

THE THIRD NATIONAL HIPAA SUMMIT


HIPAA Privacy: Impact on Business Associates

Suzy Buckovich, IBM
HIPAA National Practice



Agenda



- ☐ **Business Associate Contract (BAC) Provisions**
- ☐ **Business Impact**
- ☐ **Challenges of Meeting BAC Provisions**
- ☐ **Practical Steps Towards Fulfilling the Contractual Obligations**
 -  NASCO Case Study: One Approach
- ☐ **What to Expect from Covered Entities**





e-business

Business Associate Contract Provisions

- ☐ **Not to use or disclose Protected Health Information (PHI) not permitted by the Covered Entity (CE)**
- ☐ **Use appropriate safeguards to protect PHI**
- ☐ **Report unauthorized disclosures to CE**
- ☐ **Ensure subcontractors and agents safeguard PHI**
- ☐ **Make PHI available to support individuals rights to (1) access/copy PHI, (2) amend PHI, and (3) receive an accounting of disclosures**
- ☐ **Make internal records available to DHHS for compliance**
- ☐ **Return or destroy PHI upon termination**



e-business

Business Impact

- ☐ **Not off the hook under HIPAA**
- ☐ **Contractual responsibilities and liability (including state law)**
- ☐ **Operational, policy and procedure changes to safeguard PHI**
- ☐ **Must understand privacy practices in your organization**
- ☐ **Must identify with whom you are receiving and disclosing PHI**

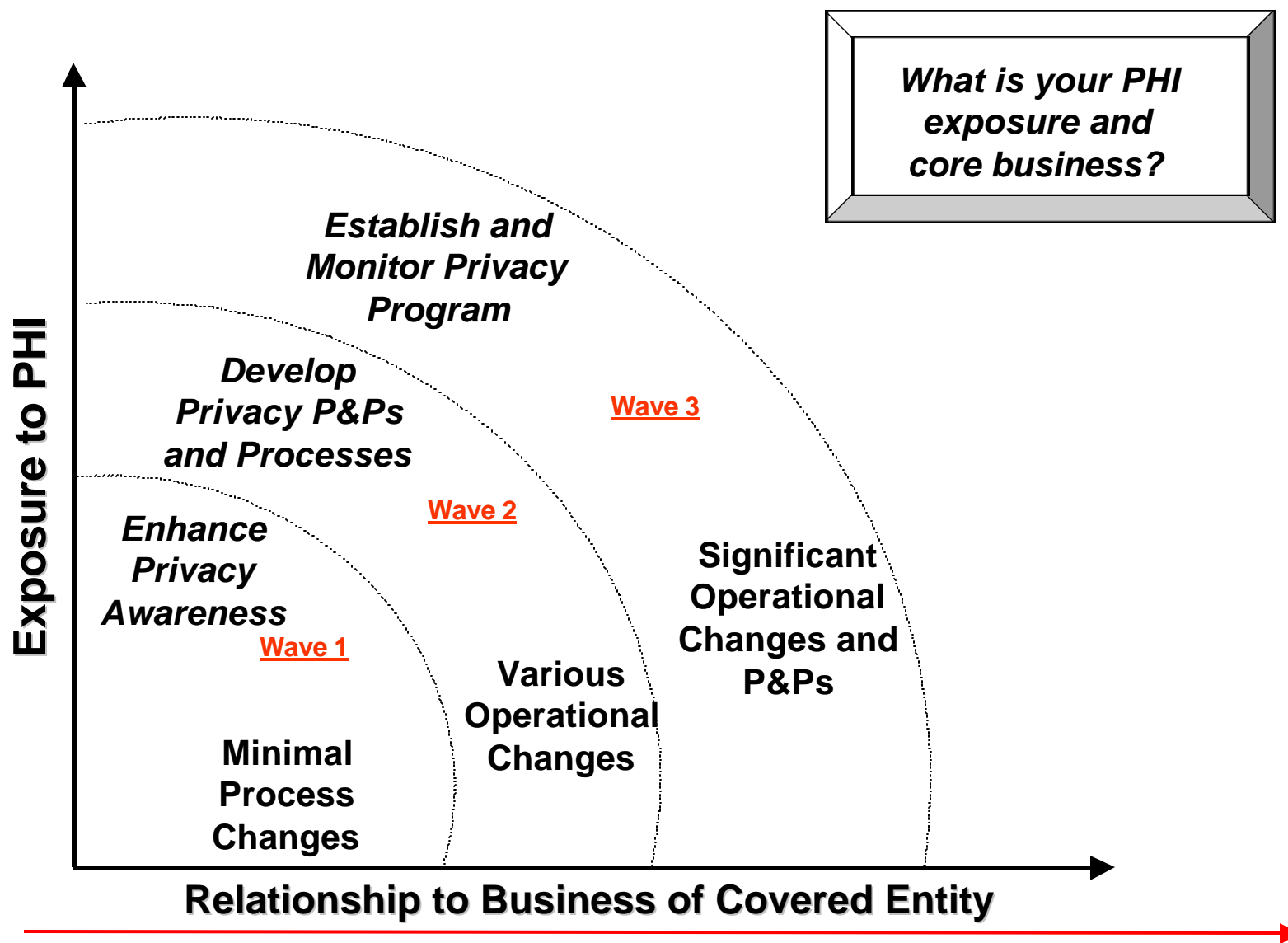
Business Associate

Contract

1. Uses and Disclosures
2. Individual Rights
3. Termination
4. Internal Books
5. Reporting
6. Accounting Disclosures



Varying operational impact depending on what you do and your PHI exposure as a business associate





e-business

Adhering to the BAC requires assessing your capability to fulfill contractual provisions

Operational

- Understanding flow of PHI
- Uses and disclosures
- Privacy responsibility
- Workforce training
- Termination procedures
- System impact

BAC

Policy and Procedures

- Organizational privacy policy
- Departmental policies
- Complaints and sanctions
- Internal books
- PHI storage

Individual Rights Processes

- Access
- Copy
- Amend
- Accounting of disclosures
- Tracking requests, actions



e-business

Challenges of Fulfilling BAC Provisions

- ☐ **Understanding PHI flow and handling within and outside of organization**
- ☐ **Ensuring subcontractors meet the same standards**
- ☐ **Providing assurances to CEs**
- ☐ **Developing processes to support individual rights**
- ☐ **Safeguarding PHI**





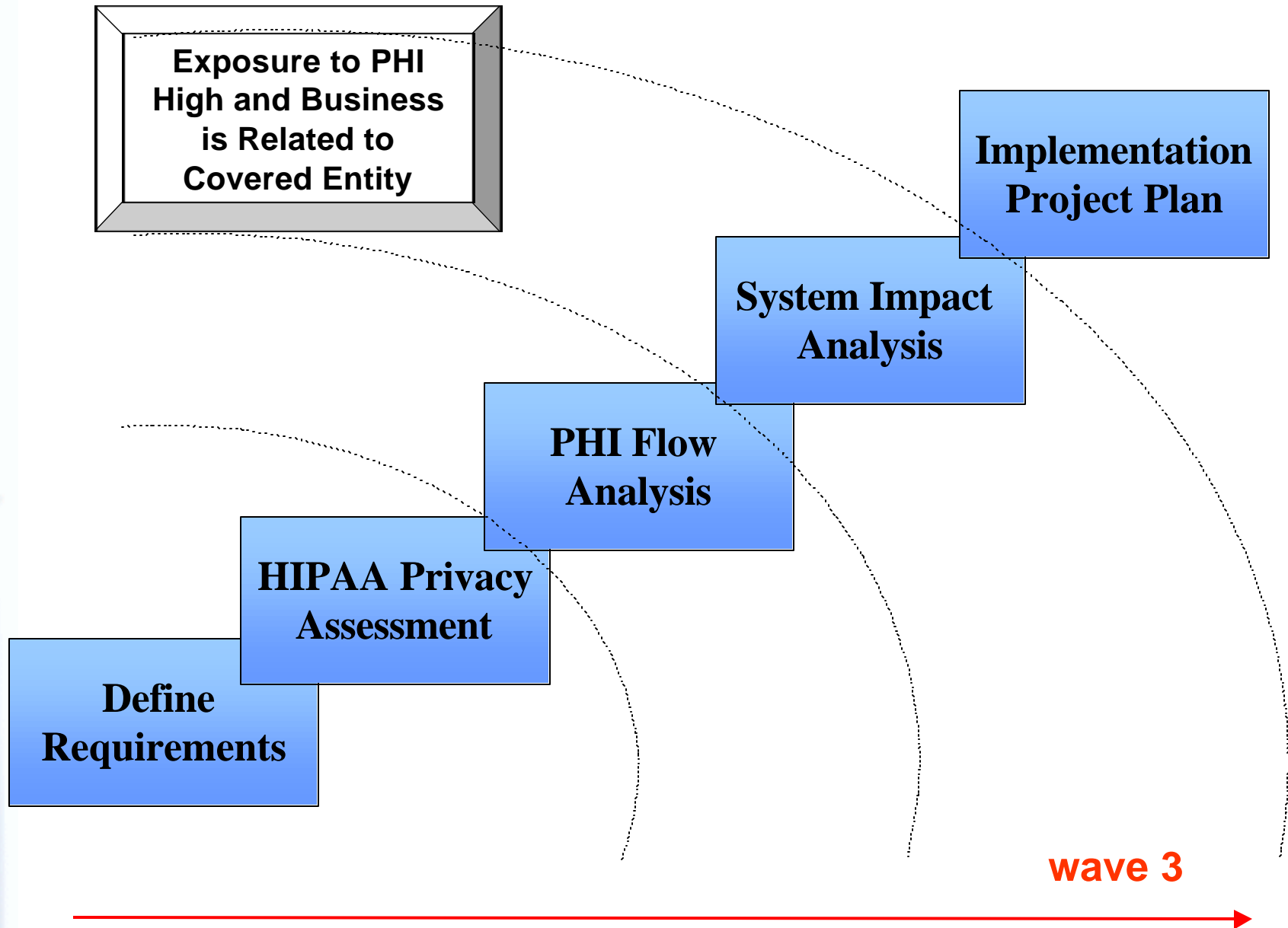
□ Background

- National Account Service Company LLC
- Transaction processing for 38 BCBS Plans, 6 million members
- 80 million claims per year
- Involves many IT vendors
- Data and application centers
- NASCO Processing System (NPS)
- Tests applications and provides Customer Plan NPS training



e-business

NASCO Privacy Approach

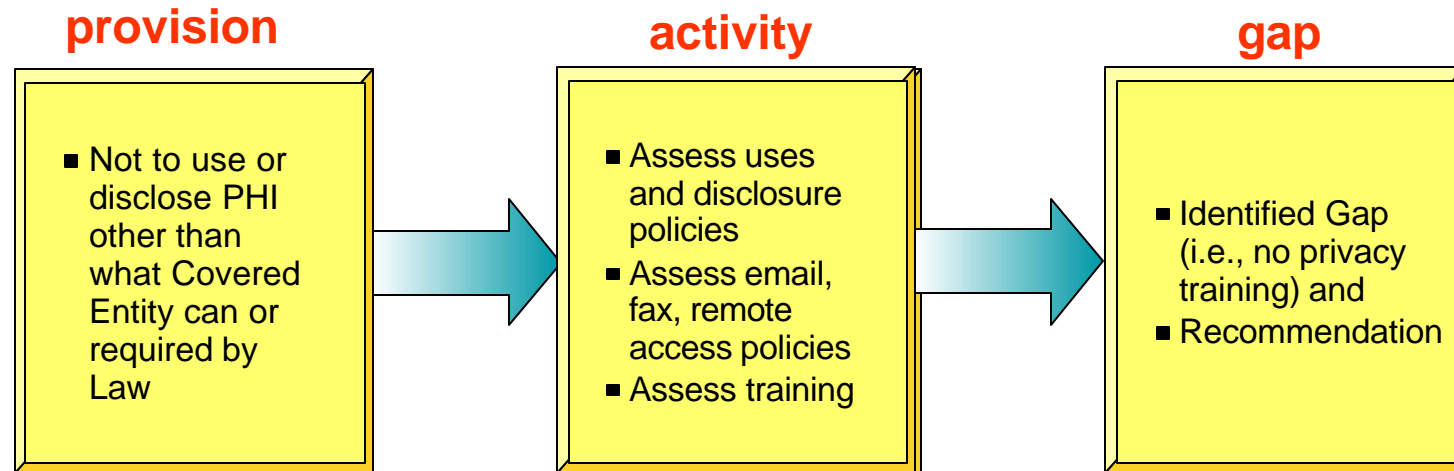




e-business

Steps to Meet BAC Requirements

- ❑ **Conduct detailed analysis of each BAC provision, associated activity, and gap**

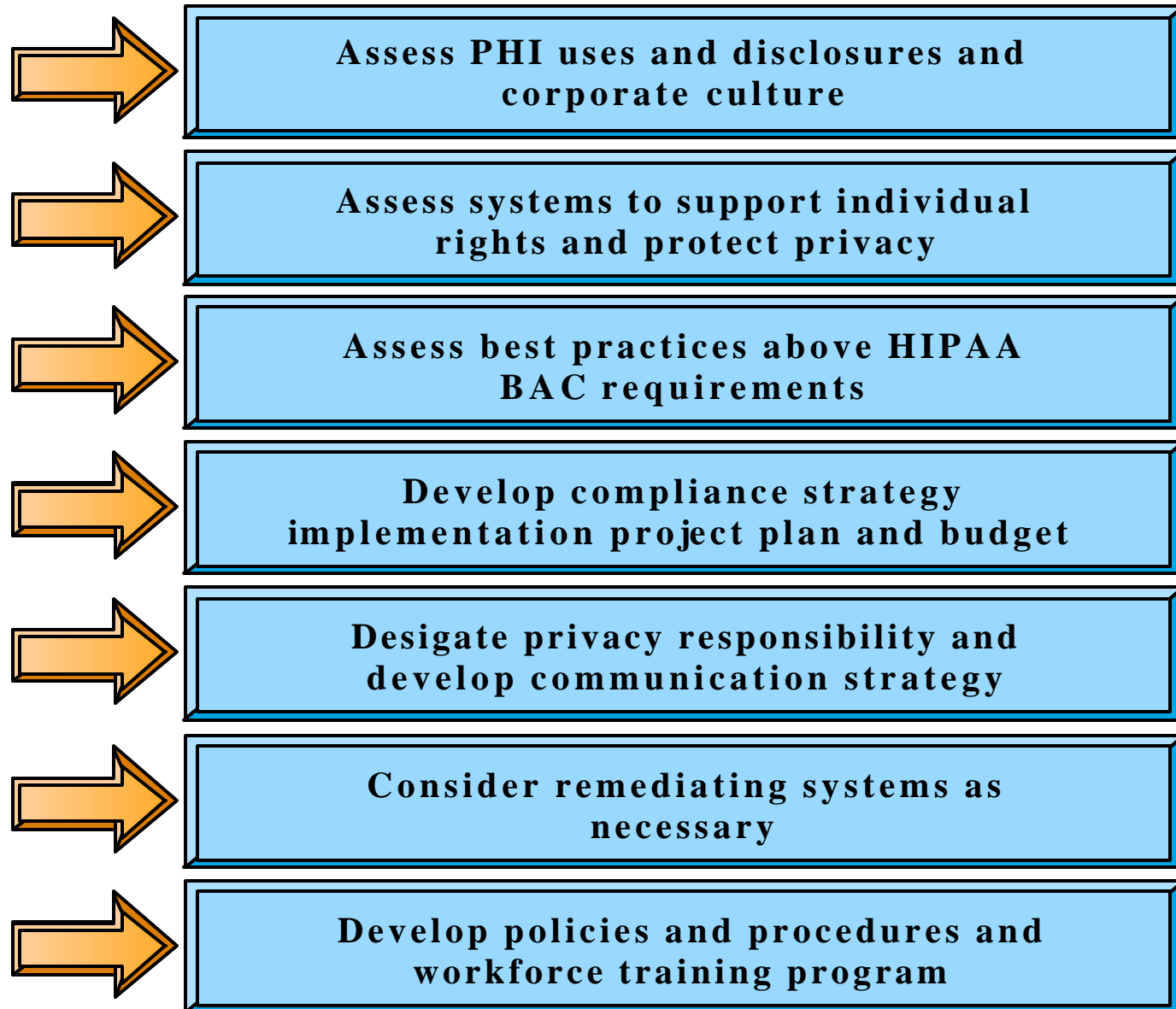


- ❑ **Assess PHI flow and exposure (wave 3)**
- ❑ **Identify and document business associates and subcontractors**
- ❑ **Review current contracts (involve legal)**



e-business

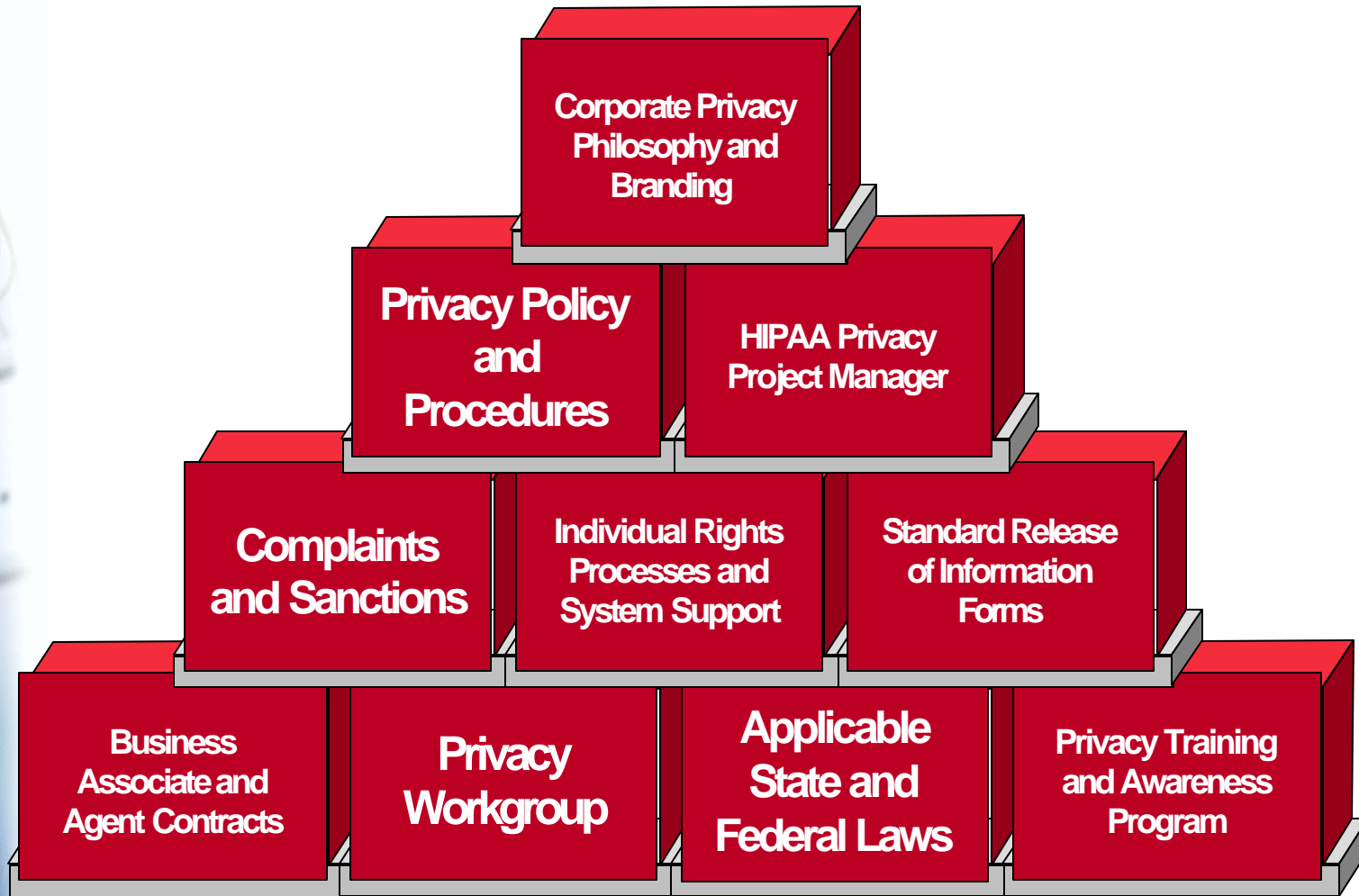
Steps to Meet BAC Requirements





e-business

Privacy Implemented at NASCO



What To Expect from CEs

- ❑ Surveys, periodic audits
- ❑ Requests for policies (yours and your subcontractors)
- ❑ Meet HIPAA regulations now!

Be proactive to get ahead of these requests

- Develop communication strategy
- Develop privacy manual, policies, statement
- Identify CEs, other business associates and agents
- Develop BAC strategy (negotiation, timetable, budget)



e-business



Thank You Questions?