HIPAA by the Numbers

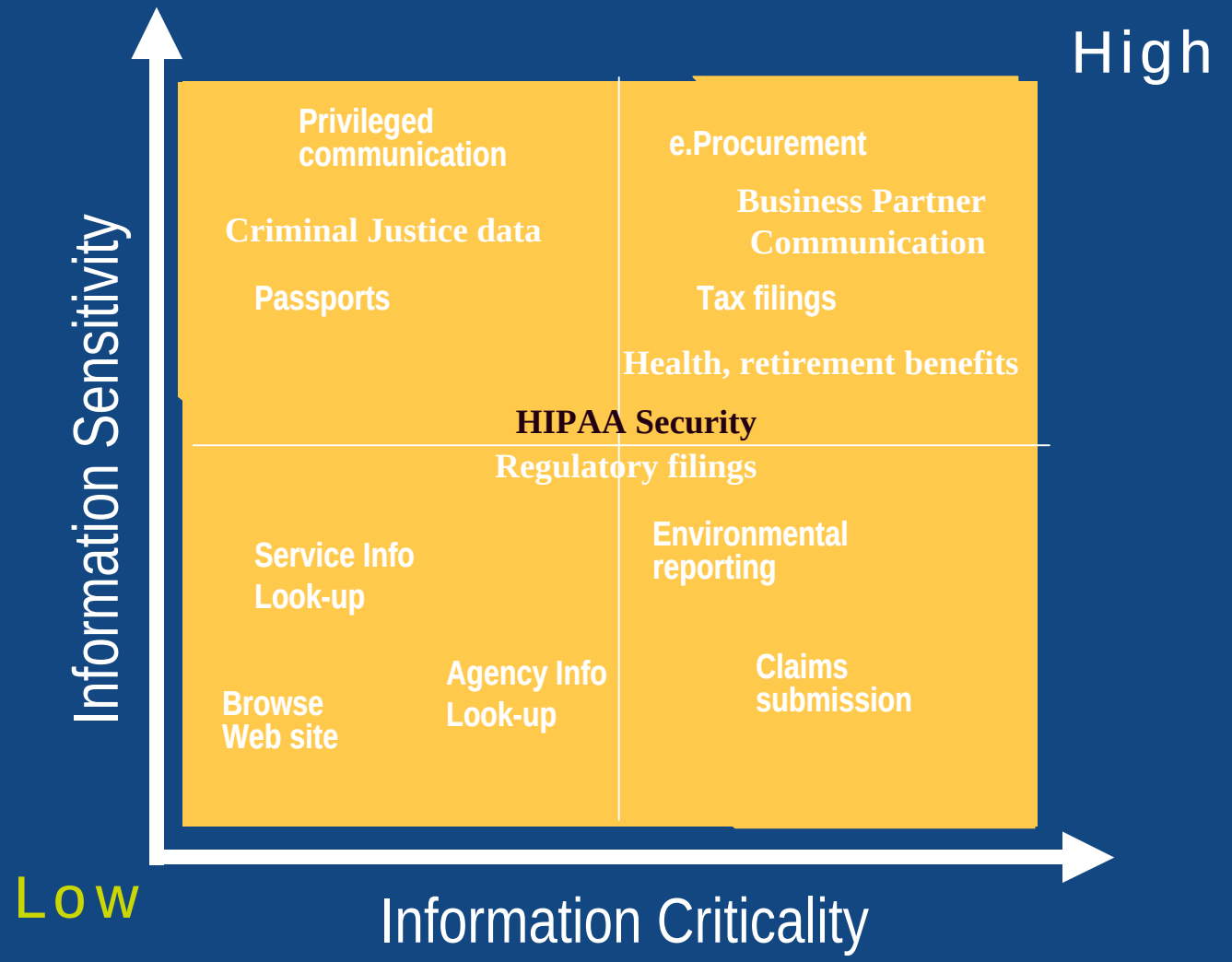
Presented by:

Mark L. Schuweiler
Director of Global Information Assurance Services
EDS Corporation

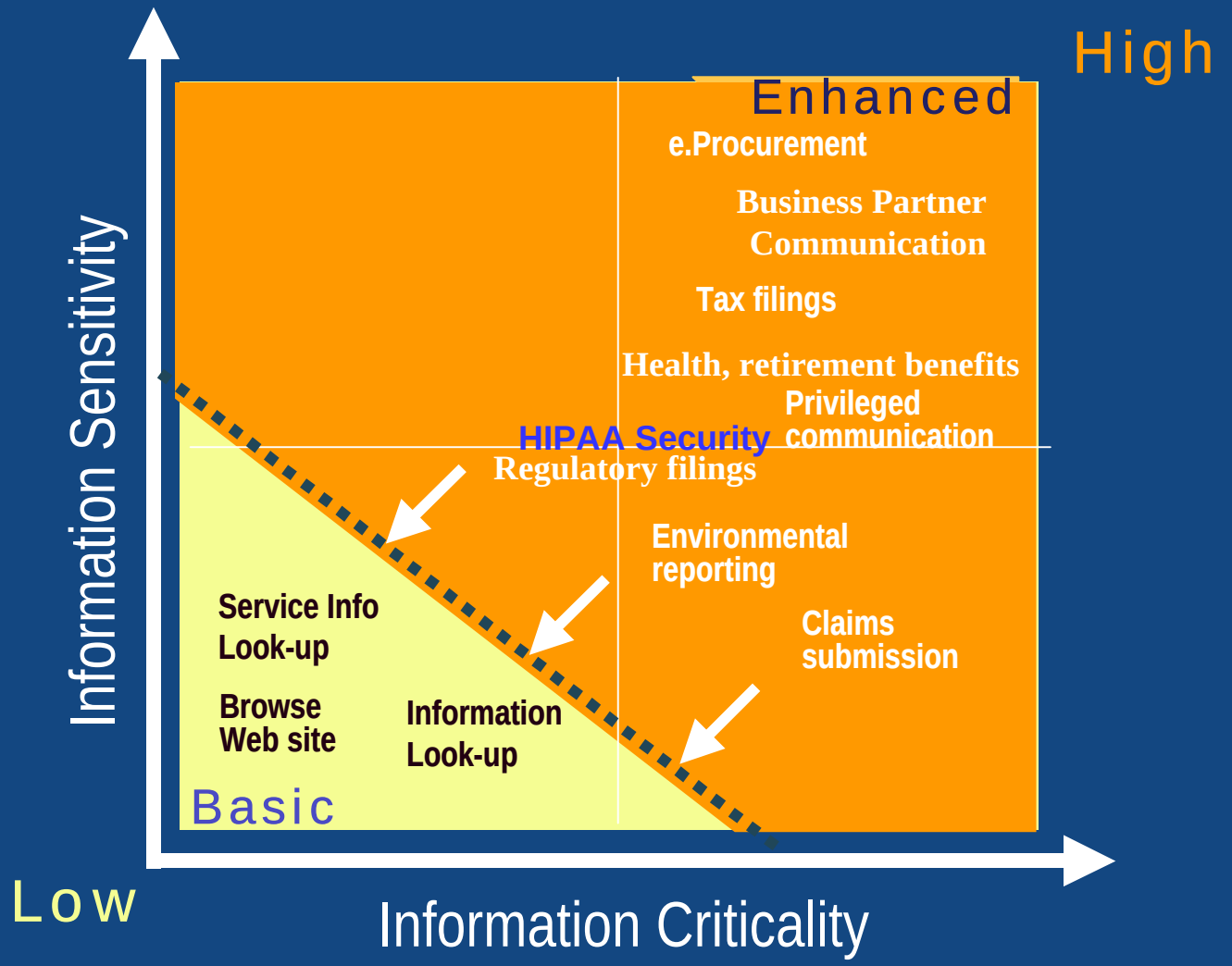
Security vs Privacy

- Privacy – right of a individual to control his/her personal information and to not have it divulged or used without permission
- Security – safeguards and mechanisms that enforce privacy through the protection of integrity, availability, and confidentiality of information.
- Current Status of the Security Rule

Trusted Business Model



Trusted Business Model – Current Status



24 HIPAA Security Rules

- Administrative Procedures
- Physical Safeguards
- Technical Security Services
- Technical Security Mechanisms

Best Practice Foundations

- ISO – 15408, 17799
- DoD – DITSCAP, Rainbow Series,
- ASTM – Health Information Standards
- NIST – SP 800 Series
- FIPS – Federal Information Protection Standards
- OMG – Corba, XML
- CMS – Internet Policy
- FDA 21 CFR Part 11 – Electronic Records-Electronic Signatures Final Rule
- IEEE – Electrical/Electronic Standards
- IETF – Internet Standards
- IATFF – Information Assurance
- CPRI-HOST - Templates
- Carnegie-Mellon – SSE CMM
- DRII – CONOPS, DRP
- CEN – European Pre-Standard Medical Informatics

12 HIPAA Security Administrative Procedures

1. Certification
2. Chain of trust partner agreement
3. Contingency plan
4. Formal mechanism for processing records
5. Information access controls
6. Internal audit
7. Personnel security
8. Security configuration management
9. Security incident reporting
10. Security management process
11. Termination procedures
12. Training

12 HIPAA Security Administrative Procedures

Key Best Practices

- ASTM E1869 – Confidentiality, Privacy, Access and Data Security Principles for Health Information
- ASTM E1985 – Standard Guide for User Authentication and Authorization Administration Procedures
- ASTM E1986 – Standard Guide for Information Access Priviledges to Health Information
- ASTM Standard PS115-99 – Provisional Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems
- CEN – European Pre-Standard Medical Informatics
- CPRI Toolkit – sample agreement templates

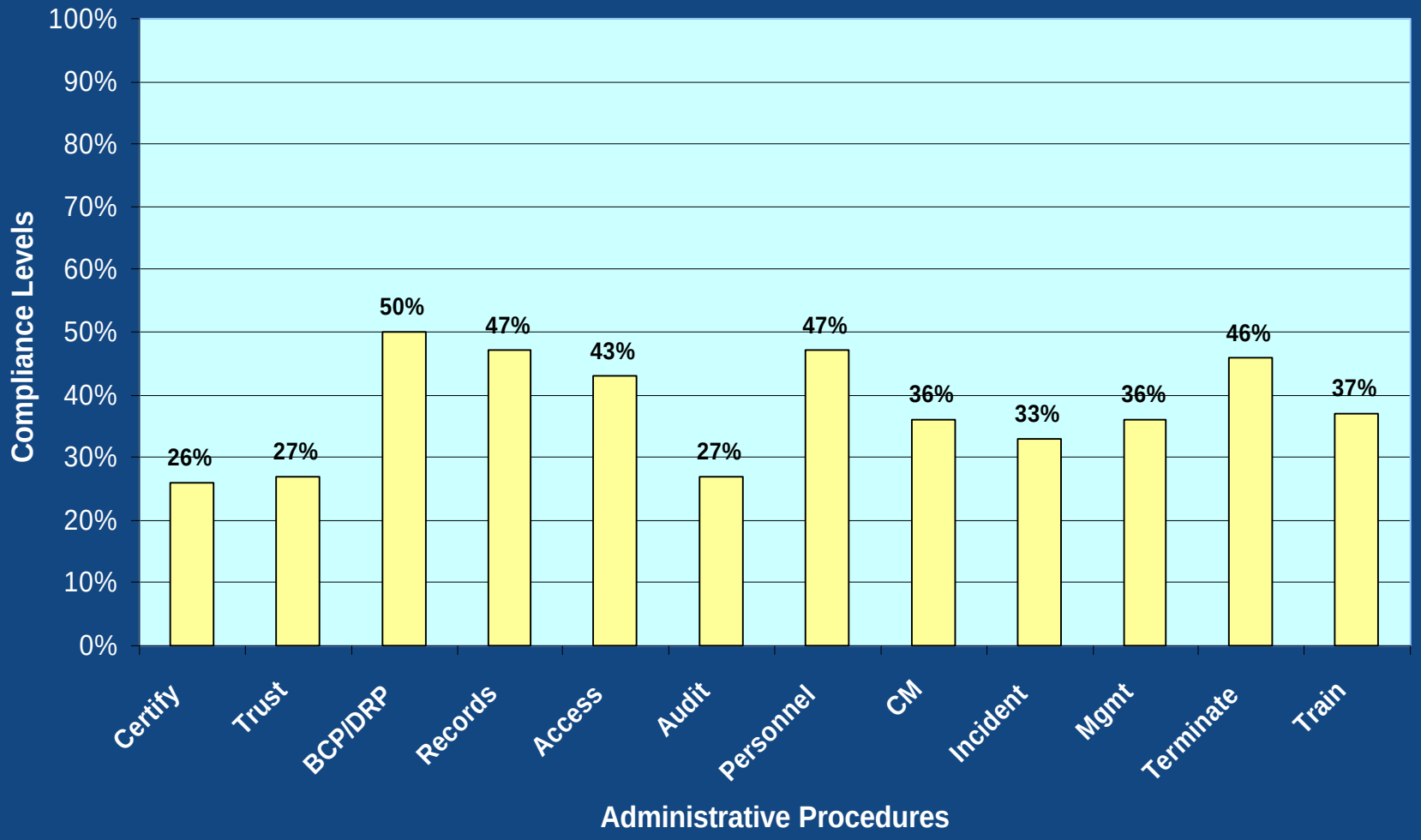
12 HIPAA Security Administrative Procedures

Key Best Practices (cont….)

- DoD Trusted Computer System Evaluation Criteria
- DoD Information Technology Security Certification & Accreditation Process
- FDA 21 CFR Part 11 – Electronic Records-Electronic Signatures Final Rule
- ISO 15408 – Common Criteria for IT Security Evaluation
- NIST SP800-12 – Introduction to Computer Security (The NIST Handbook)
- NIST SP800-14 – Generally Accepted Principles and Practices for Securing Information Technology Systems

12 HIPAA Security Administrative Procedures

Observations from Compliance Assessments



6 HIPAA Security Physical Safeguards

1. Assigned security responsibility
2. Media controls
3. Physical access controls
4. Policy/guideline on workstation use
5. Secure workstation location
6. Security awareness training

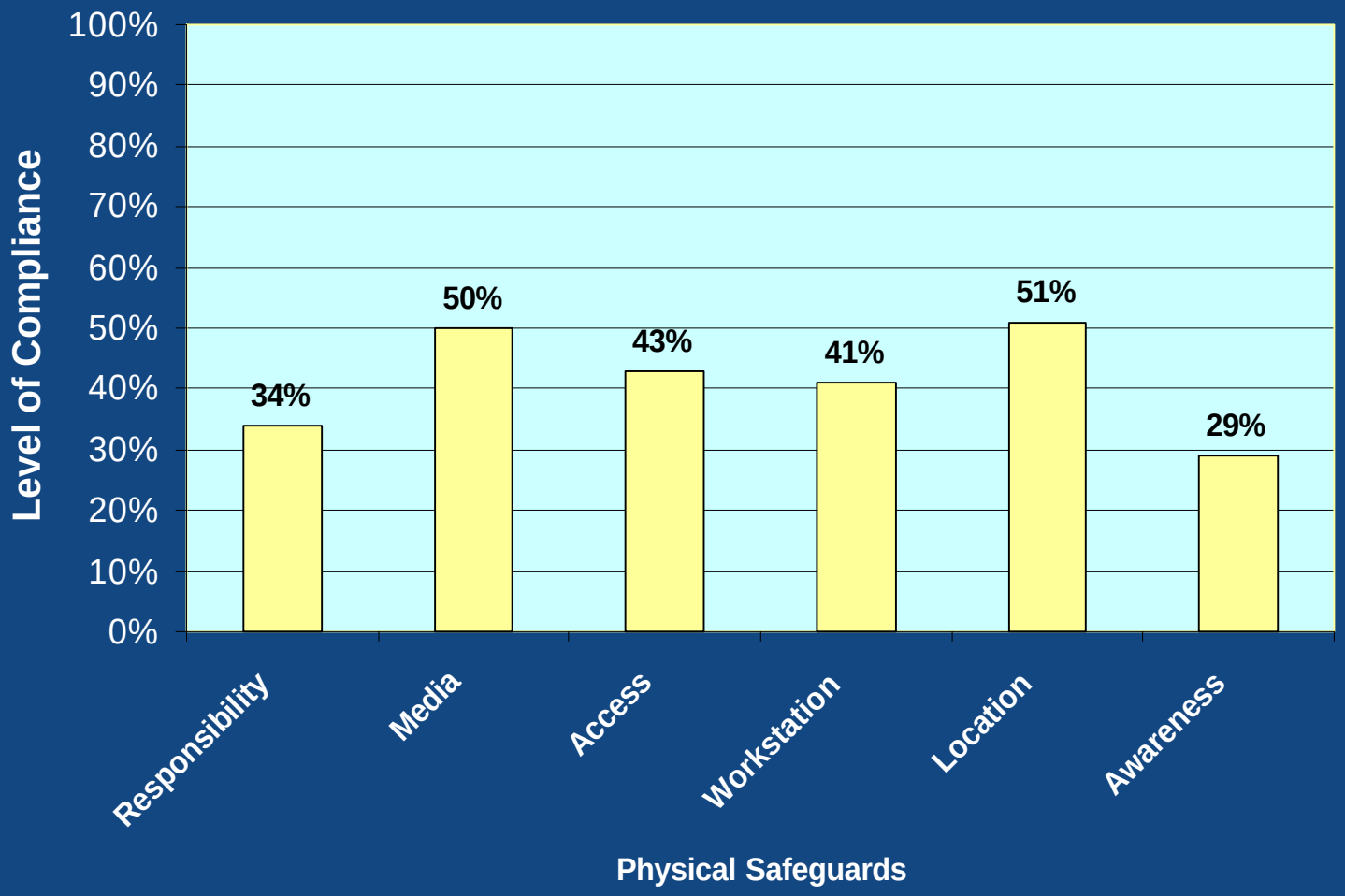
6 HIPAA Security Physical Safeguards

Key Best Practices

- ASTM E1869 – Confidentiality, Privacy, Access and Data Security Principles for Health Information
- CEN – European Pre-Standard Medical Informatics
- FDA 21 CFR Part 11 – Electronic Records-Electronic Signatures Final Rule
- NIST SP800-12 – Introduction to Computer Security (The NIST Handbook)
- NIST SP800-14 – Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP800-16 – Information Technology Security Training Requirements: A Role and Performance –based Model

6 HIPAA Security Physical Safeguards

Observations from Compliance Assessments



5 HIPAA Security Technical Security Services

1. Access controls
2. Audit controls
3. Authorization controls
4. Data authentication
5. Entity authentication

5 HIPAA Security Technical Security Services

Key Best Practices

- ANSI X3.92 – Data Encryption Standard
- ANSI X9.42 – Management of Symmetric Keys Using Diffie-Hillman
- ANSI X9.44 – Key Transport Using RSA
- ANSI X9.45 – Enhanced Management Controls Using Digital Signatures and Attribute Certificates
- ANSI X9.RFC2104 – HMAC:Keyed-Hashing for Message Authentication Triple DES Modes of Operation
- ASTM E1762-95 Standard Guide for Electronic Authentication of Health Care Information

5 HIPAA Security Technical Security Services

Key Best Practices (cont…)

- ASTM E1869-97 – Confidentiality, Privacy, Access and Data Security Principles for Health Information
- ASTM E1985-98 – Standard Guide for User Authentication and Authorization Administration Procedures
- ASTM E1986-98 – Standard Guide for Information Access Priviledges to Health Information
- ASTM Standard PS101-97 – Security Framework for Healthcare Information
- ASTM Standard PS103-97 – Authentication & Authorization Guideline

5 HIPAA Security Technical Security Services

Key Best Practices (cont…)

- ASTM Standard PS115-99 – Provisional Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems
- CEN – European Pre-Standard Medical Informatics
- FDA 21 CFR Part 11 – Electronic Records-Electronic Signatures Final Rule
- FIPS PUB 46-2 Data Encryption Standard
- FIPS PUB 112 – Password Protection
- IEEE 802.10 – Interoperable LAN/MAN Security (SILS)
- IEEE 802.10c – LAN/WAN Security-Key Management

5 HIPAA Security Technical Security Services

Key Best Practices (cont…)

- IETF ID Combined SSL/PCT Transport Layer Security Protocol
- IETF ID Secure HyperText TP Protocol (SHTTP)
- IETF ID SMIME Specification
- IETF RFC1422 – Privacy Enhanced Mail: Part 1: Message Encryption and Authentication Procedures
- IETF RFC1423 – Privacy Enhanced Mail: Part 2: Certificate-Based Key Management
- IETF RFC1424 – Privacy Enhanced Mail: Part 3: Algorithms, Modes, and Identifiers
- ISO/IEC 10181-2 – Information Technology – Security Frameworks for Healthcare Information

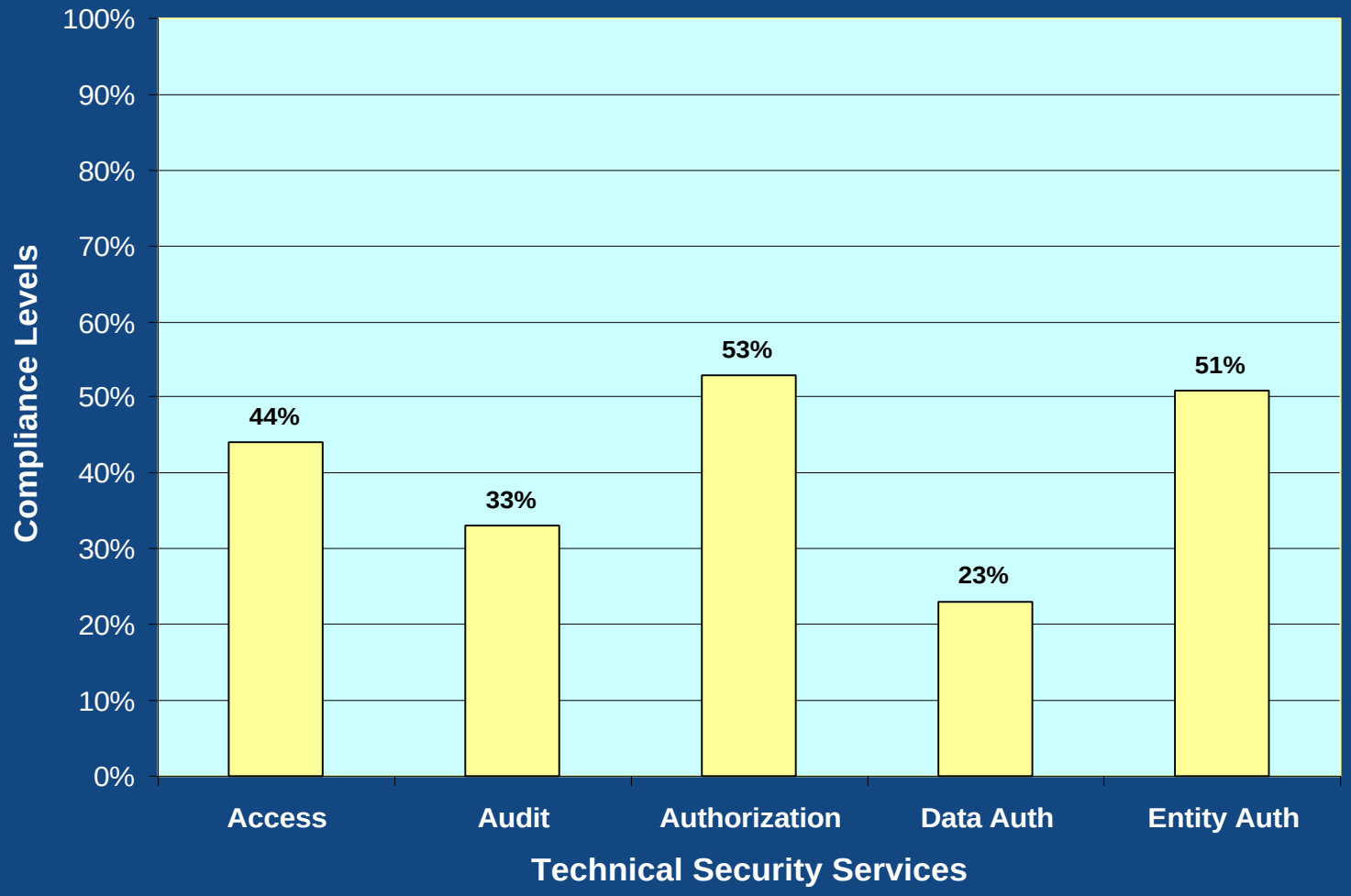
5 HIPAA Security Technical Security Services

Key Best Practices (cont…)

- ISO/IEC 10181-3 – Information Technology – Security Frameworks in Open Systems-Access Control Framework
- ISO/IEC 10164-5 – Information Technology-Open Systems Connection-Systems Management-Event Report Management Function
- NIST SP800-12 – Introduction to Computer Security (The NIST Handbook
- NIST SP800-14 – Generally Accepted Principles and Practices for Securing Information Technology Systems
- PKCS #7 – Cryptographic Message Syntax Standard
- PKCS #11 – Cryptoki B A Cryptographic Token Interface

5 HIPAA Security Technical Security Services

Observations from Compliance Assessments



HIPAA Security Technical Security Mechanism

- Communications controls
  - Integrity controls
  - Message authentication
  - Access controls
  - Encryption
- Network controls
  - Alarms
  - Audit trails
  - Entity authentication
  - Event reporting

HIPAA Security Technical Security Mechanism

Key Best Practices

- ASTM E1869-97 – Confidentiality, Privacy, Access and Data Security Principles for Health Information
- ASTM Standard PS101-97 – Security Framework for Healthcare Information
- CEN – European Pre-Standard Medical Informatics
- CMS Internet Security Policy
- DoD Trusted Computer System Evaluation Criteria
- FIPS PUB 46-2 Data Encryption Standard
- IEEE 802.10 – Interoperable LAN/MAN Security (SILS)
- IEEE 802.10c – LAN/WAN Security-Key Management

HIPAA Security Technical Security Mechanism

Key Best Practices (cont…)

- IETF ID Combined SSL/PCT Transport Layer Security Protocol
- IETF ID Secure HyperText TP Protocol (SHTTP)
- IETF ID SMIME Specification
- IETF RFC1422 – Privacy Enhanced Mail: Part 1: Message Encryption and Authentication Procedures
- IETF RFC1423 – Privacy Enhanced Mail: Part 2: Certificate-Based Key Management
- IETF RFC1424 – Privacy Enhanced Mail: Part 3: Algorithms, Modes, and Identifiers

HIPAA Security Technical Security Mechanism

Key Best Practices (cont…)

- ISO/IEC 9798-2 – Information Technology-Security Techniques-Entity Authentication Mechanisms-Part 1 Entity Authentication
- ISO/IEC 9798-2 – Information Technology-Security Techniques-Entity Authentication Mechanisms-Part 2 Authentication Mechanisms
- ISO/IEC 10164-4 – Information Technology-Open Systems Connection-Systems Management: Alarm Reporting Function
- ISO/IEC 10164-5 – Information Technology-Open Systems Connection-Systems Management-Event Report Management Function

HIPAA Security Technical Security Mechanism

Key Best Practices (cont…)

- ISO/IEC 10164-7 - Information Technology-Open Systems Connection-Systems Management: Security Alarm Reporting Function
- ISO/IEC 10164-9 – Information Technology – Open Systems Connection – System Management: Objects and Attributes for Access Control
- ISO/IEC 10181-7 – Information Technology – Security Frameworks In Open Systems-Security Audit Framework
- NIST MISPC – Minimum Interoperability Specification for PKI Components

HIPAA Security Technical Security Mechanism

Key Best Practices (cont…)

- NIST SP800-3 – Establishing a Computer Security Incident Response Capability
- NIST SP800-12 – Introduction to Computer Security (The NIST Handbook
- NIST SP800-13 – Telecommunications Guidelines for Telecommunications Management Network
- NIST SP800-17 – Modes of Operation Validation System (MOVS): Requirements and Procedures (for Data Encryption)
- NIST SP800-20 – Modes of Operation Validation System for Triple DES Encryption Algorithm (TMOVS): Requirements and Procedures

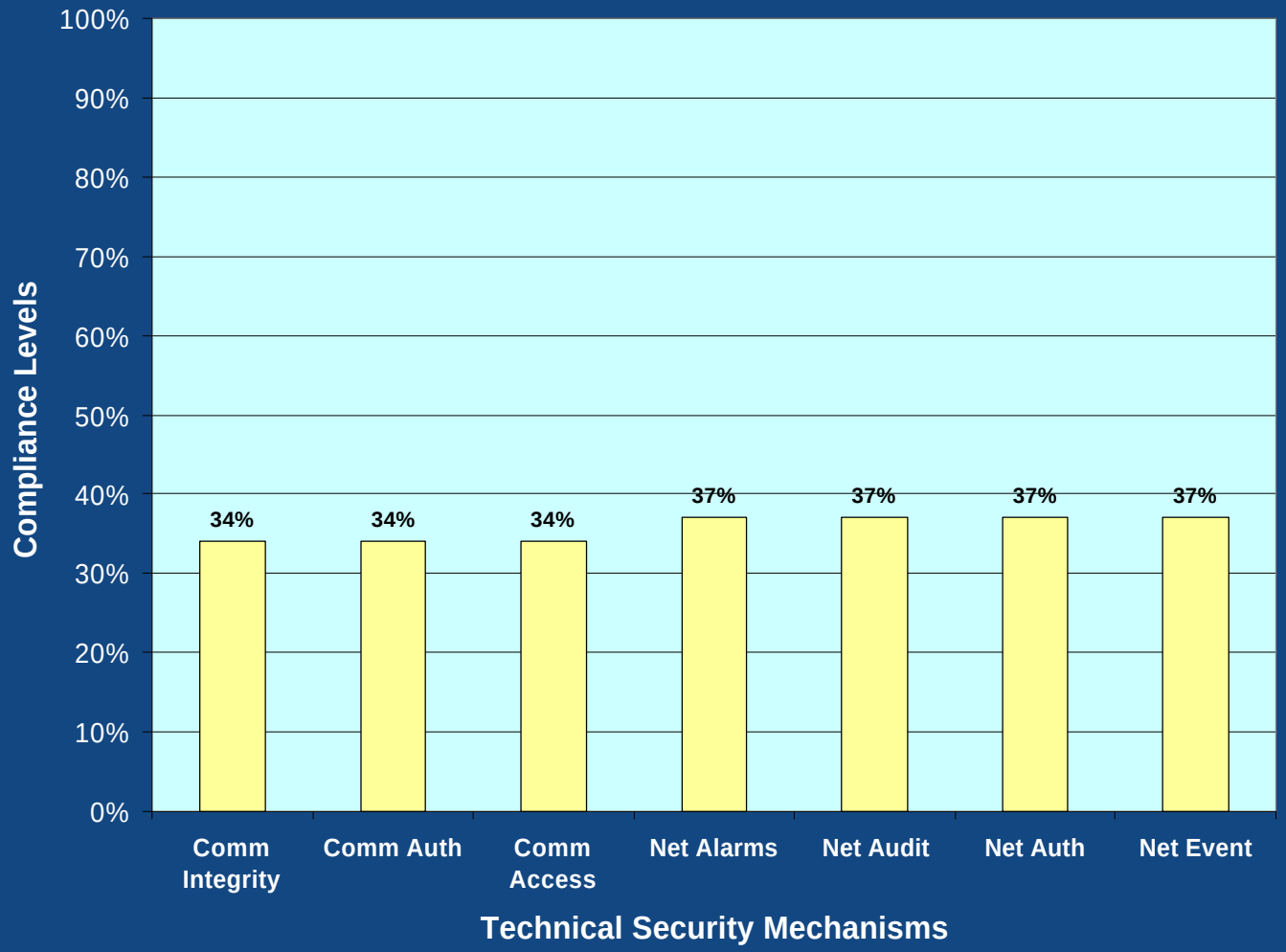
HIPAA Security Technical Security Mechanism

Key Best Practices (cont…)

- OMG Corba Security Standard
- PKCS #7 – Cryptographic Message Syntax Standard

HIPAA Security Technical Security Mechanism

Observations from Compliance Assessments



Conclusions

- HIPAA Security is only part of the solution
- Electronic Information Security fosters the trusted environment necessary for e.Health
- Electronic Information Management requires changes to business practices
- Will require substantial investment in time and money
- Benefit from established Best Practices
- Security awareness is everyone’s responsibility
- Piece meal approach will not work
- Out-of-the-box solutions do not exist
- Security personnel must have proper training

Some Useful References

- http://csrc.nist.gov
- http://www.epic.org
- http://www.iatf.net
- http://www.sans.org
- http://niap.nist.gov
- http://www.ieee.org/
- http:// www.ietf.org
- http://mattche.iiie.disa.mil
- http://www.dr.org
- http://www.omg.org
- http://www.astm.org/
- http://www.contingencyplanning.com
- http://www.iso.ch/isoen/ISOOnline.frontpage



Our Vision

EDS … the recognized global leader in ensuring clients achieve superior value in the Digital Economy

- *By delivering the right strategies, solutions and services*
- *Through superior execution on a sustained basis*