Cách tiếp cận và thực hiện ISO 27001

LƯƠNG TRUNG THÀNH

Đơn vị tổ chức:

Đơn vị tài trợ:

Vì sao chọn ISO?

- Cung cấp các tiêu chí đánh giá rõ ràng, hầu hết đều đo lường được.
- Mang tính hệ thống và linh động, dễ ‘tương tác’ và kết hợp với các tiêu chuẩn khác.
- Mục tiêu gắn kết với hoạt động doanh nghiệp.

ISO 27001

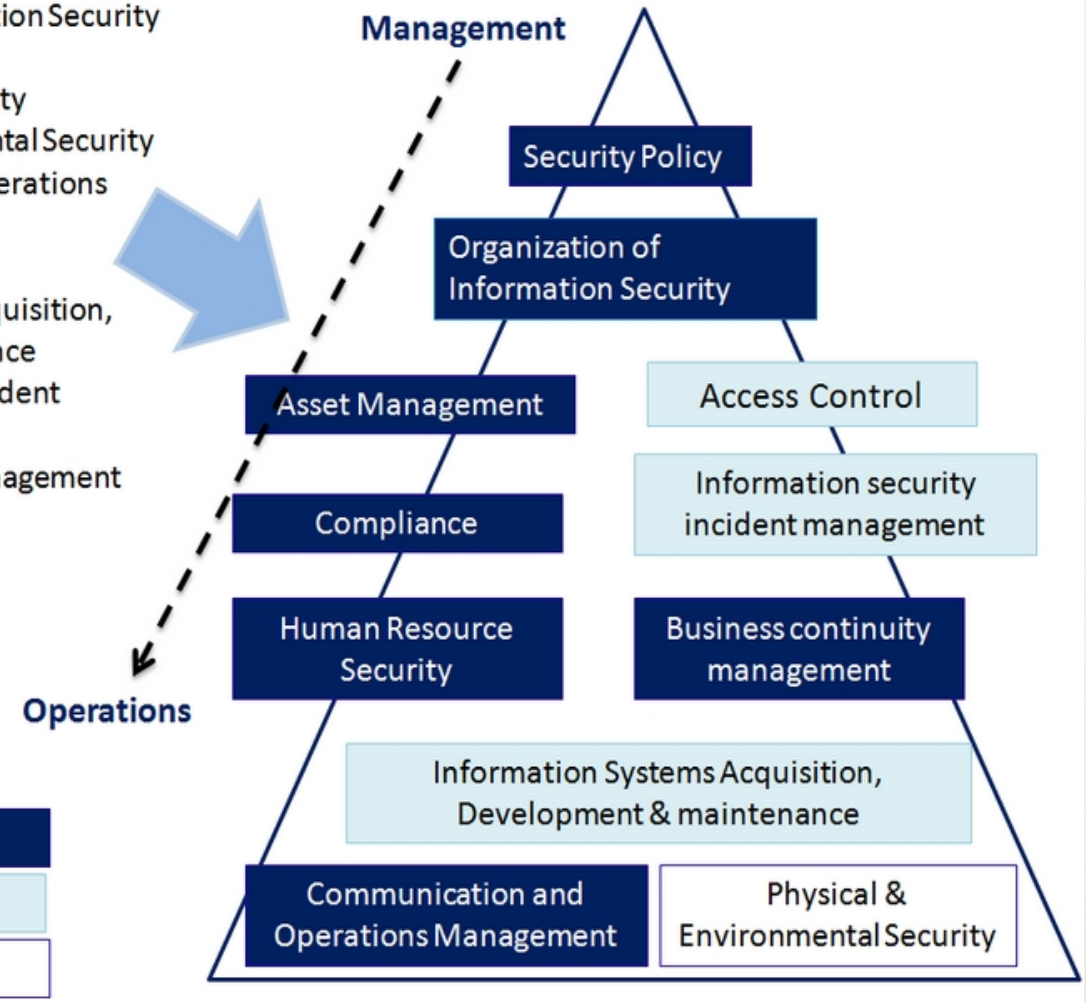
- Bao gồm các yêu cầu cần thiết để đạt được chứng nhận ISO 27001
- ISO 27001 là các yêu cầu cần thiết, tuy nhiên ISO 27002 mới cung cấp các cách thức cần thiết (làm thế nào để đạt được ISO 27001).

Conference & Training
Cần Thơ
SECURITY BOOTCAMP
2013
www.lactien.com

The 11 ISO/IEC 27001 Domains

- ❑ 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 & maintenance
- ❑ Information security incident management
- ❑ Business Continuity Management
- ❑ Compliance

Organizational Structure



Legend:

- Management Aspect
- Technical Aspect
- Physical Aspect

ISO 27001

- Mục tiêu của ISO 27001 đó là:
  - Giảm thiểu những tác động không mong muốn từ các rủi ro.
  - Vấn đề tiếp tục hoạt động kinh doanh của doanh nghiệp.
  - Nâng cao nhận thức về giá trị thông tin
- ***Không*** đảm bảo an toàn tuyệt đối trước các đợt tấn công; chỉ giảm thiểu tối đa rủi ro do các tác động.

Cách tiếp cận

- Dựa trên RISK ASSESSMENT và đánh giá những tác động lên hoạt động doanh nghiệp.
- Tham khảo Annex A (ISO 27001) và ISO 27002 để chọn lựa các Controls phù hợp.
- Hm..hm.. *Technical details*

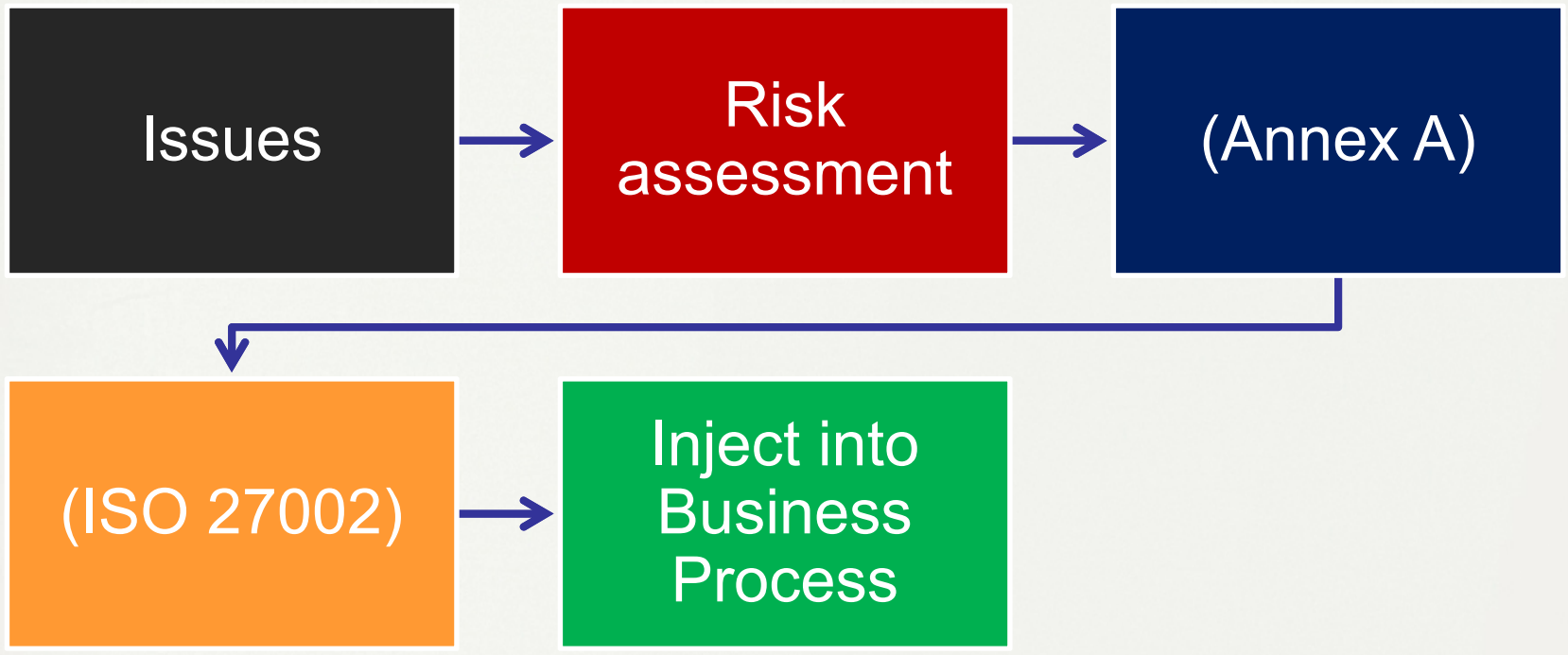
Ví dụ:

- VÍ DỤ
  - Risk Assessment
  - Annex A
  - ISO 27002 – Choose controls
  - …

Cách tiếp cận

- Xác định những gì đang có.
- Sử dụng Annex A – tập trung vào khu vực rủi ro cao.
- Sử dụng ISO 27002 để chọn Controls *phù hợp với hoạt động kinh doanh.*
- Chia thành nhiều giai đoạn nhỏ.
- ** Controls: bao gồm cả chính sách và kỹ thuật.*

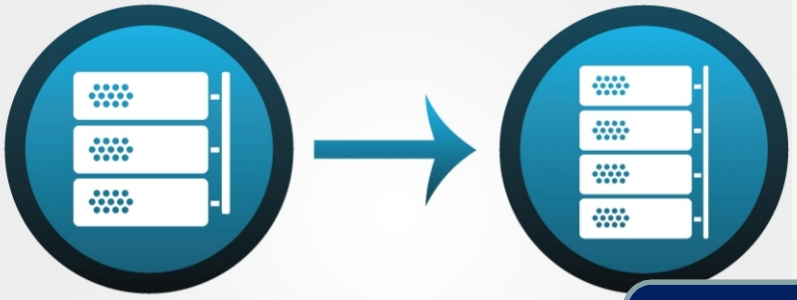

Conference &Training
Cần Thơ
SECURITY BOOTCAMP
2013
www.lactien.com


Issues
Risk assessment
(Annex A)
(ISO 27002)
Inject into Business Process

Fail & tại sao ?

- Không có sự hỗ trợ và quyết tâm.
- Sự khác biệt
- Làm đối phó / đi quá nhanh
- Chưa phù hợp với doanh nghiệp
- Mất tính ‘cạnh tranh’

<> .... <> ...

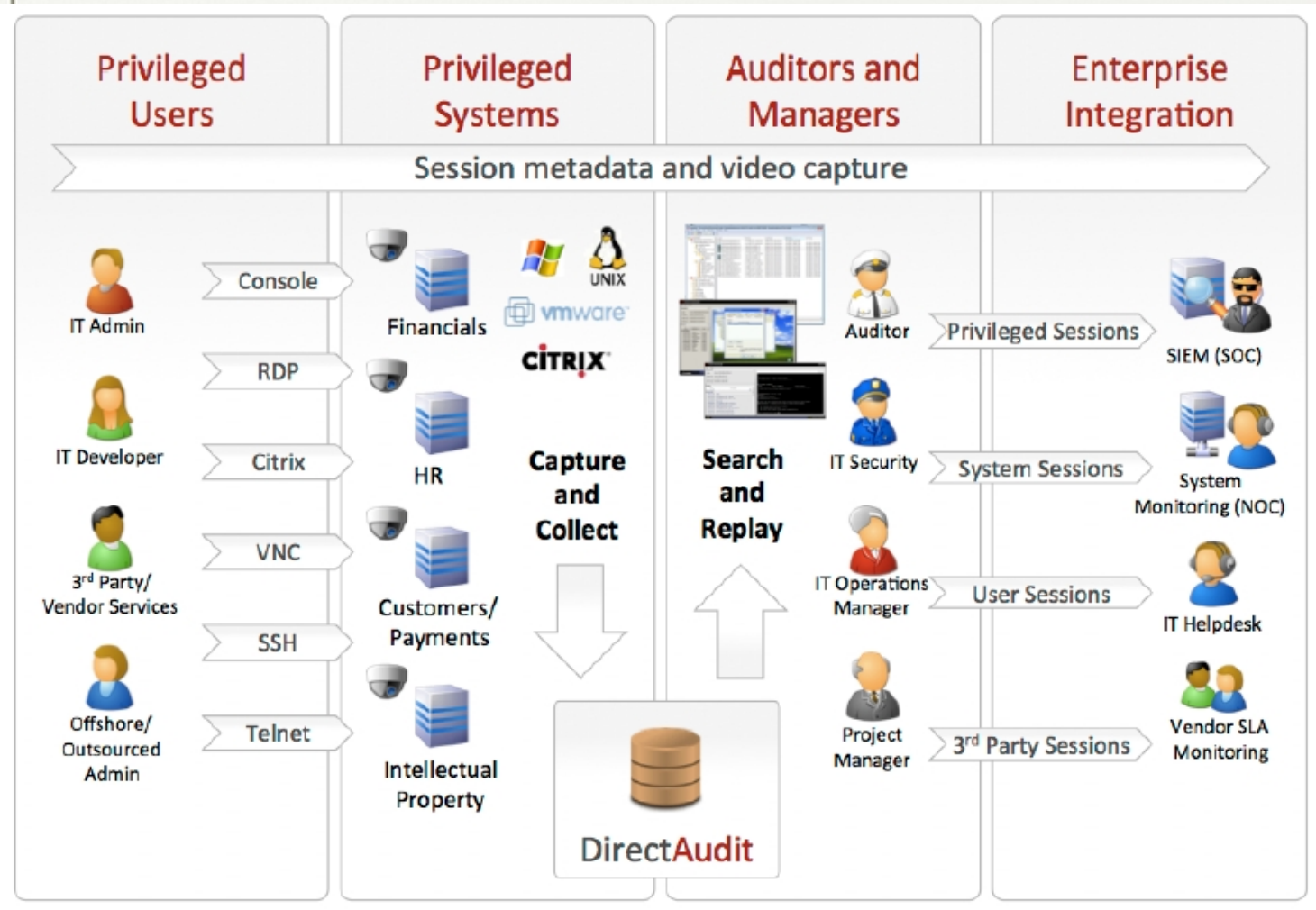


SERVER UPGRA

NOT ALIGNMENT

DOANH NGHIỆP CẦN

BẠN MUỐN?


Privileged Users
Privileged Systems
Auditors and Managers
Enterprise Integration
Session metadata and video capture
IT Admin
IT Developer
3rd Party/ Vendor Services
Offshore/ Outsourced Admin
Console
RDP
Citrix
VNC
SSH
Telnet
Financials
HR
Customers/ Payments
Intellectual Property
UNIX
vmware
CITRIX
Capture and Collect
DirectAudit
Search and Replay
Auditor
IT Security
IT Operations Manager
Project Manager
Privileged Sessions
System Sessions
User Sessions
3rd Party Sessions
SIEM (SOC)
System Monitoring (NOC)
IT Helpdesk
Vendor SLA Monitoring

Hạn chế

- Cần phải cập nhật những thay đổi công nghệ và chọn lựa controls phù hợp.
- Thay đổi môi trường hoạt động / kinh doanh.
- Thay đổi của luật và các Compliance.
- Chi phí cho việc Audit và kiểm

Hạn chế

- Duy trì & giám sát các hoạt động ở các chi nhánh
- Chi phí đầu tư cho thiết bị, con người, và quy trình.
- Tầm nhìn của người quyết định.
- Thay đổi nhân sự cấp cao

NHỮNG LƯU Ý

- Phải được sự hỗ trợ của BGĐ
- Xuất phát từ chính sách + sự hỗ trợ từ BGĐ
- Mở rộng từ từ, bắt đầu từ IT
- Tích hợp vào hoạt động của doanh nghiệp.

Q & A

- Cám ơn những góp ý/chia sẻ của:
  - Anh Bùi Thanh Phong – ISePro
  - Anh Nguyễn Hải Long – Đông Á Bank
  - Anh Trần Chí Cần – Lạc Tiên JSC
  - ….