Cost-efficient Implementation of Security Controls

ISACA and AEA - Annual General Meeting and Professional Development Days

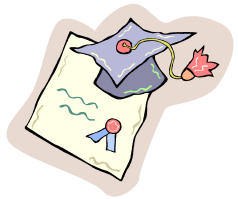
June 2019

Arnaud.Boutoille@FlexEDGE.com

(R)evolution of Cyber Security Risk Management

- Gigantic step – Revolution
- Significant needs for re-training
- Gaps in roles and responsibilities
- Outdated departmental policy instruments
- Added challenge of deficit reduction action plans

PGS, DDSM, ITSG-33



I passed C&A !!!

Continuous monitoring & alerting

The scope of security control catalogues

- 1 FAMILY: ACCESS CONTROL
- 2 FAMILY: AWARENESS AND TRAINING
- 3 FAMILY: AUDIT AND ACCOUNTABILITY
- 4 FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION
- 5 FAMILY: CONFIGURATION MANAGEMENT
- 6 FAMILY: CONTINGENCY PLANNING (CONTINUITY PLANNING)
- 7 FAMILY: IDENTIFICATION AND AUTHENTICATION
- 8 FAMILY: INCIDENT RESPONSE
- 9 FAMILY: MAINTENANCE
- 10 FAMILY: MEDIA PROTECTION
- 11 FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION
- 12 FAMILY: PLANNING
- 13 FAMILY: PERSONNEL SECURITY
- 14 FAMILY: RISK ASSESSMENT’
- 15 FAMILY: SYSTEM AND SERVICES ACQUISITION
- 16 FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION
- 17 FAMILY: SYSTEM AND INFORMATION INTEGRITY

Multiple control families

The scope of security control catalogues

- 1 FAMILY: ACCESS CONTROL
- 2 FAMILY: AWARENESS AND TRAINING
- 3 FAMILY: AUDIT AND ACCOUNTABILITY
- 4 FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION
- 5 FAMILY: CONFIGURATION MANAGEMENT
- 6 FAMILY: CONTINGENCY PLANNING (CONTINUITY PLANNING)
- 7 FAMILY: IDENTIFICATION AND AUTHENTICATION
- 8 FAMILY: INCIDENT RESPONSE
- 9 FAMILY: MAINTENANCE
- 10 FAMILY: MEDIA PROTECTION
- 11 FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION
- 12 FAMILY: PLANNING
- 13 FAMILY: PERSONNEL SECURITY
- 14 FAMILY: RISK ASSESSMENT'
- 15 FAMILY: SYSTEM AND SERVICES ACQUISITION
- 16 FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION
- 17 FAMILY: SYSTEM AND INFORMATION INTEGRITY

Multiple security controls per control family

- 1 FAMILY: ACCESS CONTROL
  - AC-1 ACCESS CONTROL POLICY AND PROCEDURES
  - AC-2 ACCOUNT MANAGEMENT
  - AC-3 ACCESS ENFORCEMENT
  - AC-4 INFORMATION FLOW ENFORCEMENT
  - AC-5 SEPARATION OF DUTIES
  - AC-6 LEAST PRIVILEGE
  - AC-7 UNSUCCESSFUL LOGIN ATTEMPTS
  - AC-8 SYSTEM USE NOTIFICATION
  - AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION
  - AC-10 CONCURRENT SESSION CONTROL
  - AC-11 SESSION LOCK
  - AC-12 SESSION TERMINATION
  - AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL
  - AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
  - AC-15 AUTOMATED MARKING
  - AC-16 SECURITY ATTRIBUTES
  - AC-17 REMOTE ACCESS
  - AC-18 WIRELESS ACCESS
  - AC-19 ACCESS CONTROL FOR MOBILE DEVICES
  - AC-20 USE OF EXTERNAL INFORMATION SYSTEMS
  - AC-21 USER-BASED COLLABORATION AND INFORMATION SHARING
  - AC-22 PUBLICLY ACCESSIBLE CONTENT
  - AC-23 DATA MINING PROTECTION
  - AC-24 ACCESS CONTROL DECISIONS
  - AC-25 REFERENCE MONITOR

The scope of security control catalogues

- 1 FAMILY: ACCESS CONTROL
  - AC-1 ACCESS CONTROL POLICY AND PROCEDURES
  - AC-2 ACCOUNT MANAGEMENT
  - AC-3 ACCESS ENFORCEMENT
  - AC-4 INFORMATION FLOW ENFORCEMENT
  - AC-5 SEPARATION OF DUTIES
  - AC-6 LEAST PRIVILEGE
  - AC-7 UNSUCCESSFUL LOGIN ATTEMPTS
  - AC-8 SYSTEM USE NOTIFICATION
  - AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION
  - AC-10 CONCURRENT SESSION CONTROL
  - AC-11 SESSION LOCK
  - AC-12 SESSION TERMINATION
  - AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL
  - AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
  - AC-15 AUTOMATED MARKING
  - AC-16 SECURITY ATTRIBUTES
  - AC-17 REMOTE ACCESS
  - AC-18 WIRELESS ACCESS
  - AC-19 ACCESS CONTROL FOR MOBILE DEVICES
  - AC-20 USE OF EXTERNAL INFORMATION SYSTEMS
  - AC-21 USER-BASED COLLABORATION AND INFORMATION SHARING
  - AC-22 PUBLICLY ACCESSIBLE CONTENT
  - AC-23 DATA MINING PROTECTION
  - AC-24 ACCESS CONTROL DECISIONS
  - AC-25 REFERENCE MONITOR

Multiple parts (A, B, C, etc.) per security control

- AC-2 ACCOUNT MANAGEMENT
- Control:
  - A - The organization identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types].
  - B - The organization assigns account managers for information system accounts.
  - C - The organization establishes conditions for group and role membership.
  - D- The organization specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
  - E - The organization requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts.
  - F - The organization creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions].
  - G - The organization monitors the use of information system accounts.
  - H - The organization notifies account managers:
    - When accounts are no longer required;
    - When users are terminated or transferred; and
    - When individual information system usage or need-to-know changes.
  - I - The organization authorizes access to the information system based on:
    - A valid access authorization;
    - Intended system usage; and
    - Other attributes as required by the organization or associated missions/business functions.
  - J - The organization reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].
  - K - The organization establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

The scope of security control catalogues

- 1 FAMILY: ACCESS CONTROL
  - AC-1 ACCESS CONTROL POLICY AND PROCEDURES
  - AC-2 ACCOUNT MANAGEMENT
  - AC-3 ACCESS ENFORCEMENT
  - AC-4 INFORMATION FLOW ENFORCEMENT
  - AC-5 SEPARATION OF DUTIES
  - AC-6 LEAST PRIVILEGE
  - AC-7 UNSUCCESSFUL LOGIN ATTEMPTS
  - AC-8 SYSTEM USE NOTIFICATION
  - AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION
  - AC-10 CONCURRENT SESSION CONTROL
  - AC-11 SESSION LOCK
  - AC-12 SESSION TERMINATION
  - AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL
  - AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
  - AC-15 AUTOMATED MARKING
  - AC-16 SECURITY ATTRIBUTES
  - AC-17 REMOTE ACCESS
  - AC-18 WIRELESS ACCESS
  - AC-19 ACCESS CONTROL FOR MOBILE DEVICES
  - AC-20 USE OF EXTERNAL INFORMATION SYSTEMS
  - AC-21 USER-BASED COLLABORATION AND INFORMATION SHARING
  - AC-22 PUBLICLY ACCESSIBLE CONTENT
  - AC-23 DATA MINING PROTECTION
  - AC-24 ACCESS CONTROL DECISIONS
  - AC-25 REFERENCE MONITOR

Supplemental guidance, links between security controls, etc.

- AC-2 ACCOUNT MANAGEMENT
- Supplemental Guidance:
  - Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or information technology security co-ordinator) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.

The scope of security control catalogues

- 1 FAMILY: ACCESS CONTROL
  - AC-1 ACCESS CONTROL POLICY AND PROCEDURES
  - AC-2 ACCOUNT MANAGEMENT
  - AC-3 ACCESS ENFORCEMENT
  - AC-4 INFORMATION FLOW ENFORCEMENT
  - AC-5 SEPARATION OF DUTIES
  - AC-6 LEAST PRIVILEGE
  - AC-7 UNSUCCESSFUL LOGIN ATTEMPTS
  - AC-8 SYSTEM USE NOTIFICATION
  - AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION
  - AC-10 CONCURRENT SESSION CONTROL
  - AC-11 SESSION LOCK
  - AC-12 SESSION TERMINATION
  - AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL
  - AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
  - AC-15 AUTOMATED MARKING
  - AC-16 SECURITY ATTRIBUTES
  - AC-17 REMOTE ACCESS
  - AC-18 WIRELESS ACCESS
  - AC-19 ACCESS CONTROL FOR MOBILE DEVICES
  - AC-20 USE OF EXTERNAL INFORMATION SYSTEMS
  - AC-21 USER-BASED COLLABORATION AND INFORMATION SHARING
  - AC-22 PUBLICLY ACCESSIBLE CONTENT
  - AC-23 DATA MINING PROTECTION
  - AC-24 ACCESS CONTROL DECISIONS
  - AC-25 REFERENCE MONITOR

And Control Enhancements

- AC-2 ACCOUNT MANAGEMENT
- Control Enhancements:
- ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT
  - The organization employs automated mechanisms to support the management of information system accounts.
- ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS
  - The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].
- ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS
  - The information system automatically disables inactive accounts after [Assignment: organization-defined time period].
- ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS
  - The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. Related controls: AU-2, AU-12.
- ACCOUNT MANAGEMENT | INACTIVITY LOGOUT
  - The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out]. Related controls: SC-23
- ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT
  - The information system implements the following dynamic privilege management capabilities: [Assignment: organization-defined list of dynamic privilege management capabilities].
- ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES
  - The organization establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
  - The organization monitors privileged role assignments; and
  - The organization takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate.
- ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION
  - The information system creates [Assignment: organization-defined information system accounts] dynamically.
- ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS
  - The organization only permits the use of shared/group accounts that meet [Assignment: organization-defined conditions for establishing shared/group accounts].
- ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION
  - The information system terminates shared/group account credentials when members leave the group.
- ACCOUNT MANAGEMENT | USAGE CONDITIONS
  - The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].
- ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE
  - The organization monitors information system accounts for [Assignment: organization-defined atypical use]; and
  - The organization reports atypical usage of information system accounts to [Assignment: organization-defined personnel or roles].
  - Enhancement Supplemental Guidance: Atypical usage includes, for example, accessing information systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations. Related controls: CA-7.
- ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS
  - The organization disables accounts of users posing a significant risk within [Assignment: organization-defined time period] of discovery of the risk.

The scope of security control catalogues

- 1 FAMILY: ACCESS CONTROL
  - AC-1 ACCESS CONTROL POLICY AND PROCEDURES
  - AC-2 ACCOUNT MANAGEMENT
  - AC-3 ACCESS ENFORCEMENT
  - AC-4 INFORMATION FLOW ENFORCEMENT
  - AC-5 SEPARATION OF DUTIES
  - AC-6 LEAST PRIVILEGE
  - AC-7 UNSUCCESSFUL LOGIN ATTEMPTS
  - AC-8 SYSTEM USE NOTIFICATION
  - AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION
  - AC-10 CONCURRENT SESSION CONTROL
  - AC-11 SESSION LOCK
  - AC-12 SESSION TERMINATION
  - AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL
  - AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
  - AC-15 AUTOMATED MARKING
  - AC-16 SECURITY ATTRIBUTES
  - AC-17 REMOTE ACCESS
  - AC-18 WIRELESS ACCESS
  - AC-19 ACCESS CONTROL FOR MOBILE DEVICES
  - AC-20 USE OF EXTERNAL INFORMATION SYSTEMS
  - AC-21 USER-BASED COLLABORATION AND INFORMATION SHARING
  - AC-22 PUBLICLY ACCESSIBLE CONTENT
  - AC-23 DATA MINING PROTECTION
  - AC-24 ACCESS CONTROL DECISIONS
  - AC-25 REFERENCE MONITOR

With supplemental guidance for control enhancements

- AC-2 ACCOUNT MANAGEMENT
- Control Enhancements:
- ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT
  - The information system implements the following dynamic privilege management capabilities: [Assignment: organization-defined list of dynamic privilege management capabilities].

  - Enhancement Supplemental Guidance:
  - In contrast to conventional access control approaches which employ static information system accounts and predefined sets of user privileges, dynamic access control approaches (e.g., service-oriented architectures) rely on run time access control decisions facilitated by dynamic privilege management. While user identities may remain relatively constant over time, user privileges may change more frequently based on ongoing mission/business requirements and operational needs of organizations. Dynamic privilege management can include, for example, the immediate revocation of privileges from users, as opposed to requiring that users terminate and restart their sessions to reflect any changes in privileges. Dynamic privilege management can also refer to mechanisms that change the privileges of users based on dynamic rules as opposed to editing specific user profiles. This type of privilege management includes, for example, automatic adjustments of privileges if users are operating outside of their normal work times, or if information systems are under duress or in emergency maintenance situations. This control enhancement also includes the ancillary effects of privilege changes, for example, the potential changes to encryption keys used for communications. Dynamic privilege management can support requirements for information system resiliency. Related controls: AC-16.

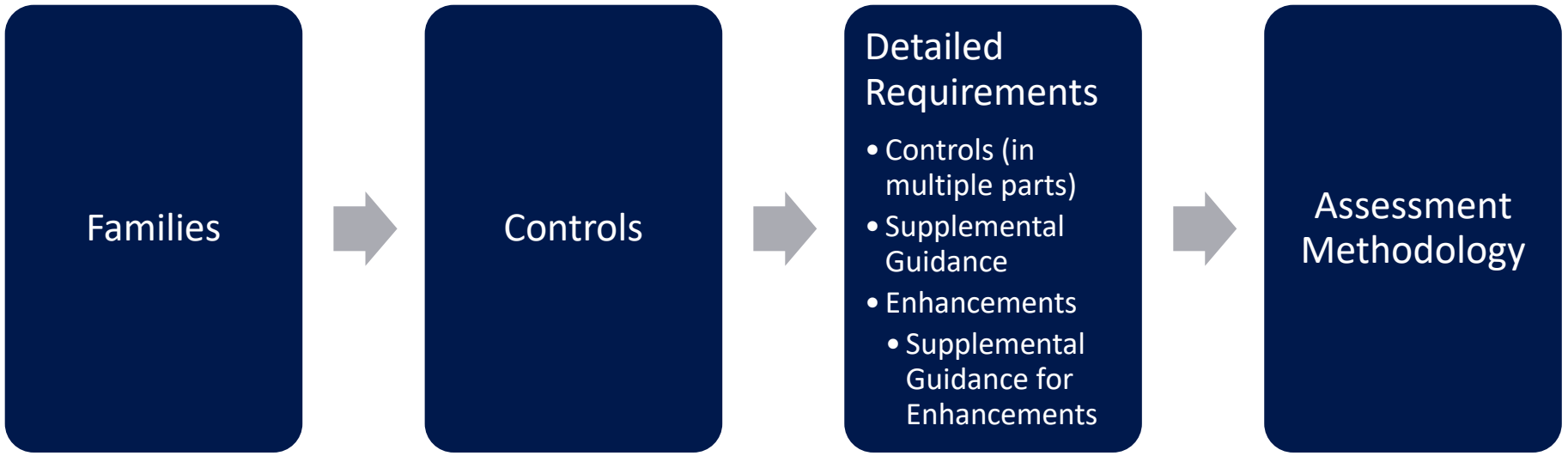
Security Controls Assessment

- POTENTIAL ASSESSMENT METHODS AND OBJECTS:
  - Examine: [SELECT FROM: Access control policy; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; list of active system accounts along with the name of the individual associated with each account; list of conditions for group and role membership; notifications or records of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; information system monitoring records; information system audit records; other relevant documents or records].
  - Interview: [SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities].
  - Test: [SELECT FROM: Organizational processes account management on the information system; automated mechanisms for implementing account management].

And let's not forget assessment guidance for each control or control enhancement

In summary…

OVERALL STRUCTURE



Meet Bill…

Employee Version: Do you have experience saving the world?

Consultant Version: M3 – The Bidder should demonstrate, using project descriptions that the proposed resource has professional work experience saving the world.

Loogmoji courtesy of Loogart www.loogart.com

Bill is a world savior…

- Bill can document a security control in 15 minutes, without requiring any colleague's time, with a unique ability to find all the relevant information, all by himself.
- Bill works 7.5 hours a day, 220 days a year (that accounts for his training, sickness, holidays, etc.).

Bill is a world savior…

- Bill can document a security control in 15 minutes, without requiring any colleague's time, with a unique ability to find all the relevant information, all by himself.
- Bill works 7.5 hours a day, 220 days a year (that accounts for his training, sickness, holidays, etc.).
- That's 1,650 hours per year.

Bill is a world savior…

- Bill’s organization has 500 applications (give or take, but the list is almost complete…).

Bill is a world savior…

- Bill’s organization has 500 applications (give or take, but the list is almost complete…).
- That’s 500 applications x 650 security controls.

Bill is a world savior…

- Bill's organization has 500 applications (give or take, but the list is almost complete…).
- That's 500 applications x 650 security controls.
- Or maybe a subset based on the security controls profile… (but we're not counting Part A and Part B and Part C and the enhancements).

Bill is a world savior…

- Bill’s organization has 500 applications (give or take, but the list is almost complete…).
- That’s 500 applications x 650 security controls x 15 minutes per control.

Bill is a world savior…

- Bill’s organization has 500 applications (give or take, but the list is almost complete…).
- That’s 500 applications x 650 security controls x 15 minutes per control.
- And some will say Bill is not a realistic assumption. Not 15 minutes? 3 hours? 2 days?

Bill is a world savior…

- Bill’s organization has 500 applications (give or take, but the list is almost complete…).
- That’s 500 applications x 650 security controls x 15 minutes per control.
- That’s 48,750 hours of work.

Bill is a world savior…

- Bill’s organization has 500 applications (give or take, but the list is almost complete…).
- That’s 500 applications x 650 security controls x 15 minutes per control.
- That’s 48,750 hours of work.
- That’s 29.5 years of work for Bill our super hero.

Bill is a world savior…

- Bill's organization has 500 applications (give or take, but the list is almost complete…).
- That's 500 applications x 650 security controls x 15 minutes per control.
- That's 48,750 hours of work.
- Or that's 30 Bills to complete in a year.

Bill is a world savior…

- US Federal Government empty MS Word template for 650 controls is 350 pages long.
- For 500 apps that's 175,000 pages (before Bill starts writing)
- And there are minor and major changes, new applications, new threats that all require on-going assessments
- Our army of 30 Bills is not going anywhere for the next century…

Reality check…

- And even if there were enough budget,
- And even if Bill performed that efficiently,
- There are not enough Bills available in the marketplace, employees and consultants combined!!!

Reality check…

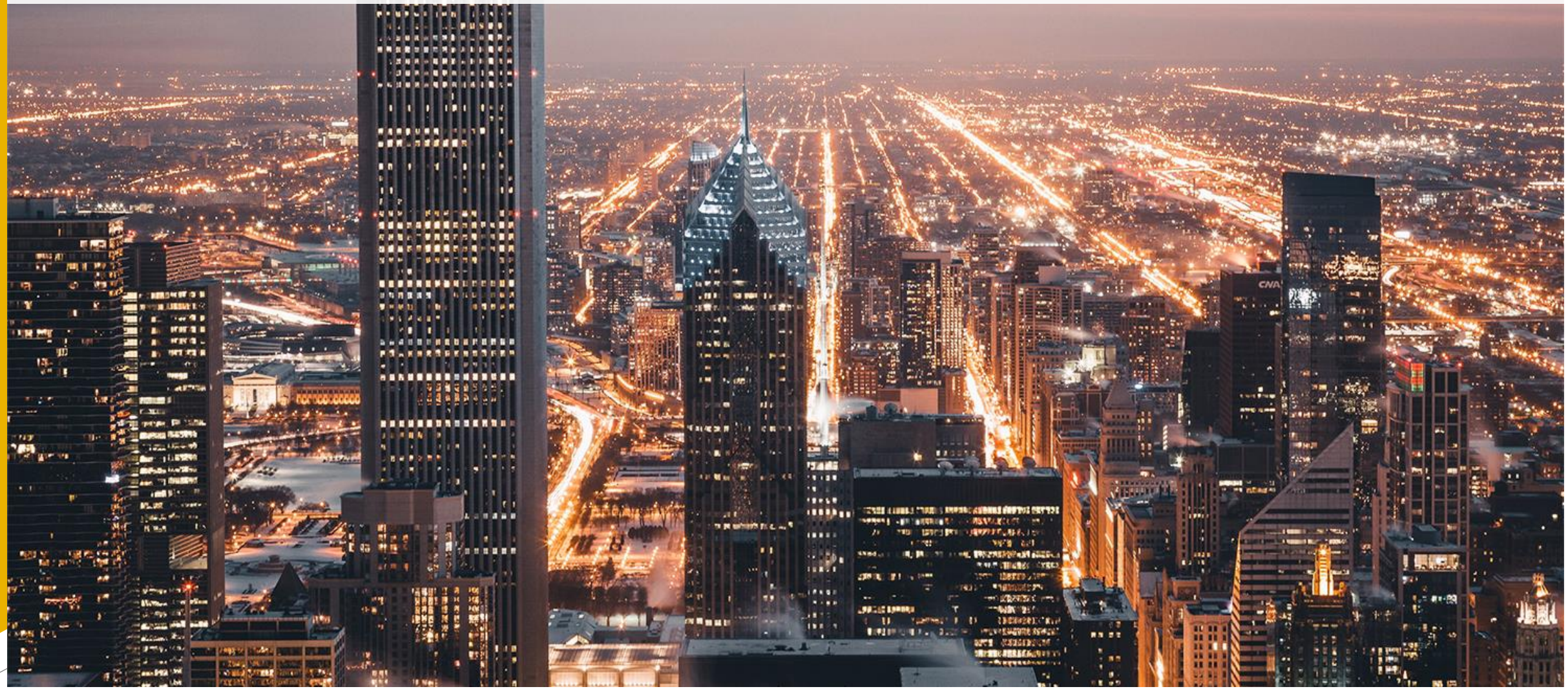
- And even if there were enough budget,
- And even if Bill performed that efficiently,
- There are not enough Bills available in the marketplace, employees and consultants combined!!!

Reality check…

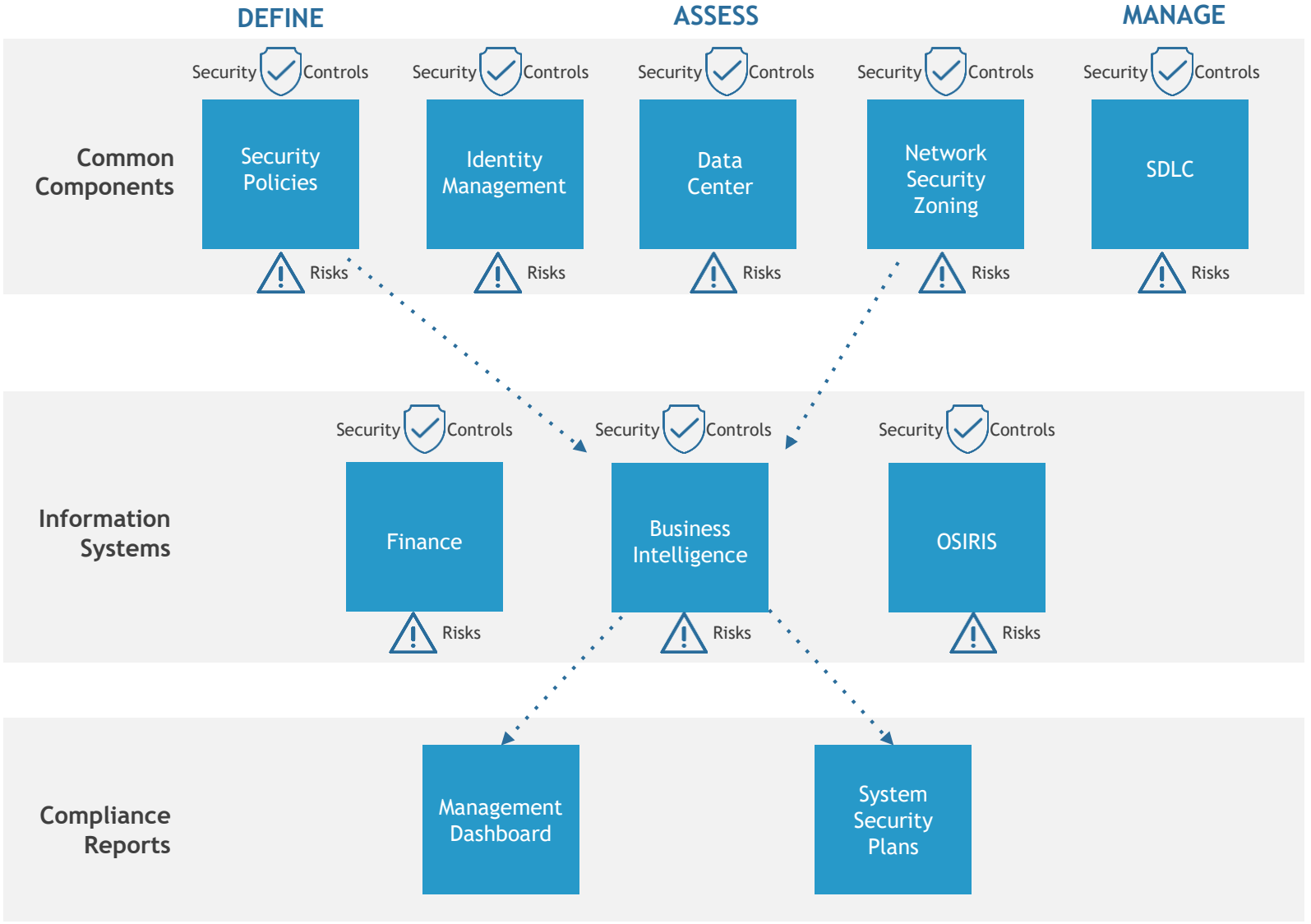
- And even if there were enough budget,
- And even if Bill performed that efficiently,
- There are not enough Bills available in the marketplace, employees and consultants combined!!!

So… Option 0? Do nothing???

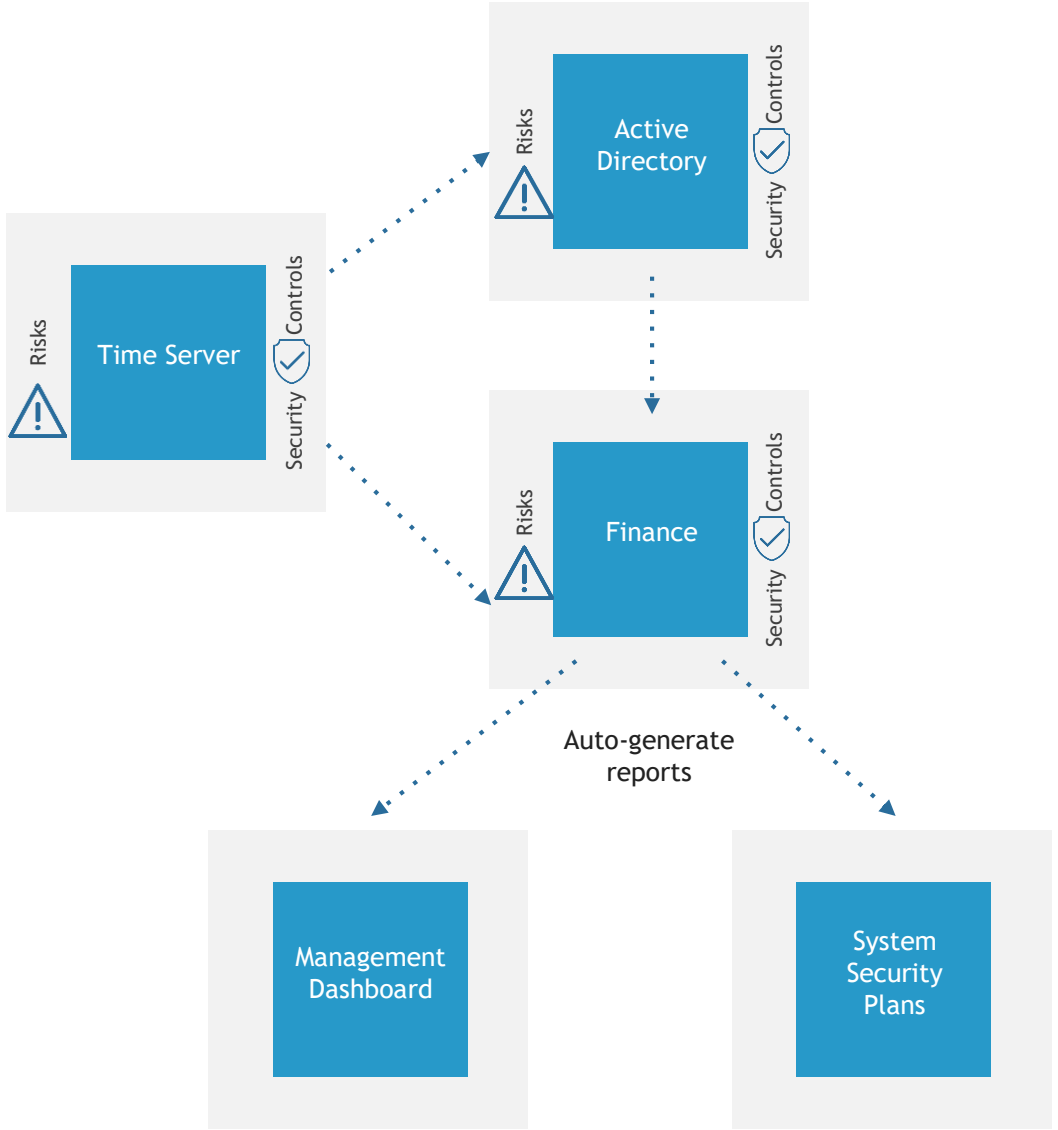
Or think outside the box…



Simplified View of Inheritance



Realistic View of Inheritance



Multiple levels of Information Systems

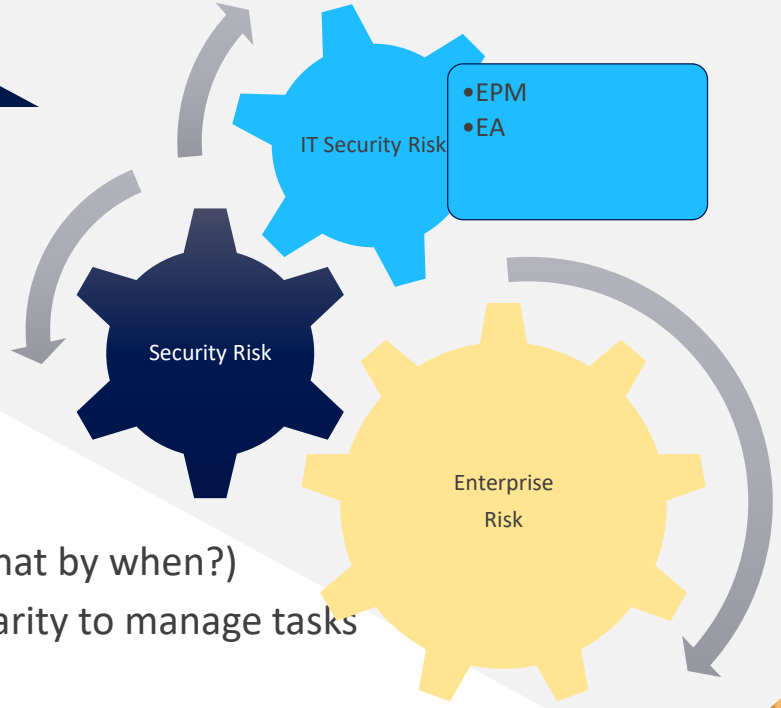
Inheritance is selective

Compliance reports assemble information -> 350 pages = 1 click

Implementation Overview

- People
  - Training
  - Staffing strategy (HR & Procurement Plans)
- Process
  - Phased implementation, starting for instance with simplified security control profiles and critical systems
- Technology
  - Adequate technology solutions for the organization (based on size and complexity)

Bigger Picture



- Complex ecosystem
  - Enterprise Project Management
    - Tracking Security Improvement Plans (who does what by when?)
    - Integration with an ePM solution could leverage clarity to manage tasks and formal projects
  - Enterprise Architecture
    - Common view of applications, common/shared components, interconnections, etc.
    - Leverage one repository instead of duplicating information
  - Enterprise Risk
    - Cyber Security Risk feeds into Security Risk (e.g. Departmental Security Plan) and Enterprise Risk

In Summary

- Practitioner focus
- Immediate tangible results
- Incremental progress
- Reasonable costs