Performing a Security Assessment

Tuesday, August 23, 2011

04:00 – 04:50 PM

Todd Marcinik, CISA, CRISC

Internal Audit Manager - IT

EXIDE® TECHNOLOGIES

GEEK WEEK ISACA Atlanta

Session Objectives

- Identify critical security topics to define the goals and objectives
- Understanding assessment depth, evidence, and documentation requirements
- Incorporating regulatory and legal requirements
- Information requests and data gathering techniques
- Performing a gap analysis and creating a recommendation road map
- Evaluating “lessons learned” and providing continuing education and awareness

Company Background

EXIDE TECHNOLOGIES

About Exide Technologies:

Exide Technologies, with operations in more than 80 countries, has the products and services to meet the world's stored energy needs in transportation and industrial markets. With more than 120 years in the battery business, Exide has the experience, advanced research and development capabilities, and knowledge to provide solutions to various stored energy requirements.

Transportation Solutions

Exide offers a full assortment of starting and deep-cycle batteries delivering a multitude of applications. Our products are made to fit automotive, truck, SUV, heavy-duty, commercial, marine, RV, lawn & garden as well as many other niche applications.

GNB Motive Power

Motive power batteries are used in materials handling, cleaning machines, airport ground support, automated guided vehicles, underground mining, personnel carriers, aerial lifts, neighborhood electric vehicles, and railway locomotive starting.

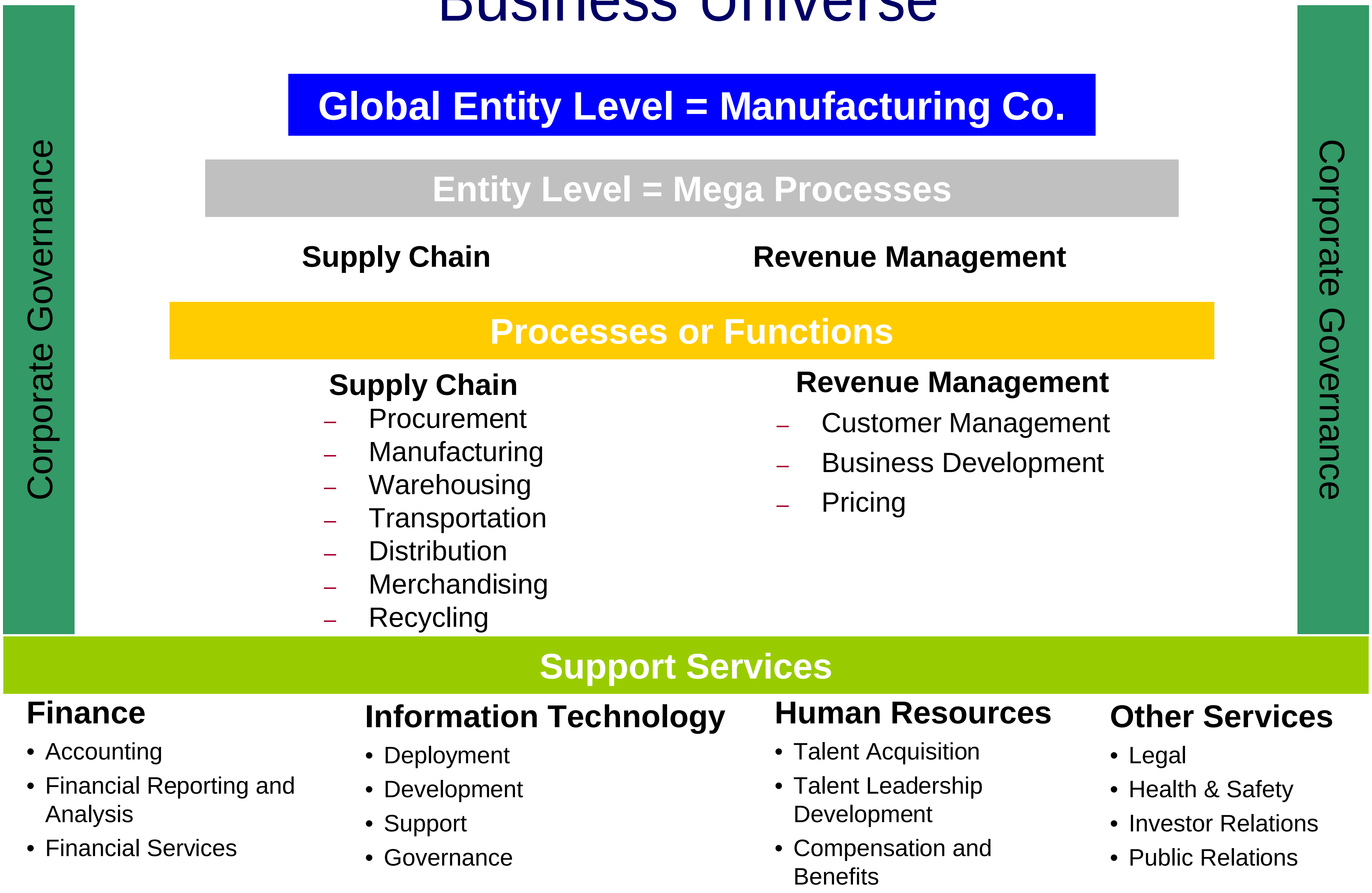
GNB Network Power

Energy storage solutions for critical systems that require uninterrupted power supply. Applications include telecommunications, computers, security systems, emergency lighting, power plant systems, medical, alternative energy, railway crossings, and various forms of military equipment used in mission critical environments.

Recycling Centers

Exide is one of the largest secondary recyclers in the world with nine recycling facilities worldwide. We are one of the few companies with the ability to provide Total Battery Management (TBM) in its own facilities. TBM frees customers from the regulatory burdens of handling spent batteries. TBM also keeps recyclable materials in the manufacturing stream instead of landfills. Recycling recovers 99% of all lead received at our recycling centers, which recycle more than 30 million batteries per year.

Business Universe



Global Entity Level = Manufacturing Co.

Entity Level = Mega Processes

Supply Chain

Revenue Management

Processes or Functions

Supply Chain
- Procurement
- Manufacturing
- Warehousing
- Transportation
- Distribution
- Merchandising
- Recycling

Revenue Management
- Customer Management
- Business Development
- Pricing

Corporate Governance

Corporate Governance

Support Services

Finance
- Accounting
- Financial Reporting and Analysis
- Financial Services

Information Technology
- Deployment
- Development
- Support
- Governance

Human Resources
- Talent Acquisition
- Talent Leadership Development
- Compensation and Benefits

Other Services
- Legal
- Health & Safety
- Investor Relations
- Public Relations

Information Security Framework Consists of...

- Business Objectives
- Governance, Policy, and Standards
- Asset Identification
- Technical Security Architecture
- Organizational Management
- Processes and Operational Practices
- Technical Specifications
- Security Program Compliance and Reporting

Information Security Framework Alignment

- CobiT
- ISO 27002:2005
- NIST
- ITIL
- Regulatory Compliance
  - SOX
  - PCI
  - HIPAA
  - Gramm-Leach-Bliley
  - FISMA
  - State and local

Information Security Assessment Overview

Assess, design, implement, and maintain a secure and high performance business environment

Security Strategy	Security Technology Implementation	Security Assessment and Testing	Security Management
Assess, design, and implement business-aligned security strategy that describes the process, controls, and infrastructure to manage risk and comply with applicable laws and regulations.	Design, implement, and integrate security solutions to address enterprise risks and exposures.	Identity security exposures and business risks created by vulnerabilities and inadequate controls in business systems, applications, and network devices.	Design and implement a practical, risk-based information security management program to maintain the confidentiality, integrity, and availability of information systems and the data processed within.
• Security governance • Data protection • Identity and access mgmt. • Application security • Threat / vulnerability mgmt. • Incident mgmt. and response • Business continuity / disaster recovery • Security architecture design	• Vendor selection • Network security • User provisioning • Role management • Data loss prevention • Secure messaging • Encryption • Security information and event Management • Multifactor authentication • Applications • Single sign on • Asset management	• Information security program • Privacy assessment • Risk / threat / vulnerability assessment • Internet/Intranet security assessment • Dial-up security assessment • Wireless security assessment • Application security assessment • Application source code review • Business continuity assessment • Incident response assessment • Physical security assessment • Social engineering assessment	• Security organization • Security policies • Security procedures and standards • Security operations planning and support • Security awareness training • Software development lifecycle security advisory • Secure coding practices training • Business continuity / disaster recovery

Assessment Planning

- Knowledge Requirements
  - Network / Hardware
  - Operating Systems / Databases
- Potential Scoping Issues
  - Customer Concerns
  - Assumptions
  - System Criticality
  - Ad Hoc Security

Assessment Planning

- Documentation
  - Policy
  - Guidelines / Requirements
  - Plans
  - Standard Operating Procedures
  - User Documentation

Assessment Planning

- Planning Survey – Partial Example
  - Organizational Environment
    - How many physical locations do you have?
    - Do you currently outsource any functions of IT? If so, what functions?
  - IT Environment
    - What types of mainframe or terminal-based system are in use?
    - What server-level operating systems (OS) are in place (Windows, UNIX, Linux, etc.)?
    - What remote access is permitted and through what medium (ISDN, VPN, etc.)?
  - Technical Security Environment
    - Are boundary firewalls in place? If so, what technology?
    - What types of centralized security have been implemented?

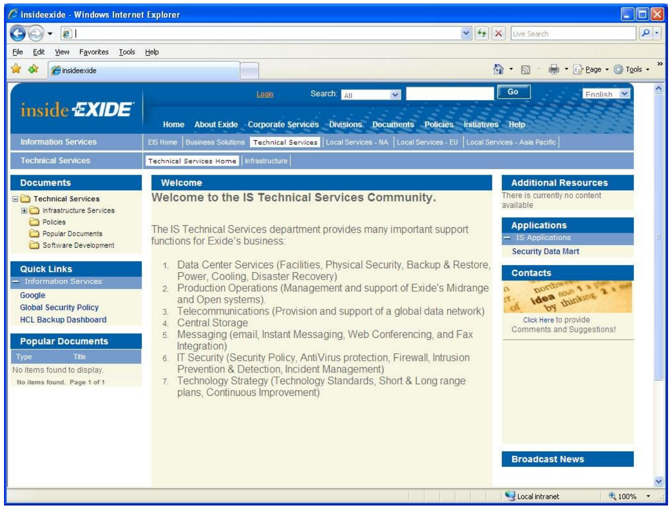
Assessment Planning

Mega Process (Level 1): Logical Access		
Major Process (Level 2)	Sub-Process (Level 3)	Activity (Level 4)
New Hire	Default Access	Create
	Job Specific Access	Create
Transfer	Old Job Specific Access	Change, Delete
	New Job Specific Access	Create
Termination	Job Specific Access	Change, Delete
Temporary/Contract Labor	Job/Project Specific Access	Create, Change, Delete
Temporary/Elevated	Project Specific Access	Change, Delete
Generic/Shared IDs	Project Specific Access	Create, Change, Delete

Business Objectives

- Operating Framework
- Regulatory Requirements
- Strategic Objectives
- Security Strategy Alignment

Governance, Policy, and Standards


insideexide - Windows Internet Explorer
Live Search
File Edit View Favorites Tools Help
insideexide
Page Tools
inside EXIDE
Login
Search: All
Go
English
Home About Exide Corporate Services Divisions Documents Policies Initiatives Help
Information Services
EIS Home | Business Solutions | Technical Services | Local Services - NA | Local Services - EU | Local Services - Asia Pacific
Technical Services
Technical Services Home | Infrastructure
Local intranet
100%

Documents

- Technical Services
  - Infrastructure Services
  - Policies
  - Popular Documents
  - Software Development

Quick Links

- Information Services
  - Google
  - Global Security Policy
  - HCL Backup Dashboard

Popular Documents

Type	Title
No items found to display.	

No items found. Page 1 of 1

Welcome

Welcome to the IS Technical Services Community.

The IS Technical Services department provides many important support functions for Exide's business:

1. Data Center Services (Facilities, Physical Security, Backup & Restore, Power, Cooling, Disaster Recovery)
2. Production Operations (Management and support of Exide's Midrange and Open systems).
3. Telecommunications (Provision and support of a global data network)
4. Central Storage
5. Messaging (email, Instant Messaging, Web Conferencing, and Fax Integration)
6. IT Security (Security Policy, AntiVirus protection, Firewall, Intrusion Prevention & Detection, Incident Management)
7. Technology Strategy (Technology Standards, Short & Long range plans, Continuous Improvement)

Additional Resources

There is currently no content available

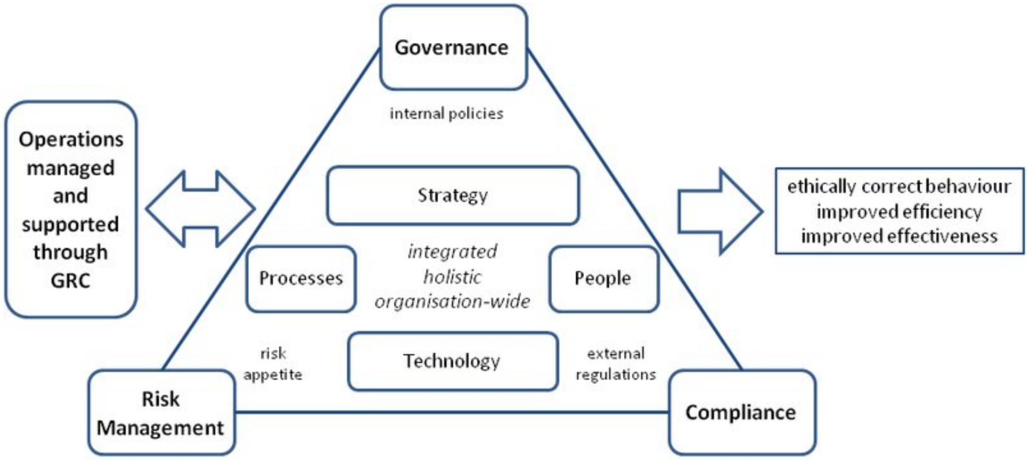
Applications

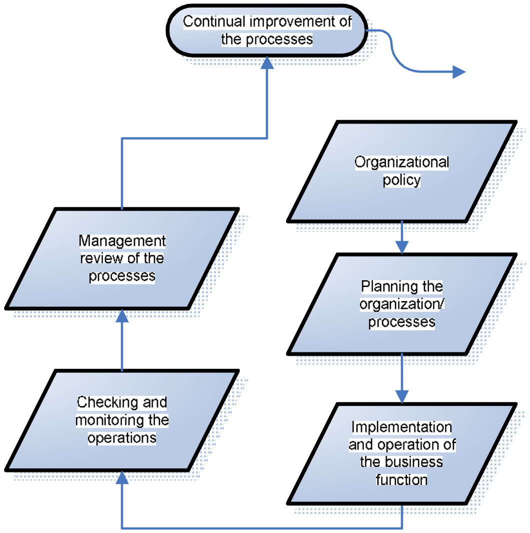
- IS Applications
  - Security Data Mart

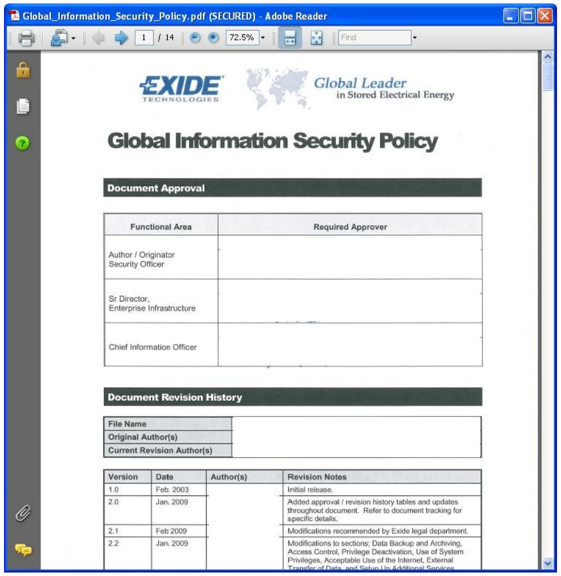
Contacts

Click Here to provide Comments and Suggestions!

Broadcast News




Continual improvement of the processes
Organizational policy
Planning the organization/ processes
Implementation and operation of the business function
Checking and monitoring the operations
Management review of the processes


Global_Information_Security_Policy.pdf (SECURED) - Adobe Reader
1 / 14
72.5%
Find
EXIDE TECHNOLOGIES
Global Leader in Stored Electrical Energy

Global Information Security Policy

Document Approval

Functional Area	Required Approver
Author / Originator Security Officer	
Sr Director, Enterprise Infrastructure	
Chief Information Officer	

Document Revision History

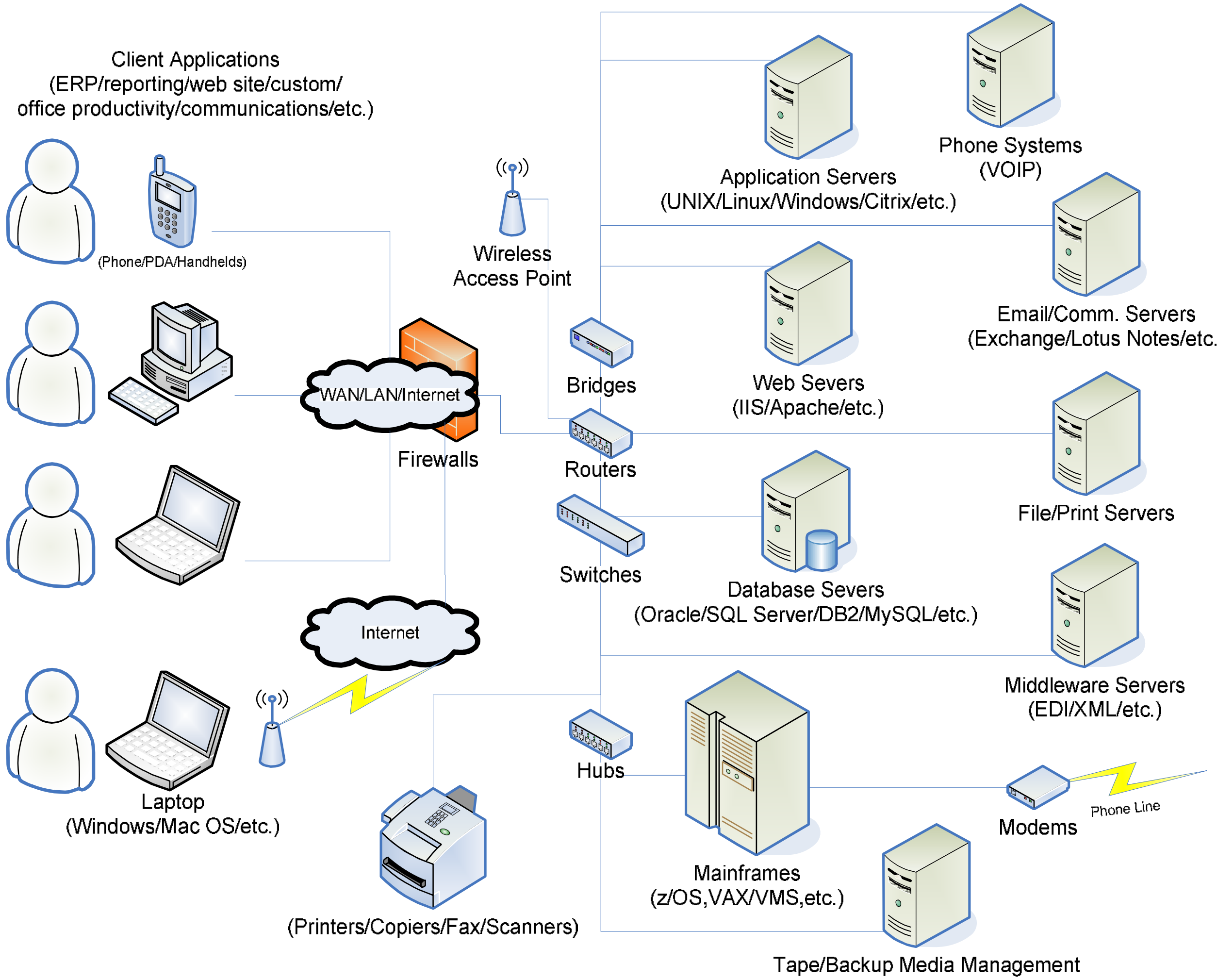
File Name	
Original Author(s)	
Current Revision Author(s)	

Version	Date	Author(s)	Revision Notes
1.0	Feb. 2003		Initial release.
2.0	Jan. 2009		Added approval / revision history tables and updates throughout document. Refer to document tracking for specific details.
2.1	Feb 2009		Modifications recommended by Exide legal department.
2.2	Jan. 2009		Modifications to sections; Data Backup and Archiving, Access Control, Privilege Deactivation, Use of System Privileges, Acceptable Use of the Internet, External Transfer of Data, and Setup Up Additional Services

Asset Identification

- Asset Inventory
- Applications
- Risk Model
- Information/Data Classification
- Asset Provisioning
- Security Software Distribution

Technical Security Architecture



Organizational Management

- Organizational Structure
  - Reporting Relationships and Structure
- Functional Definitions
- Roles and Responsibilities
  - Defined
  - Alignment

Processes and Operational Practices

- Threat and Vulnerability Management
  - Threat Awareness
  - Vulnerability Management
  - Security Event Analysis
  - Intrusion Detection / Prevention
  - Security Incident Response
  - Internet Content Filtering
  - Malware / Spyware Protection

Processes and Operational Practices

- Identity and Access Management
  - User Provisioning / Deprovisioning
    - New Hire (Perm. & Temp. / Contract Labor)
    - Transfers
    - Terminations
    - Generic / Shared IDs
    - Temp. / Elevated Access
  - Remote Access

Processes and Operational Practices

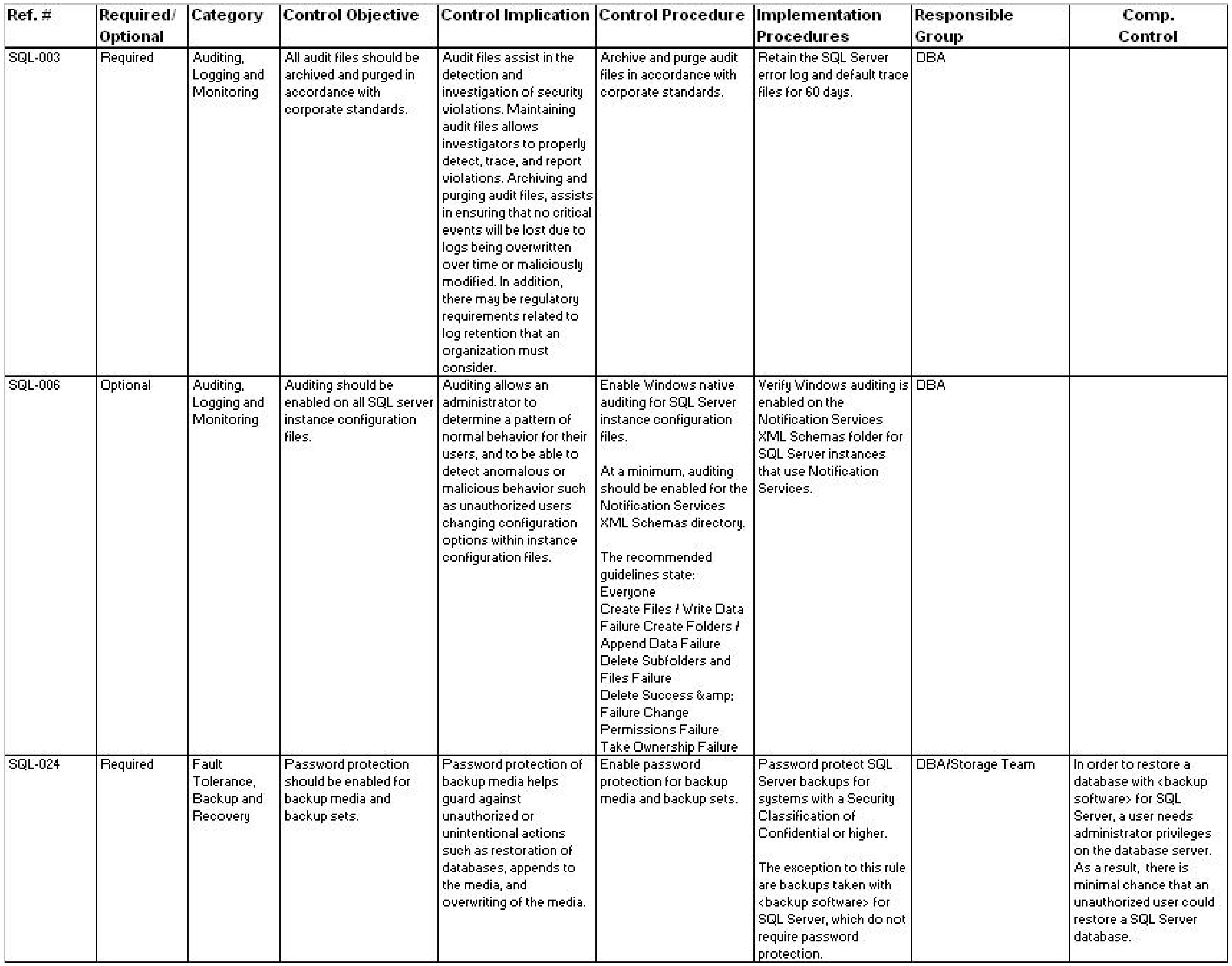
- Education and Awareness
  - Security Education
    - New Hire Training
      - Perm. & Temp. / Contract Labor
    - Ongoing User Training
  - Security Awareness – General Communications

Processes and Operational Practices

- Support Services
  - BCP / DR / Problem Management
  - Security Activities – Business Support / Alignment
  - Encryption
  - Change / Configuration Management

Technical Specifications

EXAMPLE: SQL Server



Ref. #	Required/ Optional	Category	Control Objective	Control Implication	Control Procedure	Implementation Procedures	Responsible Group	Comp. Control
SQL-003	Required	Auditing, Logging and Monitoring	All audit files should be archived and purged in accordance with corporate standards.	Audit files assist in the detection and investigation of security violations. Maintaining audit files allows investigators to properly detect, trace, and report violations. Archiving and purging audit files, assists in ensuring that no critical events will be lost due to logs being overwritten over time or maliciously modified. In addition, there may be regulatory requirements related to log retention that an organization must consider.	Archive and purge audit files in accordance with corporate standards.	Retain the SQL Server error log and default trace files for 60 days.	DBA	
SQL-006	Optional	Auditing, Logging and Monitoring	Auditing should be enabled on all SQL server instance configuration files.	Auditing allows an administrator to determine a pattern of normal behavior for their users, and to be able to detect anomalous or malicious behavior such as unauthorized users changing configuration options within instance configuration files.	Enable Windows native auditing for SQL Server instance configuration files. At a minimum, auditing should be enabled for the Notification Services XML Schemas directory. The recommended guidelines state: Everyone Create Files / Write Data Failure Create Folders / Append Data Failure Delete Subfolders and Files Failure Delete Success &amp; Failure Change Permissions Failure Take Ownership Failure	Verify Windows auditing is enabled on the Notification Services XML Schemas folder for SQL Server instances that use Notification Services.	DBA	
SQL-024	Required	Fault Tolerance, Backup and Recovery	Password protection should be enabled for backup media and backup sets.	Password protection of backup media helps guard against unauthorized or unintentional actions such as restoration of databases, appends to the media, and overwriting of the media.	Enable password protection for backup media and backup sets.	Password protect SQL Server backups for systems with a Security Classification of Confidential or higher. The exception to this rule are backups taken with <backup software> for SQL Server, which do not require password protection.	DBA/Storage Team	In order to restore a database with <backup software> for SQL Server, a user needs administrator privileges on the database server. As a result, there is minimal chance that an unauthorized user could restore a SQL Server database.

Technical Specifications

EXAMPLE: UNIX

Considerations, policy references, and required actions

- Physical
  - Control physical access to system hardware
    Policy Ref.: [Facilities / Security]
    Procedures: Monitor and maintain physical access controls; document control and response procedures; audit routinely
  - Detect, report, and manage breeches of physical access security
    Policy Ref.: [Security]
    Procedures: Detect and respond to breeches or attempted breeches of physical security; provide activity reports to appropriate parties (e.g., Incident Response Team, platform support team)
- Logical
  - Account creation approvers
    Policy Ref.: [Help Desk / Management]
    Procedures: Management approval is required for all new account creation
  - Account creation approval process
    Policy Ref.: [Help Desk / Security Administration / Management]
    Procedures: Management approval of any new user account request is required; approving manager assumes an audit role for accounts they sponsor; Help Desk receives account creation requests and forwards same, with the accountable manager's approval, to security administration for account creation
- Sendmail aliases for root, postmaster, or MAILER-DAEMON should not resolve to nobody or to /dev/null
  Policy Ref.: [Unix]
  Procedures:

```
grep -v ^# /etc/aliases
 MAILER-DAEMON:root
 postmaster:root
  nobody: /dev/null
```

Security Program Compliance and Reporting

- Security Assessments
- Metrics Definition and Collection
- Reporting to Management
- Regulatory Reviews

Security Program Compliance and Reporting

← Maturity Model →

0	1	2	3	4	5
Non-existent	Initial / Ad Hoc	Repeatable but Intuitive	Defined Process	Managed and Measureable	Optimized

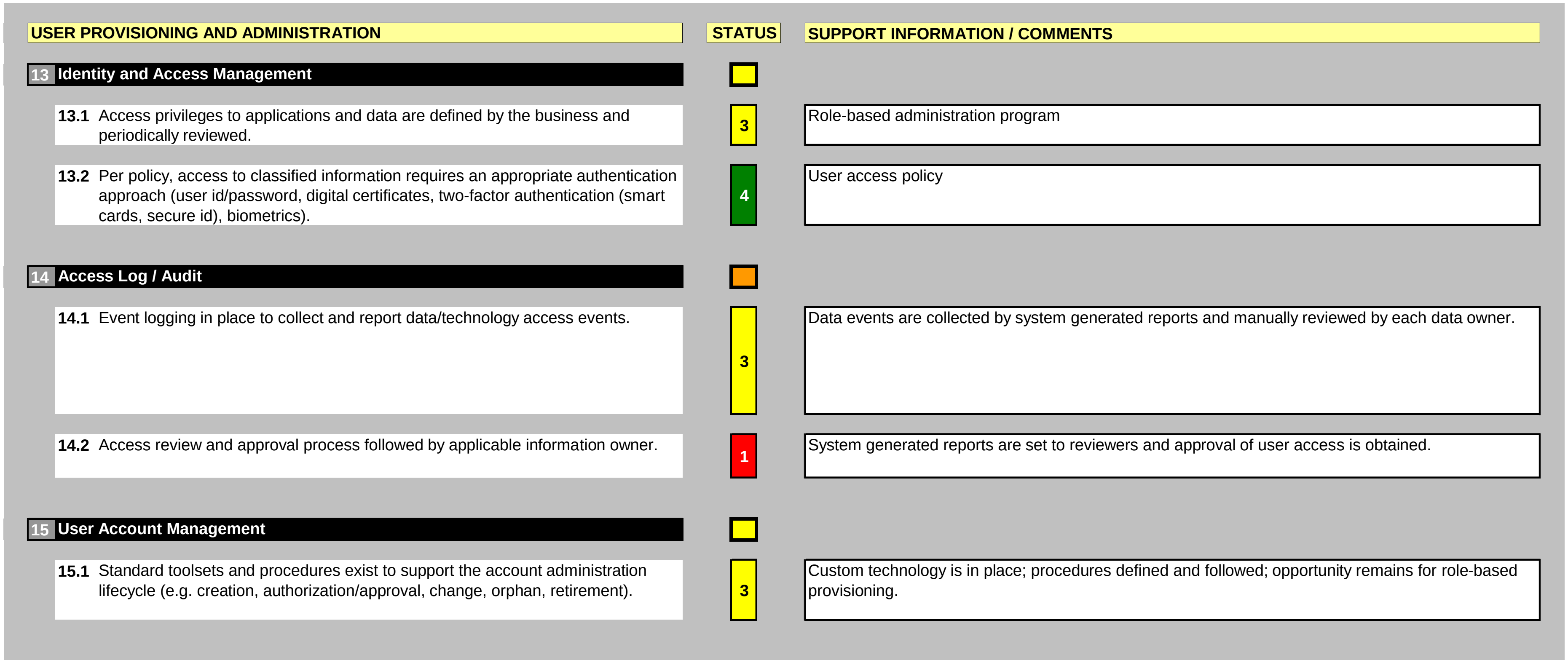
OR

← Maturity Model →

1	2	3	4
Ad Hoc	Formal / Aligned	Defined Process	Managed and Measureable

Security Program Compliance and Reporting

EXAMPLE: Worksheet



USER PROVISIONING AND ADMINISTRATION		STATUS	SUPPORT INFORMATION / COMMENTS
13	**Identity and Access Management**	🟨	
13.1	Access privileges to applications and data are defined by the business and periodically reviewed.	3	Role-based administration program
13.2	Per policy, access to classified information requires an appropriate authentication approach (user id/password, digital certificates, two-factor authentication (smart cards, secure id), biometrics).	4	User access policy
14	**Access Log / Audit**	🟧	
14.1	Event logging in place to collect and report data/technology access events.	3	Data events are collected by system generated reports and manually reviewed by each data owner.
14.2	Access review and approval process followed by applicable information owner.	1	System generated reports are set to reviewers and approval of user access is obtained.
15	**User Account Management**	🟨	
15.1	Standard toolsets and procedures exist to support the account administration lifecycle (e.g. creation, authorization/approval, change, orphan, retirement).	3	Custom technology is in place; procedures defined and followed; opportunity remains for role-based provisioning.

Security Program Compliance and Reporting

EXAMPLE: Reporting Dashboard

Strategy and Governance		Access Controls	Vulnerability and Threat Management		Incident Response
Executive Management Sponsorship	Organizational Accountability & Capacity	Identity & Access Management	Patch Management	Device Discovery & Identification	Vulnerability Alert Notification
Security Vision	Security Policies	Access Log/Audit	Anti-Virus, SPAM, Spyware	External Threat Assessment	Incident Response
Architecture & Standards	Audit, Sarbanes-Oxley	User Account Management	Network Security	Pre-/Post Production Assessment	Investigation & Forensic Analysis
Training & Awareness	Data Classification		Data Protection & Encryption	Intrusion Prevention & Detection	Incident Management & Crisis Resolution
Portfolio Management	Data Privacy		Asset Management	Compliance Monitoring & Reporting	
Vendor Management	Data Retention		Data Center Security	Disaster Recovery; Business Continuity	

Security Program Compliance and Reporting

EXAMPLE: Reporting Dashboard

Strategy and Governance		Access Controls	Vulnerability and Threat Management		Incident Response
🟨 Executive Management Sponsorship	🟩 Organizational Accountability & Capacity	🟧 Identity & Access Management	🟩 Patch Management	🟧 Device Discovery & Identification	🟩 Vulnerability Alert Notification
🟨 Security Vision	🟩 Security Policies	🟧 Access Log/Audit	🟩 Anti-Virus, SPAM, Spyware	🟩 External Threat Assessment	🟩 Incident Response
🟨 Architecture & Standards	🟩 Audit, Sarbanes-Oxley	🟨 User Account Management	🟩 Network Security	🟨 Pre-/Post Production Assessment	🟩 Investigation & Forensic Analysis
🟨 Training & Awareness	🟥 Data Classification		🟥 Data Protection & Encryption	🟨 Intrusion Prevention & Detection	🟨 Incident Management & Crisis Resolution
🟨 Portfolio Management	🟨 Data Privacy		🟨 Asset Management	🟨 Compliance Monitoring & Reporting	
🟨 Vendor Management	🟨 Data Retention		🟩 Data Center Security	🟧 Disaster Recovery; Business Continuity	

🟩 Full Compliant	🟧 Partially Compliant
🟨 Mostly Compliant	🟥 Limited/Not Compliant

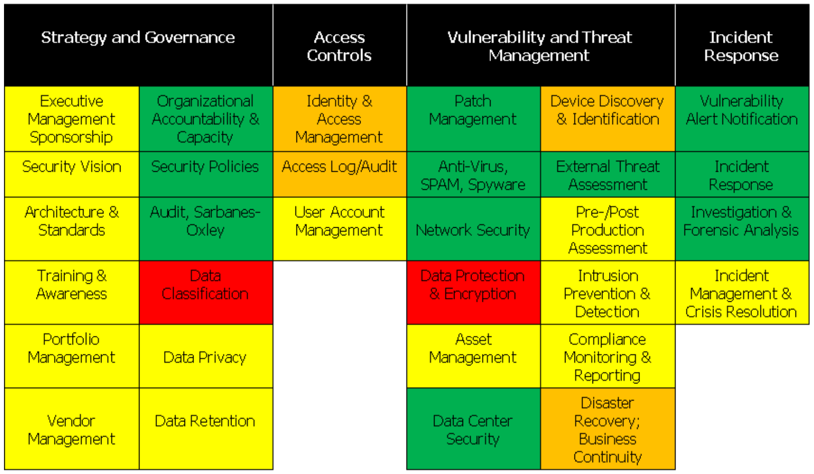
Security Program Compliance and Reporting

EXAMPLE: Compliance Plan

Goal/Objectives	Plan Overview

- No SOX significant or material weakness
- No high-risk or repeat audit findings
- Sustainable processes and practices that mitigate risk
- Compliance with security standards and practices
- Proactive focus on emerging security threats
- Personal (PII) data identified and protected
- Trained associates; Visible security compliance
- Business-defined information access controls
- Clear, executable business continuity plans
- Engagement and program compliance

RED = Areas of Focus



Strategy and Governance		Access Controls	Vulnerability and Threat Management		Incident Response
🟨 Executive Management Sponsorship	🟩 Organizational Accountability & Capacity	🟧 Identity & Access Management	🟩 Patch Management	🟧 Device Discovery & Identification	🟩 Vulnerability Alert Notification
🟨 Security Vision	🟩 Security Policies	🟧 Access Log/Audit	🟩 Anti-Virus, SPAM, Spyware	🟩 External Threat Assessment	🟩 Incident Response
🟨 Architecture & Standards	🟩 Audit, Sarbanes-Oxley	🟨 User Account Management	🟩 Network Security	🟨 Pre-/Post Production Assessment	🟩 Investigation & Forensic Analysis
🟨 Training & Awareness	🟥 Data Classification		🟥 Data Protection & Encryption	🟨 Intrusion Prevention & Detection	🟨 Incident Management & Crisis Resolution
🟨 Portfolio Management	🟨 Data Privacy		🟨 Asset Management	🟨 Compliance Monitoring & Reporting	
🟨 Vendor Management	🟨 Data Retention		🟩 Data Center Security	🟧 Disaster Recovery; Business Continuity	

- Continue & extend information security leadership across company
- Increase organizational capability and execution
- Execute a training program to minimize risk and elevate compliance
- Deploy capabilities to improve data classification and protection
- Update data retention practices to ensure compliance and information availability
- Improve the authorization and controls associated with access to information
- Expand vulnerability assessment, detection, and prevention capabilities
- Expand the monitoring and reporting of technical standard compliance
- Strengthen self-assessment program and achieve sustainable compliance

Summary

- What are the motivating factors affecting the business?
- What assets are currently in place?
- How is the technology managed and supported?
- What is evidence is available?
- How mature are the processes?
- Is there continuous improvement?

Questions / Comments

- Contact Information:
  - Todd Marcinik, CISA, CRISC
  - Exide Technologies
  - http://www.exide.com
  - Todd.Marcinik@exide.com
  - 678-566-9191

EXIDE®
TECHNOLOGIES