources used effectively** **Information is timely and reliable**

IT Control Objectives For Sarbanes-Oxley

Documenting Compliance

- Company level
- Activity level

Problem Statement

Problem Statement

SOX

- Section 302 deals with quarterly and annual disclosures of material weaknesses in internal controls that can effect financial statements.
- Section 404 mandates that the public company use a recognized internal control framework and to annually assess the effectiveness of its implementation of the framework over the financial reporting process, in conjunction with an attestation by its registered public accountant as to the assessment of management
- Section 409 requires that these disclosures occur in "*real or near-real time"*

Acceleration of Periodic Report Filing Dates and Disclosure

PCAOB Auditing Standard No. 2

- treat the audit of internal controls and the annual audit of financial statements as an "*integrated activity*"

Problem Statement

Internal Control System
- Infrastructure controls
- Application controls
- Real-time self documenting controls

Financial Reporting System
- Accelerated reporting → Virtual close
- Integration of heterogeneous components
  - Data synchronization
  - Business Rules synchronization & change management
    - Compliance
    - Metadata synchronization
    - Derivations
- Multi-location issues

Feedback loops

Current State of Technologies

XML

- Extensible Markup Language (XML)
- Self describing documents
  - Elements & Attributes
  - Namespaces
- Well-Formedness
- Processing XML
  - SAX
  - DOM
  - XSLT (XSL)

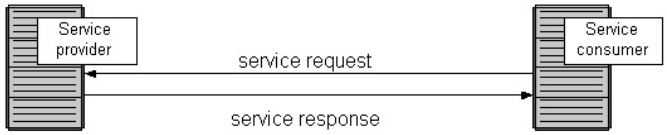
XML Schema

- Portable, platform independent, type system for XML based computing systems
- 2 parts
  - DataTypes (simple types-restrictions,union,list; complex types and extensibility)
  - Describing XML instance document structure and constraining the contents
- Valid Documents

Service Oriented Architectures

Distributed systems

- Distributed object systems
- SOA



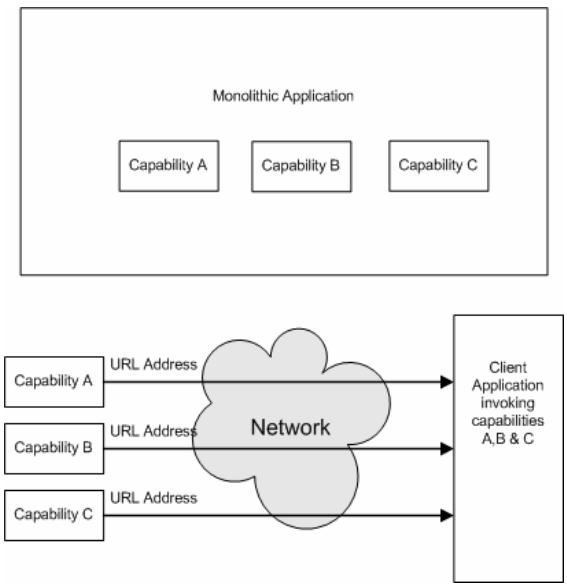
Service Oriented Architectures

In general SOA and Web services are most appropriate for applications: [26]

- That must operate over the Internet where reliability and speed cannot be guaranteed;
- Where there is no ability to manage deployment so that all requesters and providers are upgraded at once;

Web Services

- Web services are instances of the Service Oriented Architecture (SOA) pattern
- W3C- *"a Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards"*

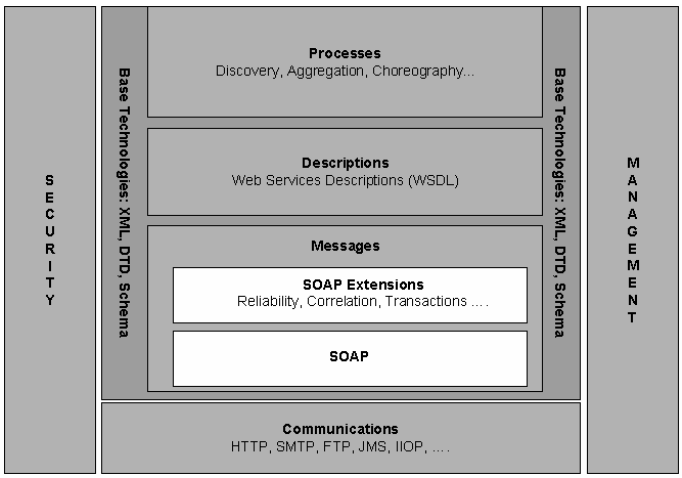


Web Services

The capabilities provided by a web service can fall into a variety of categories, including:

- Functions, such as a routine for calculating Earnings Per Share.
- Data, such at fetching the trial balance of a foreign subsidiary.
- Business processes, such as inter-company elimination processing.

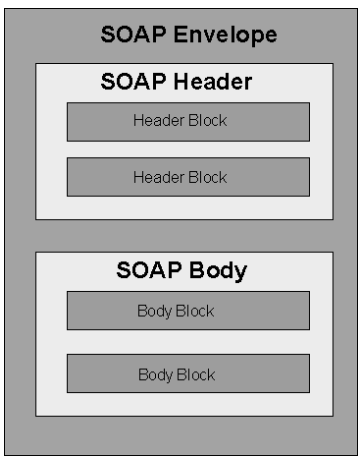
Web Services Technologies



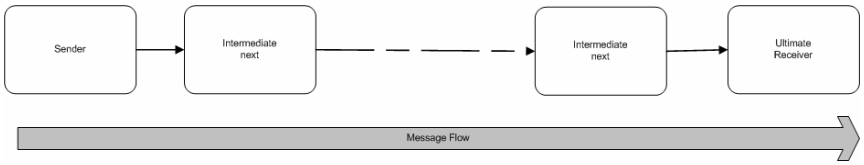
SOAP

- Service Oriented Architecture Protocol: In the general case, a SOAP message represents the information needed to invoke a service or reflect the results of a service invocation, and contains the information specified in the service interface definition.
- Simple Object Access Protocol: When using the optional SOAP RPC Representation, a SOAP message represents a method invocation on a remote object, and the serialization of in the argument list of that method that must be moved from the local environment to the remote environment.

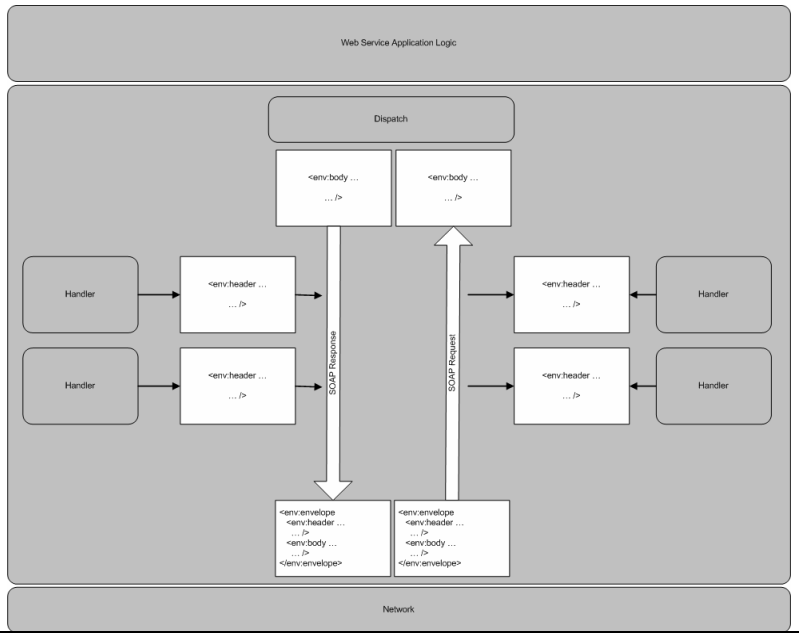
SOAP Message



SOAP Message Path



SOAP Server



WSDL

According to the W3C, *"Web Services Description Language (WSDL) provides a model and an XML format for describing Web services. WSDL enables one to separate the description of the abstract functionality offered by a service from concrete details of a service description such as "how" and "where" that functionality is offered."*

WSDL

```
<?xml version="1.0" encoding="utf-8"?>
<definitions>
  <types>
  </types>
  <message ...>
  </message>
  <interface>
    <operation>
      <input ... />
      <output ... />
    </operation>
  </interface>
  <binding ...>
    <soap:binding ... />
    <operation ... >
      <soap:operation ... />
      <input>...</input>
      <output>...</output>
    </operation>
  </binding>
  <service ...>
    <port ...>...</port>
  </service>
</definitions>
```

Key is extensibility in WSDL schema (substitution group heads)

Business Rule Management Systems

What are business rules?

According to the Business Rules Group

Business Rules from the business perspective

From the business perspective,
...a business rule is a directive, intended to influence or guide business behavior, in support of business policy that has been formulated in response to an opportunity, threat, strength, or weakness.

Business Rules from the I/S perspective

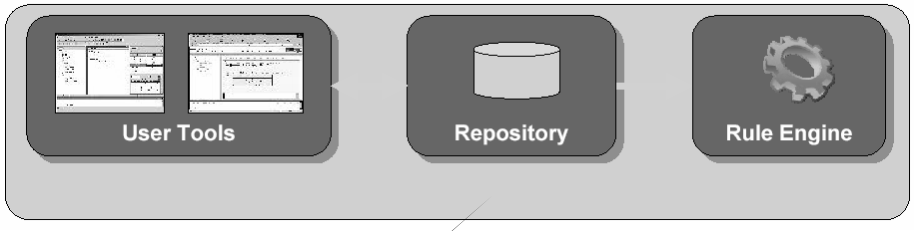
From the information system perspective,
...a business rule is a statement that defines or constrains some aspect of the business. It is intended to assert business structure, or to control or influence the behavior of the business.

What is a BRMS?

- An intuitive application for business users to author and maintain rules
- A complete and secure environment for developers to manage and deploy rules
- A system that controls access to rules by role-based access levels

Offspring of Expert Systems

Business Rule Management Systems



Challenges:

Rule Testing

Change Management & Complete audit trail

PROPOSED SOLUTION

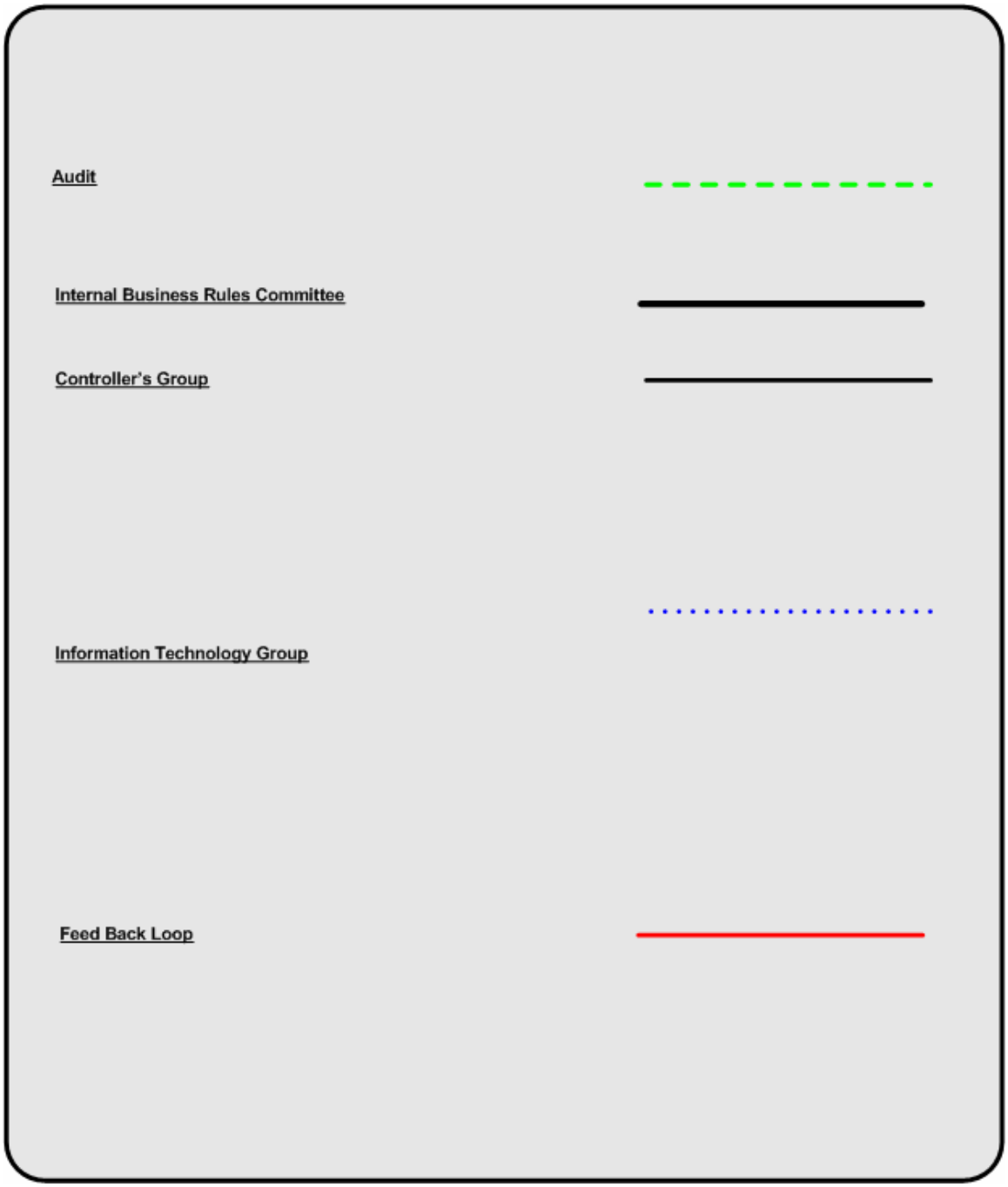
"Work in Progress" – see attached diagrams

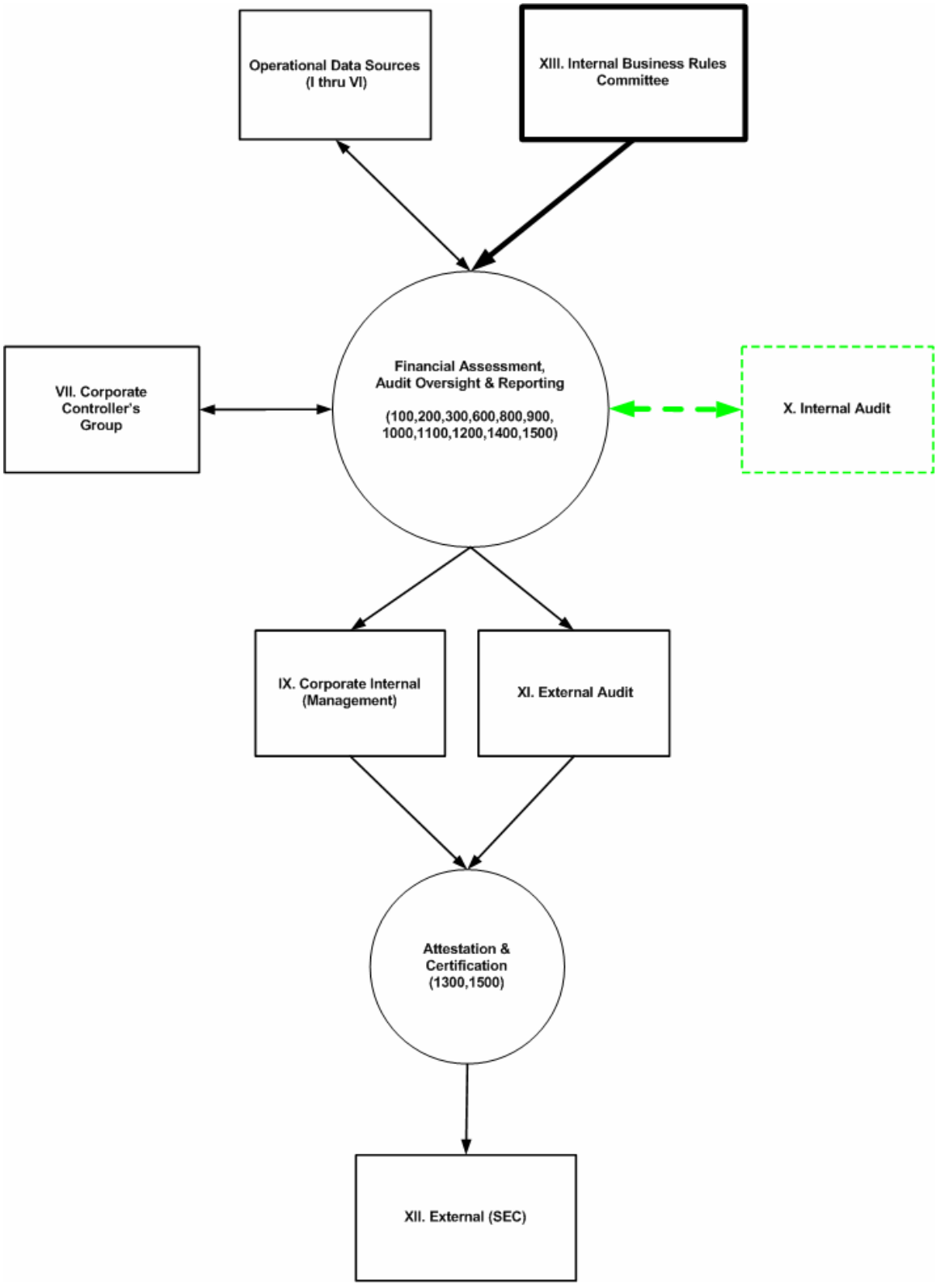
Additional Chapters

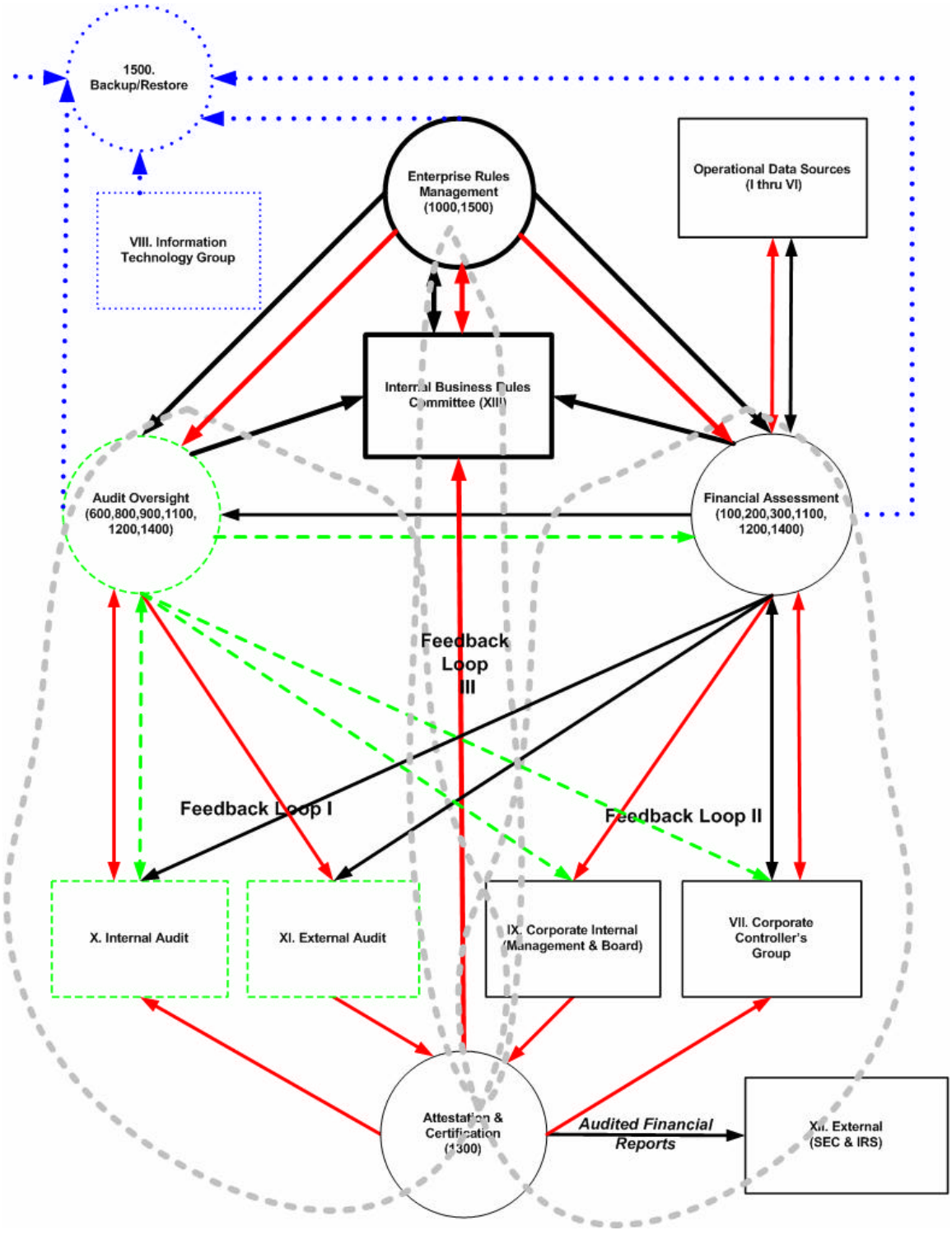
- DISCUSSION OF THE ADVANTAGES OF THE SOLUTION
- FUTURE WORK

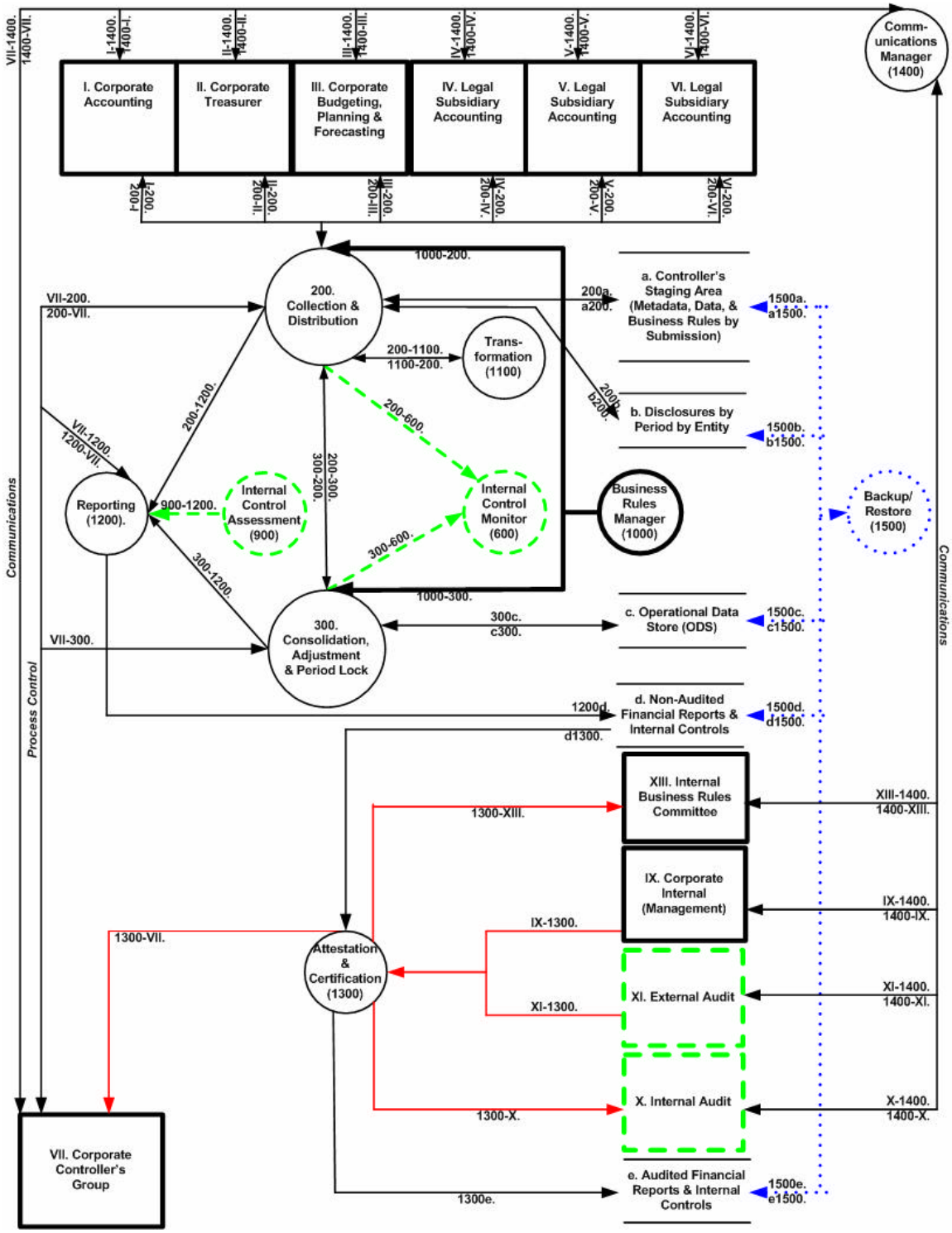
- Review Manuscript "Table of Contents"

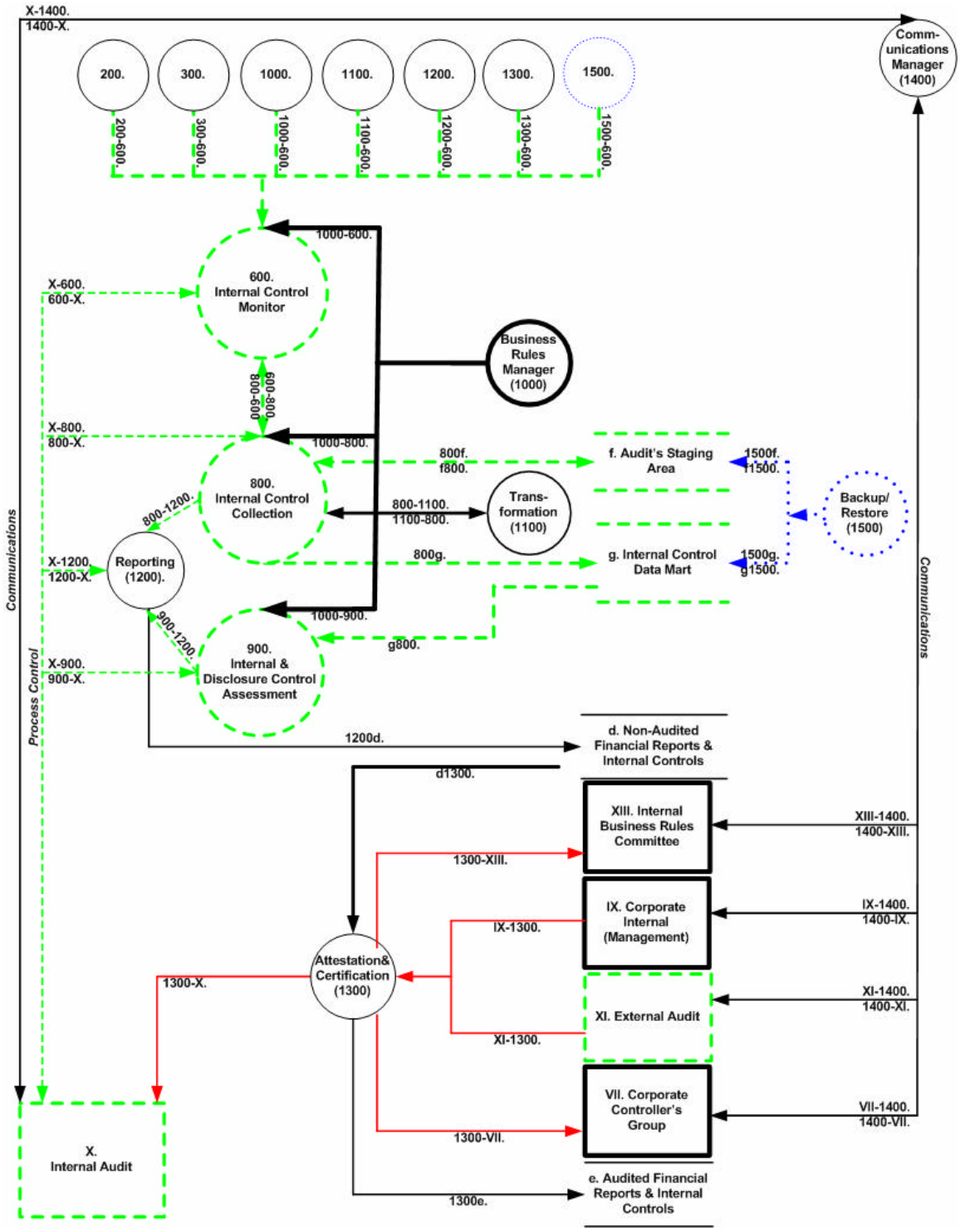
Questions

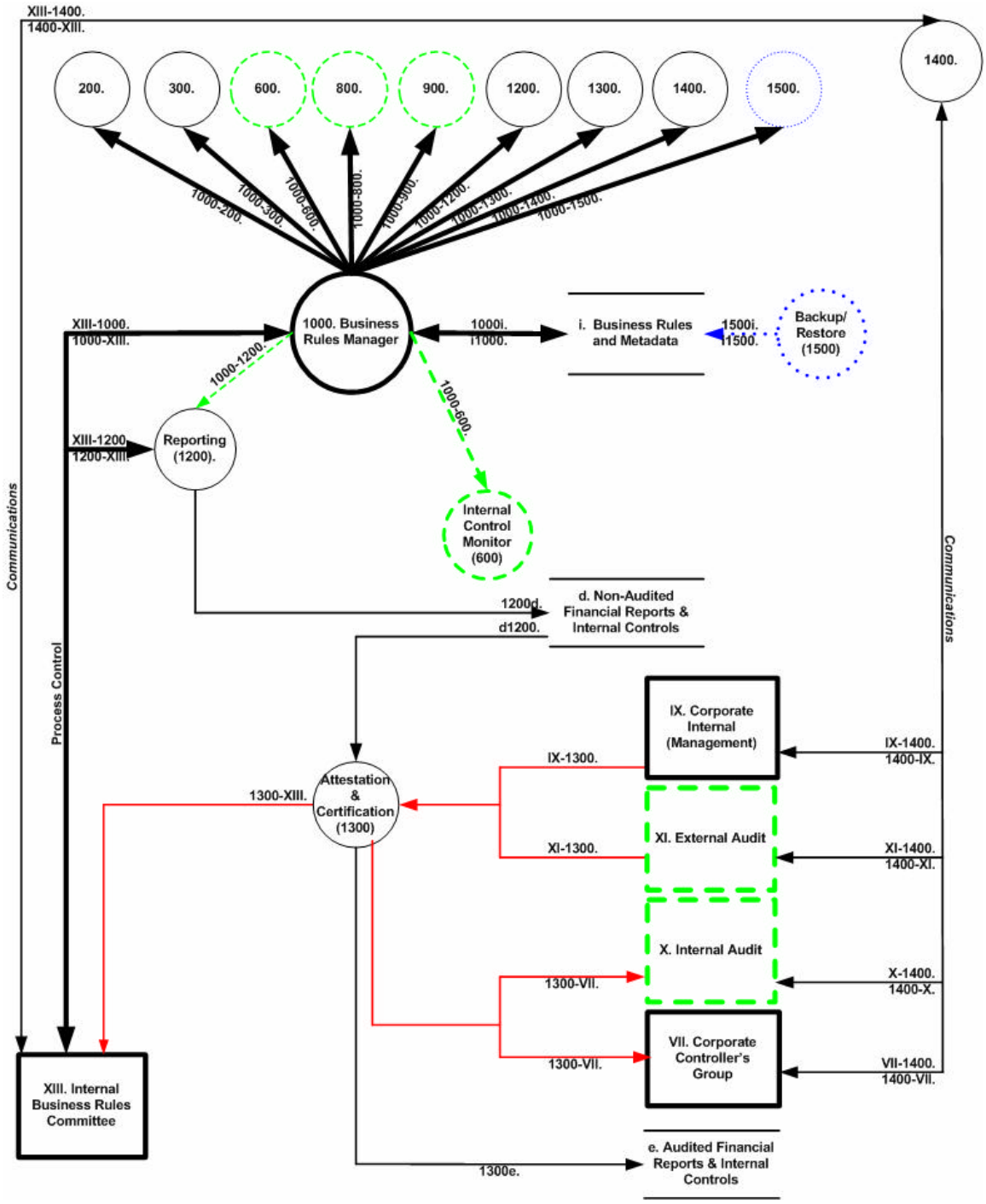

Audit
Internal Business Rules Committee
Controller's Group
Information Technology Group
Feed Back Loop

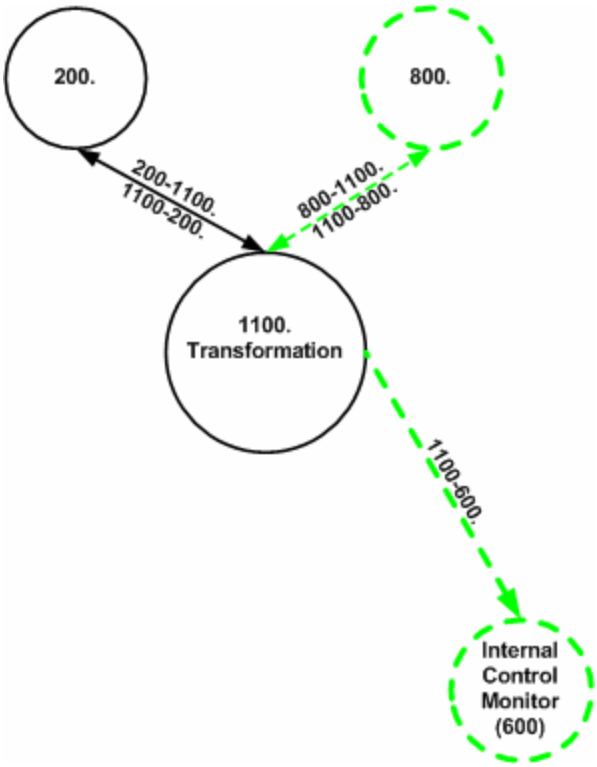

Operational Data Sources
(I thru VI)
XIII. Internal Business Rules
Committee
VII. Corporate
Controller's
Group
Financial Assessment,
Audit Oversight & Reporting
(100,200,300,600,800,900,
1000,1100,1200,1400,1500)
X. Internal Audit
IX. Corporate Internal
(Management)
XI. External Audit
Attestation &
Certification
(1300,1500)
XII. External (SEC)

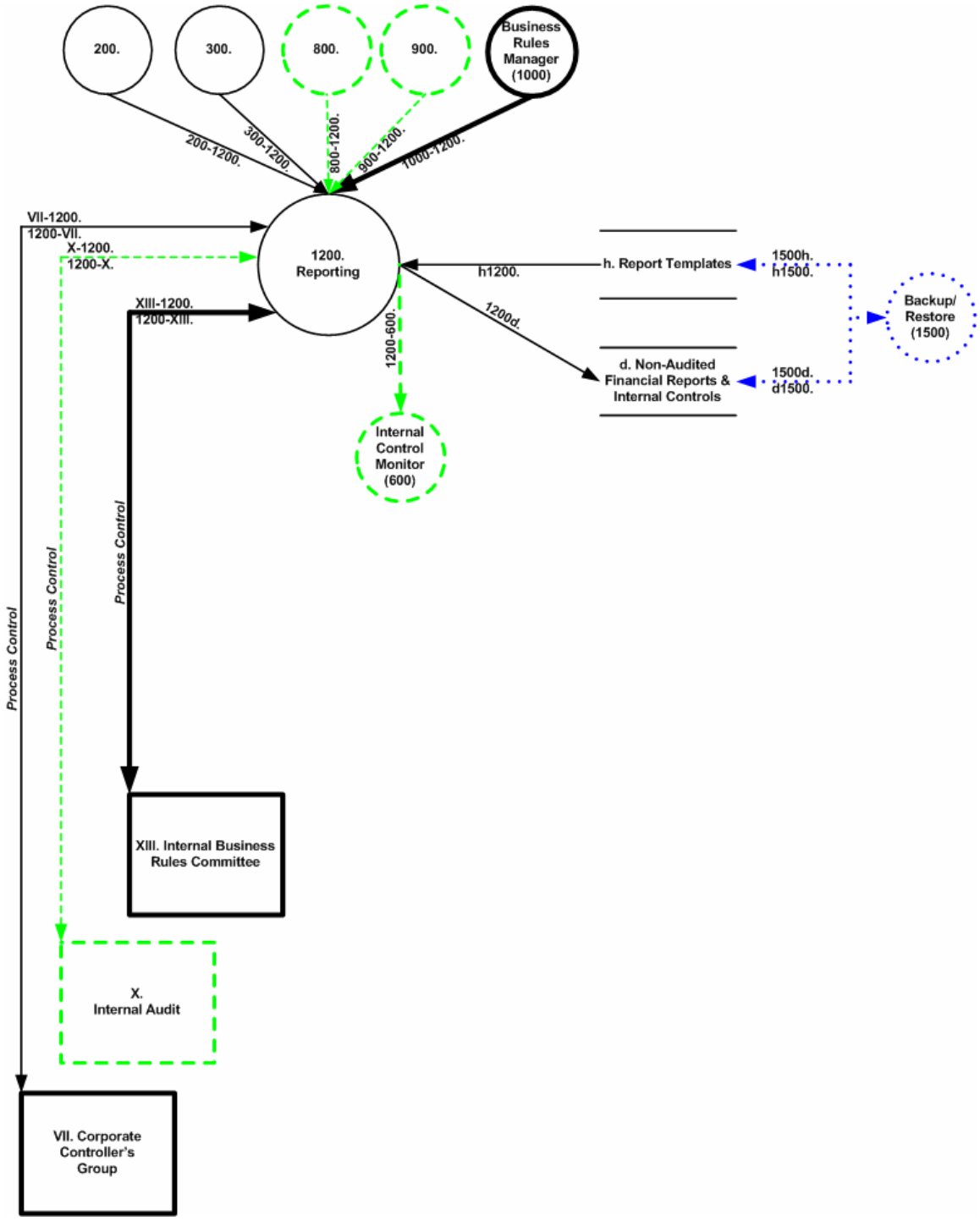

1500.
Backup/Restore
VIII. Information
Technology Group
Enterprise Rules
Management
(1000,1500)
Operational Data Sources
(I thru VI)
Internal Business Rules
Committee (XIII)
Audit Oversight
(600,800,900,1100,
1200,1400)
Financial Assessment
(100,200,300,1100,
1200,1400)
Feedback
Loop
III
Feedback Loop I
Feedback Loop II
X. Internal Audit
XI. External Audit
IX. Corporate Internal
(Management & Board)
VII. Corporate
Controller's
Group
Attestation &
Certification
(1300)
Audited Financial
Reports
XII. External
(SEC & IRS)

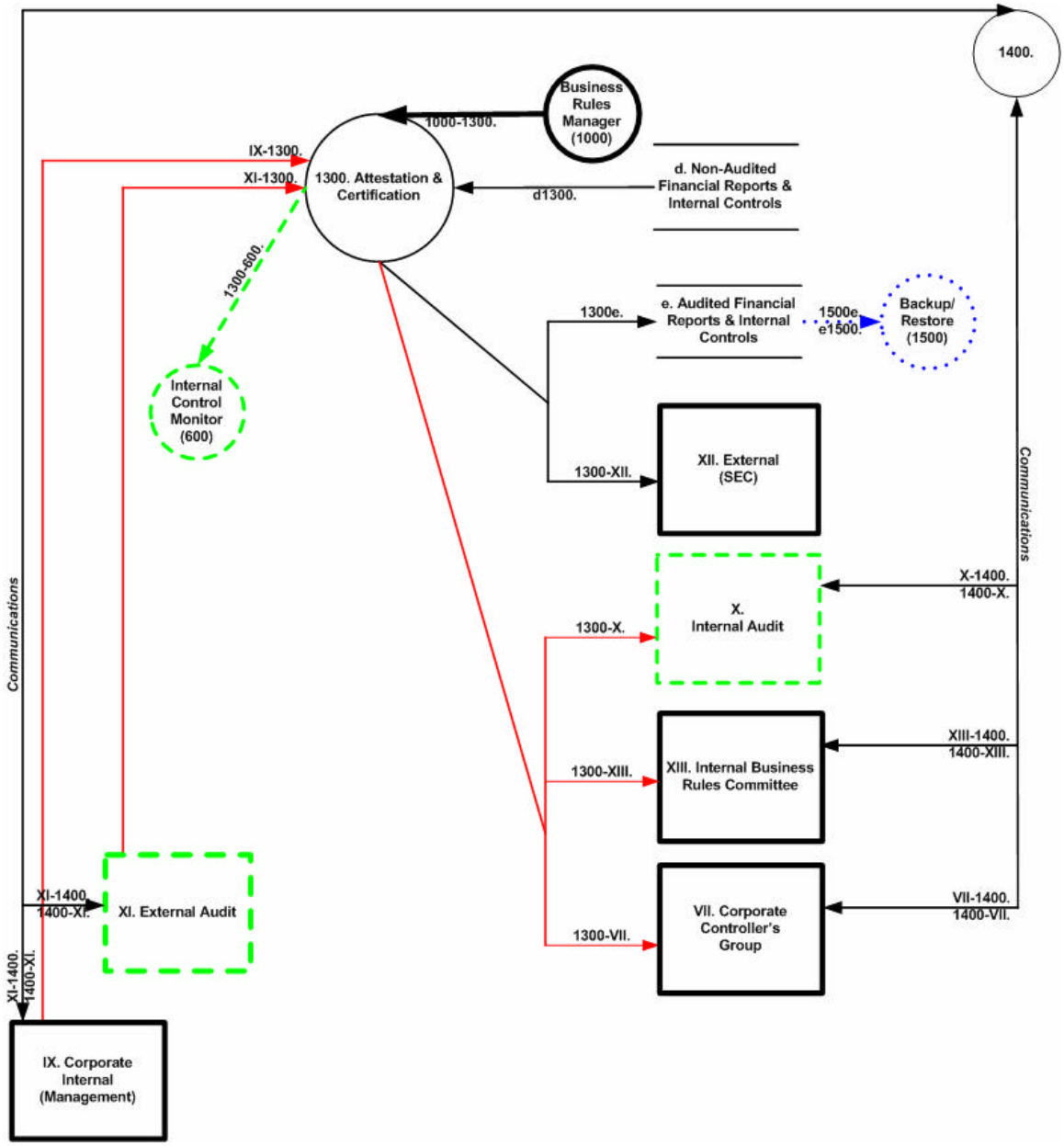

I. Corporate Accounting
II. Corporate Treasurer
III. Corporate Budgeting, Planning & Forecasting
IV. Legal Subsidiary Accounting
V. Legal Subsidiary Accounting
VI. Legal Subsidiary Accounting
Comm-unications Manager (1400)
VII-1400. 1400-VII.
I-1400. 1400-I.
II-1400. 1400-II.
III-1400. 1400-III.
IV-1400. 1400-IV.
V-1400. 1400-V.
VI-1400. 1400-VI.
I-200. 200-I.
II-200. 200-II.
III-200. 200-III.
IV-200. 200-IV.
V-200. 200-V.
VI-200. 200-VI.
200. Collection & Distribution
1000-200.
VII-200. 200-VII.
200-1200.
200-1100. 1100-200.
Trans-formation (1100)
200-600.
200-300.
300-200.
VII-1200. 1200-VII.
Reporting (1200).
900-1200.
Internal Control Assessment (900)
Internal Control Monitor (600)
300-600.
300-1200.
Business Rules Manager (1000)
1000-300.
300. Consolidation, Adjustment & Period Lock
VII-300.
200a. a200.
a. Controller's Staging Area (Metadata, Data, & Business Rules by Submission)
1500a. a1500.
200b. b200.
b. Disclosures by Period by Entity
1500b. b1500.
Backup/ Restore (1500)
300c. c300.
c. Operational Data Store (ODS)
1500c. c1500.
1200d. d1300.
d. Non-Audited Financial Reports & Internal Controls
1500d. d1500.
XIII. Internal Business Rules Committee
1300-XIII.
XIII-1400. 1400-XIII.
IX. Corporate Internal (Management)
IX-1400. 1400-IX.
IX-1300.
1300-VII.
Attestation & Certification (1300)
XI. External Audit
XI-1400. 1400-XI.
XI-1300.
X. Internal Audit
X-1400. 1400-X.
1300-X.
VII. Corporate Controller's Group
e. Audited Financial Reports & Internal Controls
1500e. e1500.
1300e.
Communications
Process Control
Communications


X-1400.
1400-X.
Comm-unications Manager (1400)
200.
300.
1000.
1100.
1200.
1300.
1500.
200-600.
300-600.
1000-600.
1100-600.
1200-600.
1300-600.
1500-600.
600. Internal Control Monitor
X-600.
600-X.
Business Rules Manager (1000)
600-800.
800-600.
X-800.
800-X.
1000-800.
800. Internal Control Collection
800f.
f800.
f. Audit's Staging Area
1500f.
f1500.
Backup/ Restore (1500)
800-1200.
800-1100.
1100-800.
Trans-formation (1100)
Reporting (1200).
X-1200.
1200-X.
800g.
g. Internal Control Data Mart
1500g.
g1500.
1000-900.
g800.
900-1200.
900. Internal & Disclosure Control Assessment
X-900.
900-X.
Communications
Process Control
1200d.
d. Non-Audited Financial Reports & Internal Controls
d1300.
XIII. Internal Business Rules Committee
XIII-1400.
1400-XIII.
1300-XIII.
IX. Corporate Internal (Management)
IX-1400.
1400-IX.
IX-1300.
Attestation& Certification (1300)
1300-X.
XI. External Audit
XI-1400.
1400-XI.
XI-1300.
VII. Corporate Controller's Group
VII-1400.
1400-VII.
1300-VII.
X. Internal Audit
e. Audited Financial Reports & Internal Controls
1300e.


XIII-1400.
1400-XIII.
1400.
200.
300.
600.
800.
900.
1200.
1300.
1400.
1500.
1000-200.
1000-300.
1000-600.
1000-800.
1000-900.
1000-1200.
1000-1300.
1000-1400.
1000-1500.
XIII-1000.
1000-XIII.
1000. Business Rules Manager
1000i.
i1000.
i. Business Rules and Metadata
1500i.
i1500.
Backup/ Restore (1500)
1000-1200.
1000-600.
XIII-1200.
1200-XIII.
Reporting (1200).
Internal Control Monitor (600)
Communications
1200d.
d1200.
d. Non-Audited Financial Reports & Internal Controls
Process Control
IX. Corporate Internal (Management)
IX-1400.
1400-IX.
IX-1300.
1300-XIII.
Attestation & Certification (1300)
XI. External Audit
XI-1300.
XI-1400.
1400-XI.
X. Internal Audit
1300-VII.
X-1400.
1400-X.
VII. Corporate Controller's Group
1300-VII.
VII-1400.
1400-VII.
XIII. Internal Business Rules Committee
1300e.
e. Audited Financial Reports & Internal Controls


200.
800.
200-1100.
1100-200.
800-1100.
1100-800.
1100.
Transformation
1100-600.
Internal
Control
Monitor
(600)


200.
300.
800.
900.
Business Rules Manager (1000)
200-1200.
300-1200.
800-1200.
900-1200.
1000-1200.
VII-1200.
1200-VII.
X-1200.
1200-X.
XIII-1200.
1200-XIII.
1200. Reporting
h1200.
h. Report Templates
1500h.
h1500.
1200d.
d. Non-Audited Financial Reports & Internal Controls
1500d.
d1500.
Backup/ Restore (1500)
1200-600.
Internal Control Monitor (600)
Process Control
Process Control
Process Control
XIII. Internal Business Rules Committee
X. Internal Audit
VII. Corporate Controller's Group


1400.
Business Rules Manager (1000)
1000-1300.
IX-1300.
XI-1300.
1300. Attestation & Certification
d1300.
d. Non-Audited Financial Reports & Internal Controls
1300-600.
Internal Control Monitor (600)
1300e.
e. Audited Financial Reports & Internal Controls
1500e.
e1500.
Backup/ Restore (1500)
1300-XII.
XII. External (SEC)
Communications
X-1400.
1400-X.
1300-X.
X. Internal Audit
XIII-1400.
1400-XIII.
1300-XIII.
XIII. Internal Business Rules Committee
VII-1400.
1400-VII.
1300-VII.
VII. Corporate Controller's Group
XI-1400.
1400-XI.
XI. External Audit
XI-1400.
1400-XI.
IX. Corporate Internal (Management)

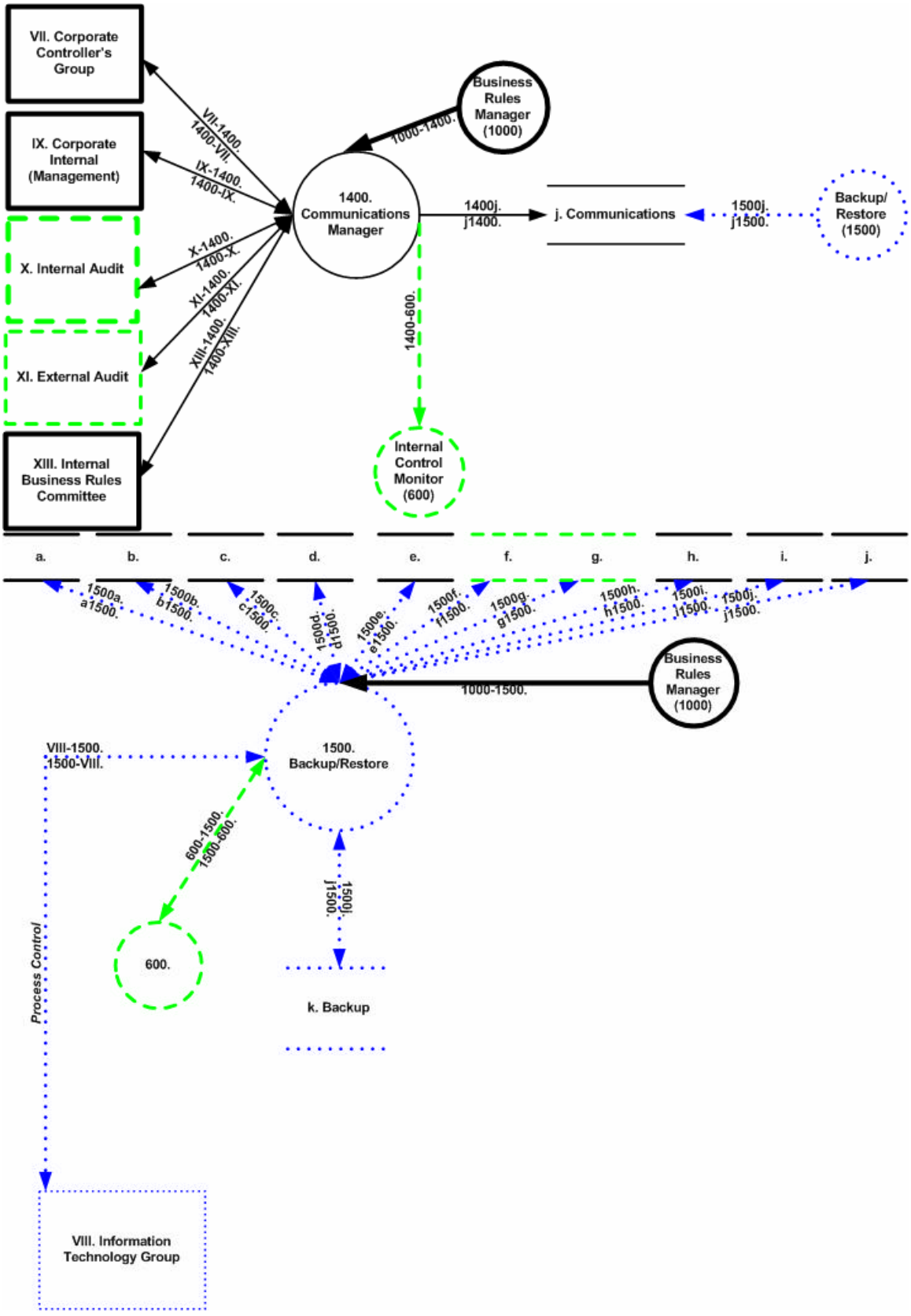

VII. Corporate Controller's Group
IX. Corporate Internal (Management)
X. Internal Audit
XI. External Audit
XIII. Internal Business Rules Committee
VII-1400.
1400-VII.
IX-1400.
1400-IX.
X-1400.
1400-X.
XI-1400.
1400-XI.
XIII-1400.
1400-XIII.
Business Rules Manager (1000)
1000-1400.
1400. Communications Manager
1400j.
j1400.
j. Communications
1500j.
j1500.
Backup/ Restore (1500)
1400-600.
Internal Control Monitor (600)
a.
b.
c.
d.
e.
f.
g.
h.
i.
j.
1500a.
a1500.
1500b.
b1500.
1500c.
c1500.
1500d.
d1500.
1500e.
e1500.
1500f.
f1500.
1500g.
g1500.
1500h.
h1500.
1500i.
i1500.
1500j.
j1500.
Business Rules Manager (1000)
1000-1500.
VIII-1500.
1500-VIII.
1500. Backup/Restore
600-1500.
1500-600.
1500j.
j1500.
600.
k. Backup
Process Control
VIII. Information Technology Group

TABLE OF CONTENTS