Опыт внедрения системы управления информационной безопасностью в ESAB Россия

Aleksey Kvasnikov
IS services manager,
Russia & CIS

ESAB – это:

- ✔ Высококачественные расходные материалы для сварки и резки металлов
- ✔ Оборудование для сварки и резки металлов
- ✔ Годовой доход в 2009 – 1031,4 млн. фунтов
- ✔ Число сотрудников - 8581

На момент начала проекта:

- Процессная модель работы не была формализована
- Многие процессы существовали на уровне “repeatable”

Требования аудита:

- Система управления информационной безопасностью должна быть “эквивалентна ISO27001”
- Должна быть определена процессная модель работы отдела IT.

Стандарт ISO / IEC 27001:2005

- Определяет общую модель системы управления информационной безопасности (ISMS)
- Основывается на цикле Plan – Do - Check – Act
- Определяет цели управления и средства управления (control objectives & controls)

Risk = Impact x Probability

Управление риском:

- Уменьшение риска
- Принятие риска
- Избежание риска
- Передача риска третьей стороне

Дополнительные документы:

- ISO17799 – практические правила и средства управления информационной безопасностью
- ISO20000 – стандарт, описывающий систему управления IT сервисами
- ITIL – “хорошие” практики разработки процессов и системы управления IT сервисами
- COBIT – цели процессов, контроли, метрики

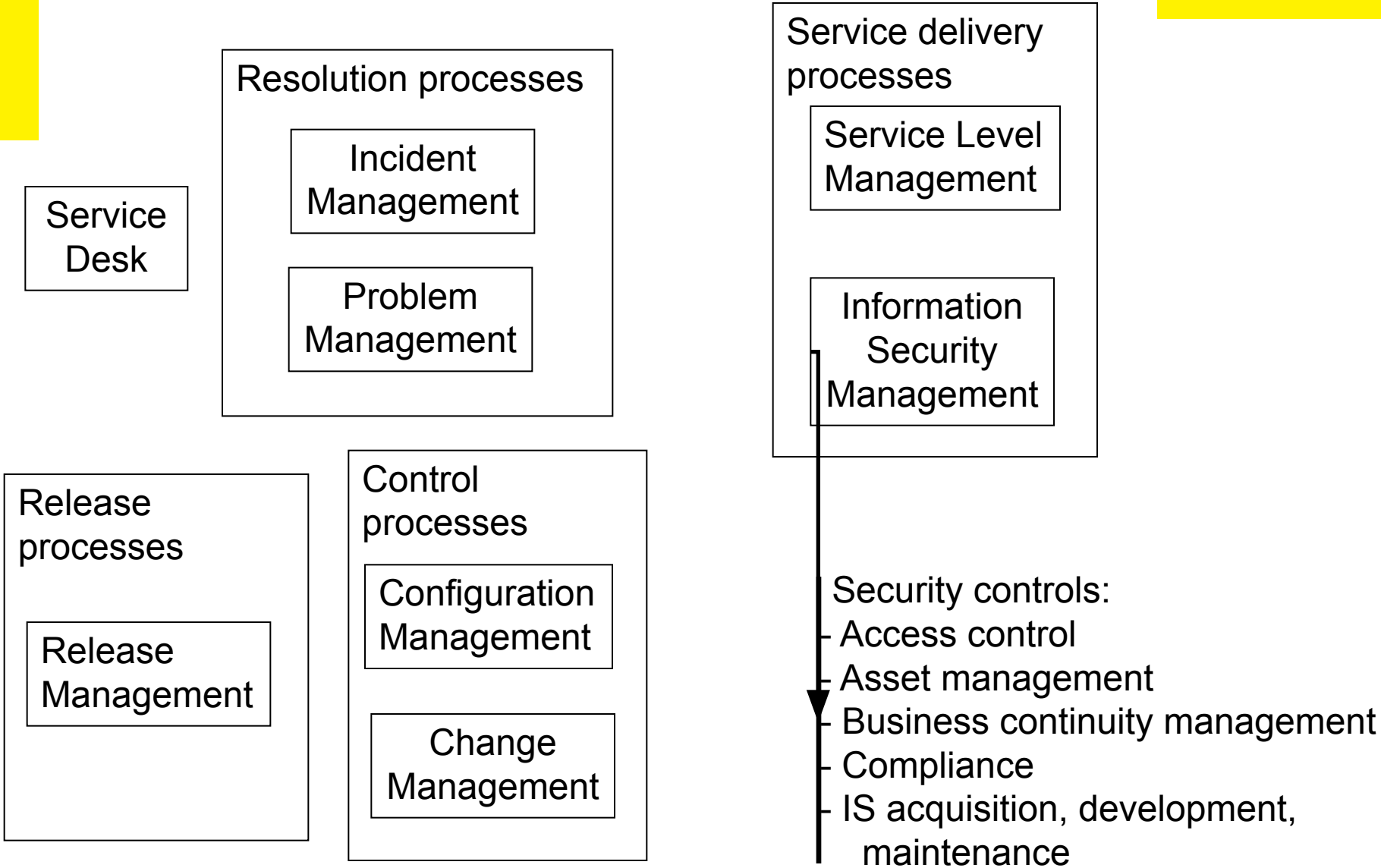
Внутренние документы, описывающие требования HQ:

- Раздел “IT Security” документа ”GLOBAL FINANCIAL PROCESS & CONTROL FRAMEWORK”
- Чек-лист, Internal Control Questionnaire
- Чек-лист Global Information risk assessment

Список приоритетных для HQ контролей ИБ

- Access control: процедуры создания / удаления пользователей, процедуры предоставления доступа к информационным системам
- IT disaster recovery plan
- Процедуры резервного копирования
- Должен быть разработан список информационных систем компании, бизнес - владельцев этих систем, классификация систем по CIA
- Учетные записи пользователей должны быть индивидуальными
- IT персонал должен использовать отдельные учетные записи для администрирования систем и для обычной работы в системах
- Наличие антивирусной программы на серверах и рабочих местах
- Наличие межсетевого экрана

Реализованная процессная модель



Спасибо за внимание!

Алексей Квасников