



Incident Response: What to do *Before* It Hits the Fan!

Presented to:
**Minnesota Information
System Forensics
Association**

Thursday, October 19, 2006

John B. Weaver

CISSP, CISA, CISM, CPP

President/CEO

Principal Consultant

A Standards-Based Approach

Agenda

- ❑ Introduction
- ❑ Information Security
- ❑ Current Business Environment
- ❑ Standards-Based Approach
- ❑ Incident Response
- ❑ Incident Management Process
- ❑ Proactive Strategies
- ❑ Reactive Strategies
- ❑ Incident Response Metrics
- ❑ Continuous Improvement

John B. Weaver – CISSP, CISA, CISM, CPP

- ❑ Over 16 years as a professional paranoid.
- ❑ Former director of world-wide & IP network security at Qwest
- ❑ Vice President, Executive Board of InfraGard - FBI/private sector coalition for the protection of the national infrastructure.
- ❑ Founded JBW Group International, a full service information security consultancy in 2002.
- ❑ Consulted with clients in the US, Canada, Mexico, and Japan.
- ❑ Fortune 50 companies to small businesses
- ❑ Taught BS7799 Audit and Implementation for BSI Americas
- ❑ ISO 27001 implementation
- ❑ IRCA-certified ISO 27001 auditor
- ❑ Disaster Preparedness Planning
- ❑ Security program deployment
- ❑ Incident response

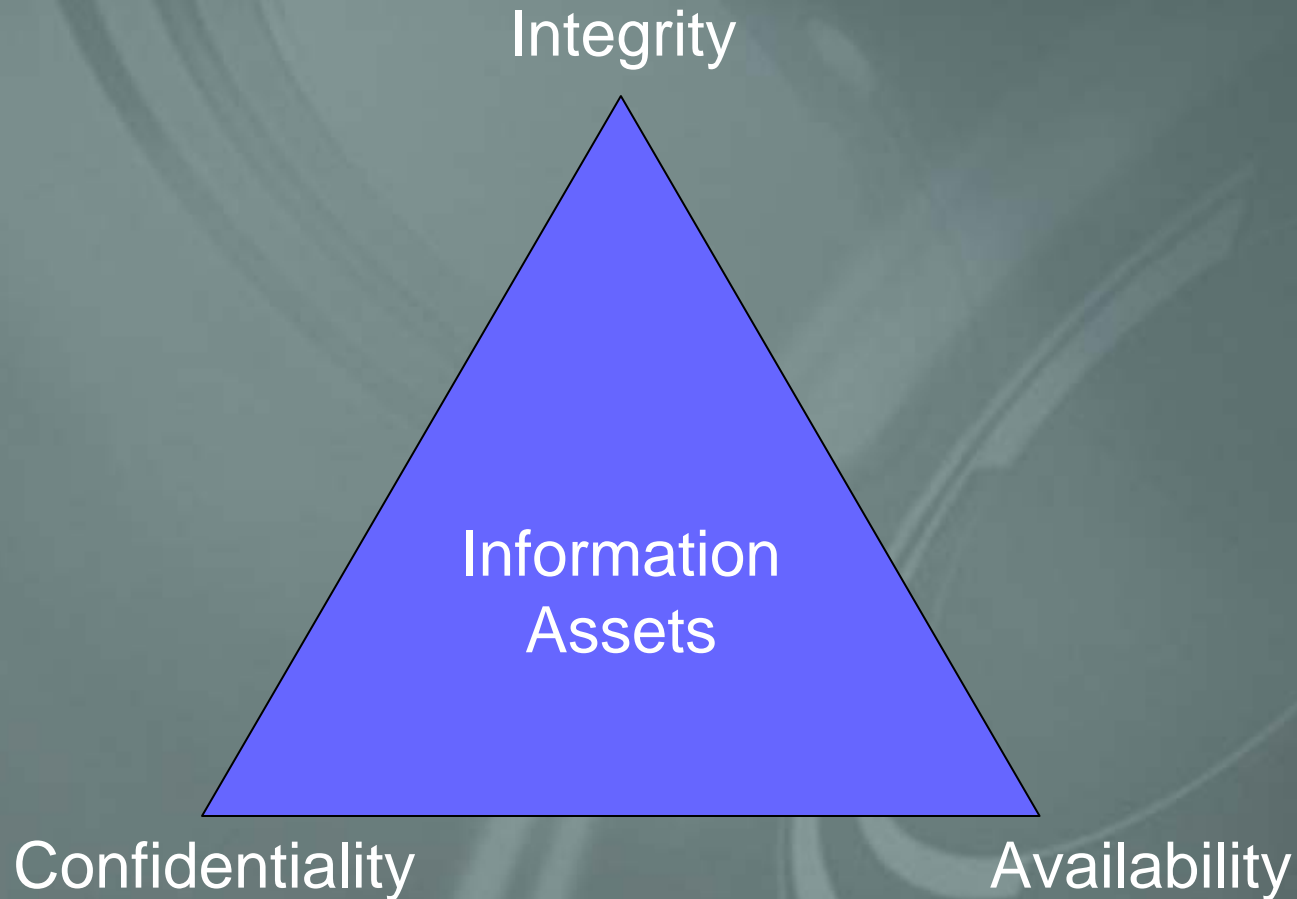


Information

“Information is an asset that, like other important business assets, is essential to an organization’s business and consequently needs to be suitably protected.”

BS ISO/IEC 17799:2005

Information Security



Business Environment

- ❑ Internet connectivity is ubiquitous
- ❑ Businesses and government *require* network inter-connectivity
- ❑ Infrastructure has expanded as technology and business process have become inseparable
- ❑ Out-sourcing of critical business functions is common
- ❑ Migration of critical business functions off-shore

Domestic Regulatory Environment

- ❑ Sarbanes-Oxley Act
- ❑ PCAOB Rel. 2004-001 Audit Section
- ❑ SAS94
- ❑ Fair Credit Reporting Act (FCRA)
- ❑ AICPA Suitability Trust Services Criteria
- ❑ SEC CFR 17: 240.15d-15 Controls and Procedures
- ❑ NASD/NYSE 240.17Ad-7 Transfer Agent Record Retention
- ❑ GLBA (15 USC Sec 6801-6809) 16 CFR 314
- ❑ Appendix: 12 CFR 30, 208, 225, 364 & 570
- ❑ Federal Financial Institutions Examination Council (FFIEC) Information Security
- ❑ FFIEC Business Continuity Planning
- ❑ FFIEC Audit
- ❑ FFIEC Operations
- ❑ Health Insurance Portability and Accountability Act (HIPAA) § 164
- ❑ 21 CFR Part 11 – FDA Regulation of Electronic Records and Electronic Signatures
- ❑ Payment Card Industry Data Security Standard (PCI-DSS)
- ❑ Federal Trade Commission (FTC)
- ❑ CC1798 (SB1386)
- ❑ Federal Information Security Management Act (FISMA)
- ❑ USA PATRIOT
- ❑ Community Choice Aggregation (CCA)
- ❑ Federal Information System Controls Audit Manual (FISCAM)
- ❑ General Accounting Office (GAO)
- ❑ FDA 510(k)
- ❑ Federal Energy Regulatory Commission (FERC)
- ❑ Nuclear Regulatory Commission (NRC) 10CFR Part 95
- ❑ Critical Energy Infrastructure Information (CEII)
- ❑ Communications Assistance for Law Enforcement Act (CALEA)
- ❑ Digital Millennium Copyright Act (DMCA)
- ❑ Business Software Alliance (BSA)
- ❑ New Basel Capital Accord (Basel-II)
- ❑ Customs-Trade Partnership Against Terrorism (C-TPAT)
- ❑ Video Privacy Protection Act of 1988 (codified at 18 U.S.C. § 2710 (2002))

International Regulatory Environment

- ❑ New Basel Capital Accord (Basel-II)
- ❑ Payment Card Industry Data Security Standard (PCI-DSS)
- ❑ Society for Worldwide Interbank Funds Transfer (SWIFT)
- ❑ Personal Information Protection Act (PIPA) – Canada
- ❑ Personal Information and Electronic Documents Act (PIPEDA) – Canada
- ❑ Personal Information Privacy Act (JPIPA) – Japan
- ❑ SafeSecure ISP – Japan
- ❑ Federal Consumer Protection Code, E-Commerce Act – Mexico
- ❑ Privacy and Electronic Communications (EC Directive) Regulations 2003
- ❑ Directive 95/46/EC Directive on Privacy and Electronic Communications – European Union
- ❑ Central Information System Security Division (DCSSI) Encryption – France
- ❑ Federal Data Protection Act (FDPA - Bundesdatenschutzgesetz - BDSG) of 2001 – Germany
- ❑ Privacy Protection Act (PPA) of Schleswig-Holstein of 2000 – Germany
- ❑ US Department of Commerce “Safe Harbor”

Why ISO/IEC 27001:2005?

- ❑ Business oriented, process driven
- ❑ Comprehensive and holistic framework – Information Security Management as a complete system
- ❑ Measurable – Valuation of assets and scaling of risk
- ❑ Repeatable – Formal approach, structured processes
- ❑ Scalable – Facilitates prototyping, adaptable
- ❑ Defensible – Articulates level of assurance
- ❑ Recognizes information in all forms
- ❑ Requires governance (management buy-in)
- ❑ Utilizes “best practices”
- ❑ Promotes security awareness throughout organization
- ❑ Incorporates Total Quality Management (continuous improvement)

Code of Practice and Specification for Use

ISO/IEC17799:2005

Code of Practice For
Information Security
Management

Draft Specification
Released, June 2005

ISO 27001:2005

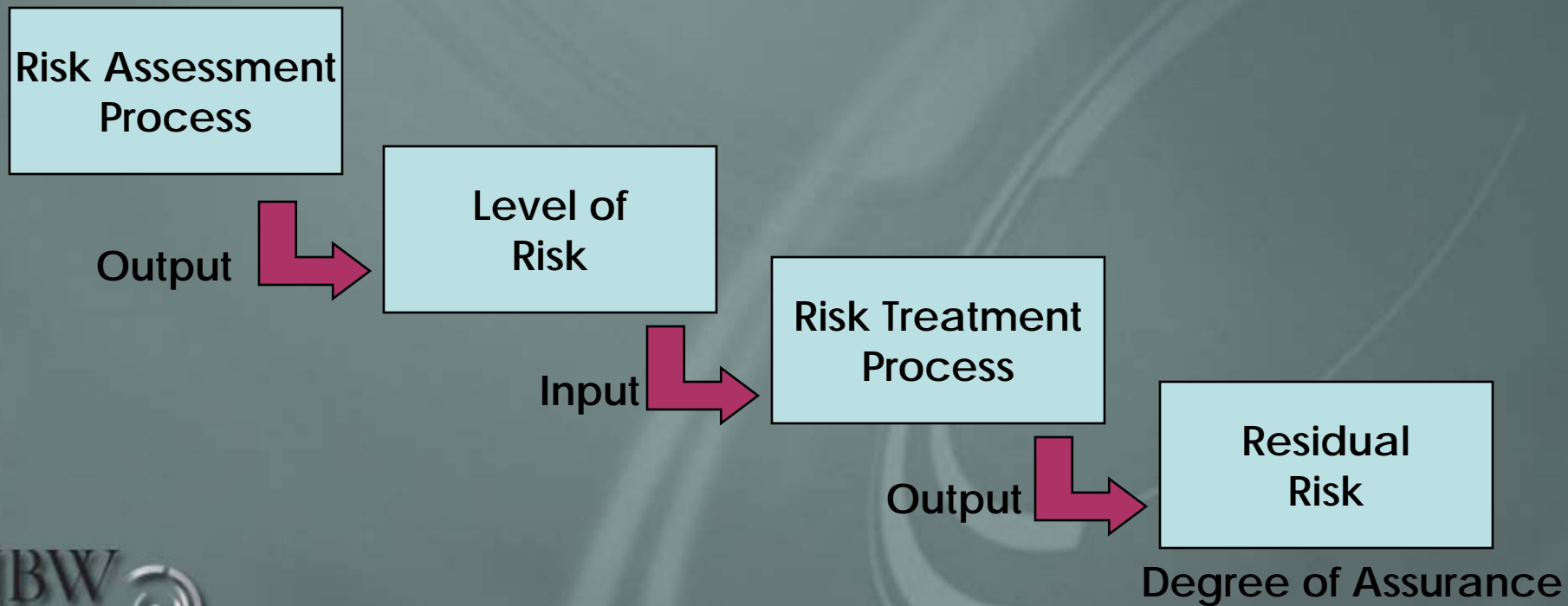
Information Security
Management
Requirements Specification

Adopted by ISO
October, 2005

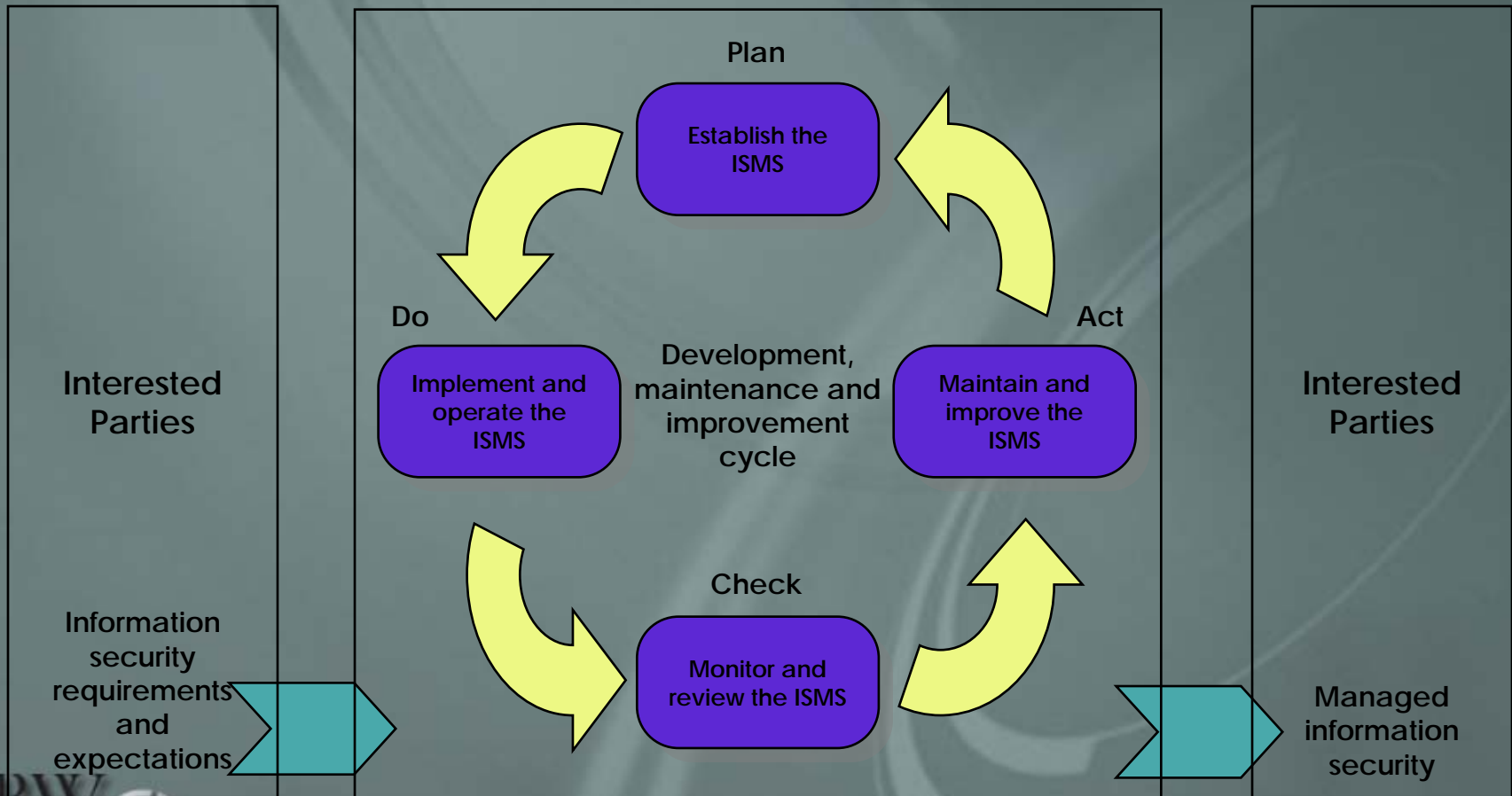


Risk Management

Key element of ISO27001 is the
Degree of Assurance determined by:



PDCA Model Applied to ISMS



ISO 27001:2005

General Requirements

Control Objectives and Controls (Annex A)

- ❑ Security Policy
- ❑ Organization of Information Security
- ❑ Asset Management
- ❑ Human Resources Security
- ❑ Physical and Environmental Security
- ❑ Communications and Operations Management
- ❑ Access Control
- ❑ Information Systems Acquisition, Development and Maintenance
- ❑ *Information Security Incident Management*
- ❑ Business Continuity Management
- ❑ Compliance

A.13 Information Security Incident Management

A.13.1 Reporting Information security events and weaknesses

A.13.1.1 Reporting Information Security events

A.13.1.2 Reporting security weaknesses

A.13.2 Management of information security incidents and improvements

A.13.2.1 Responsibilities and procedures

A.13.2.2 Learning from Information Security incidents

A.13.2.3 Collection of evidence

Incident Types

- ❑ Natural disasters
- ❑ Physical security breaches
- ❑ Viruses and worms
- ❑ Trojans and spyware
- ❑ Employee misconduct
- ❑ Accidental or inadvertent incidents
- ❑ Labor and trade union actions
- ❑ Terrorism and Cyber-terrorism
- ❑ System or network security breaches
- ❑ CGI exploits
- ❑ Distributed denial of service
- ❑ Hoaxes
- ❑ Theft of proprietary data (IP)
- ❑ Router compromise
- ❑ System compromise
- ❑ Lost/stolen laptop
- ❑ ????

Standards-based Incident Response

- ❑ Management Oversight (Governance)
- ❑ Risk management strategy
 - Asset identification and classification
 - Documented risk assessment process
 - Documented risk treatment strategy
- ❑ Incident Response policy
- ❑ Incident Response planning
 - Disaster recovery/business continuity planning
 - Security incident response
 - Employee awareness training
 - Testing
- ❑ Quality management/continuous improvement

Incident Response

Strategic:

Governance and oversight

**Incident
Response
Policy**

Proactive:

Team deployment

**Incident
Response
Team**

**Scope &
Objectives**

Constituency

Reactive:

*Response
and recovery*

Incident Response Procedures

Successful Incident Response

Required components

- ❑ Senior management commitment
- ❑ Clearly defined constituency
- ❑ Clearly defined objectives
- ❑ Clearly defined services
- ❑ Business impact analysis
- ❑ Documented and approved policy
- ❑ Response team members identified
- ❑ Defined roles and responsibilities
- ❑ Documented processes, procedures and work instructions
- ❑ Identified measurement points (metrics)
- ❑ Linkages to other internal and external organizations

Incident Response Philosophy

“Immature strategy is the cause of grief”

- Miyamoto Musashi (1584 – 1645)

Incident Response Process

❑ Proactive strategies

- Planning
- Testing
- Monitoring and detection

❑ Reactive strategies

- Analysis
- Isolation
- Containment
- Investigation
- Mitigation
- After-action analysis and reporting (TQM)

Incident Response Team

Clearly defined and static core team

- ❑ Technical lead
- ❑ Management
- ❑ Engineering
- ❑ Logistics/Project management
- ❑ Legal
- ❑ Public Relations
- ❑ “Deputized” team members
- ❑ All team members must be vetted and vested

Proactive Strategies

Avoiding immature strategy

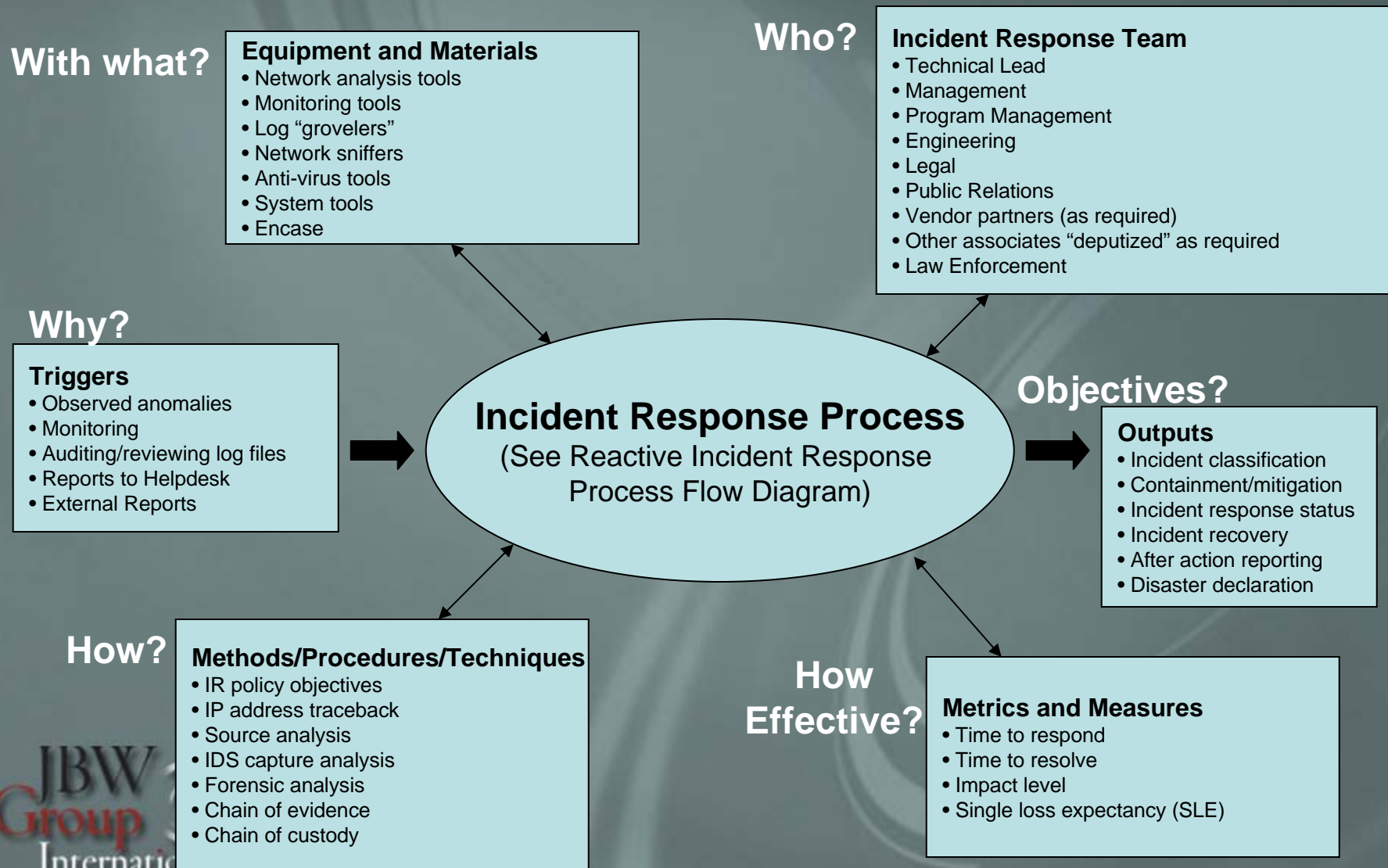
- ❑ Planning is critical to success
- ❑ Anticipate logistical needs
- ❑ Establish linkages external to the core team
- ❑ Test frequently and urgently
- ❑ Deploy, assess and improve monitoring and detection capabilities
- ❑ Deploy enterprise-wide security awareness training
- ❑ Develop metrics to meet objectives
- ❑ Encourage management/sponsor review
- ❑ Analyze for areas of improvement

Incident Response Metrics

Measure and report on performance

- ❑ Include quantitative *and* qualitative
- ❑ Time to respond
- ❑ Time to resolve
- ❑ Incident classification (type and severity)
- ❑ Number and type of incidents
- ❑ Single loss expectancy (SLE)
- ❑ Annualized loss expectancy (ALE)

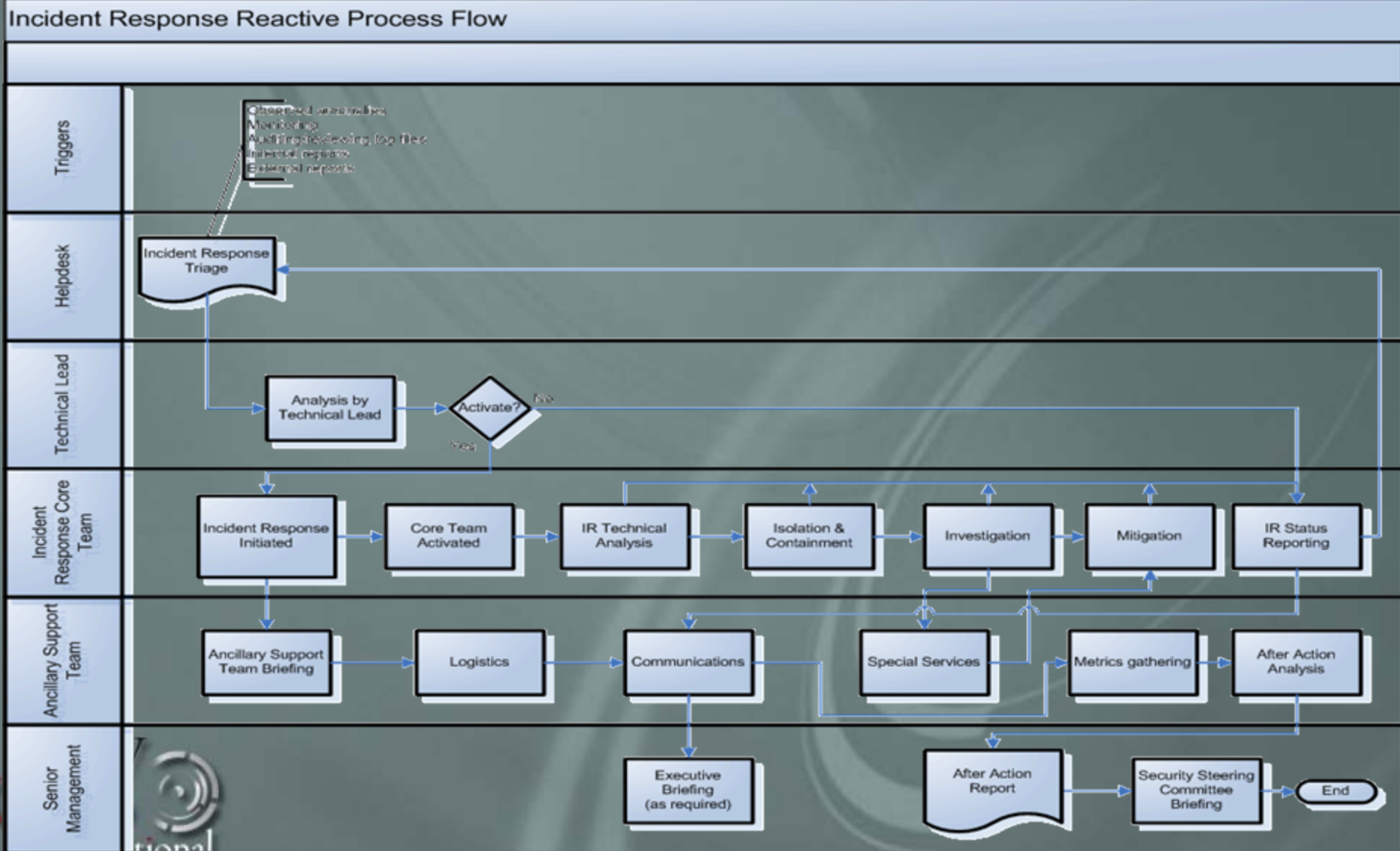
Incident Response Process Diagram



Reactive Response

- ❑ Analysis – Systematic review of data
- ❑ Isolation – Separation from the environment
- ❑ Containment – Maintain isolation of the incident
- ❑ Investigation – Cause and effect
- ❑ Mitigation – Fix, diminish, deploy countermeasures or otherwise deal
- ❑ After-action Analysis – (TQM) Includes root cause and recommended solutions

Reactive Response Process Flow



Continuous Improvement

After-action reporting should:

- ❑ Include Incident Response world view
- ❑ Describe incident environment
- ❑ Describe response methodology
- ❑ Report response metrics
- ❑ Document results of after action analysis
- ❑ Recommend opportunities for improvement

After-action Reporting

Possible resulting goals and objectives:

- ❑ Ranked by urgency/criticality
- ❑ Tackle “low-hanging fruit” first
- ❑ Greatest cost-benefit ratio
- ❑ Legal or regulatory requirements
- ❑ As input to policy development

Practical Matters

- ❑ Gather your “hacker intel”
- ❑ Be prepared to provide awareness training services
- ❑ Be prepared to provide non-emergency services
- ❑ Support your local sheriff

Mature Strategy

Formula for Successful Incident Response

- ❑ Incident response is guided by a well understood framework
- ❑ Mandated by management
- ❑ Focused by risk assessment and impact analysis
- ❑ Supported by clear policy and guidelines
- ❑ Well documented process and procedures
- ❑ Frequently exercised
- ❑ Vetted and vested team
- ❑ Clearly defined and understood roles and responsibilities
- ❑ Develop and report metrics
- ❑ Build on knowledge and experience to continually improve.

Top Ten List

Top Ten Things the Incident Response Team doesn't want to hear:

1. "The CEO forgot the pass phrase for the encrypted files on his laptop. Can you swing by quick and help him out?"
2. "Write protected?"
3. "I thought somebody tipped the server but I've been digging around for a couple of hours and haven't found anything."
4. "Show me the policy that says I can't . . ."
5. "I just emailed you a bunch of jpg files. Can you give them a look and me tell if they're child porn or not?"
6. "Whatever you need as long as it doesn't cost anything."
7. "Tell me again why we're not supposed to open email attachments?"
8. "Well, of course it's plugged in!"
9. "I heard that there was a new email virus that would kill my dog and get my daughter pregnant!"
10. "I think there's a problem with my mac."



Information Assurance

John B. Weaver

CISSP, CISA, CISM, CPP
President/CEO – Principle Consultant

JBW Group International

PO Box 19393
Minneapolis, MN 55419

877.97.27001

www.JBWGroup.com