



2007 11th CISSE
2007-06-05
Boston, Massachusetts, USA

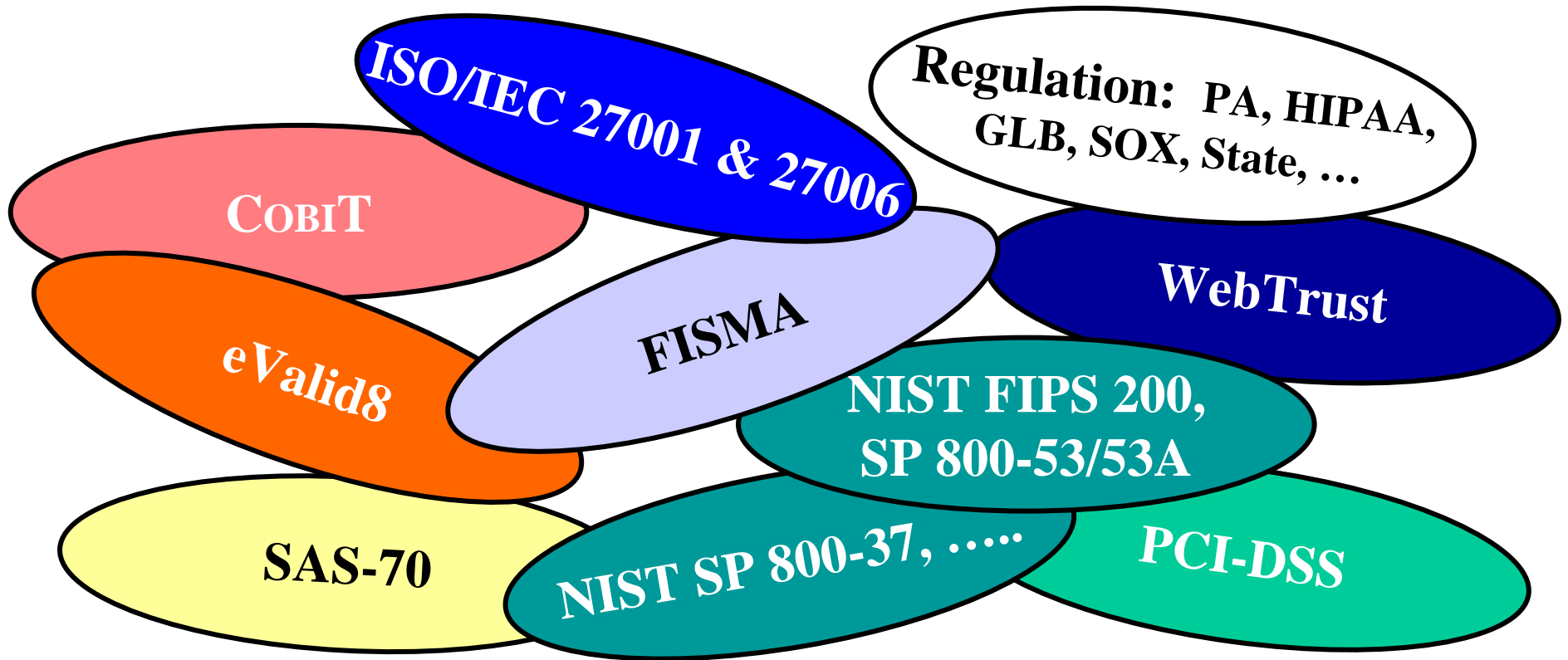
*Alignment of
Information Security Assessment
Best Practices*

Richard G. Wilsher & Matt King



what's the problem?

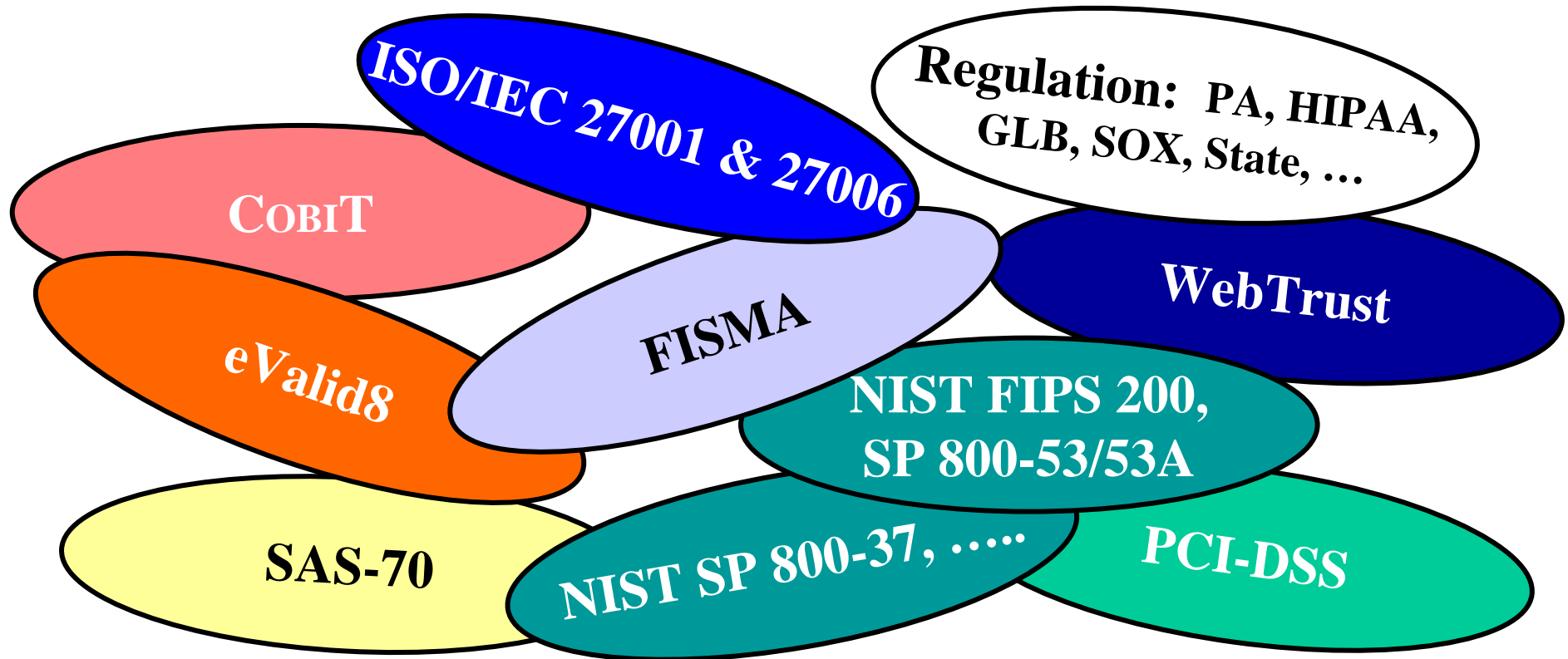
- A plethora of regulation, standards, processes, models for or requiring assessment / auditing





where's our focus?

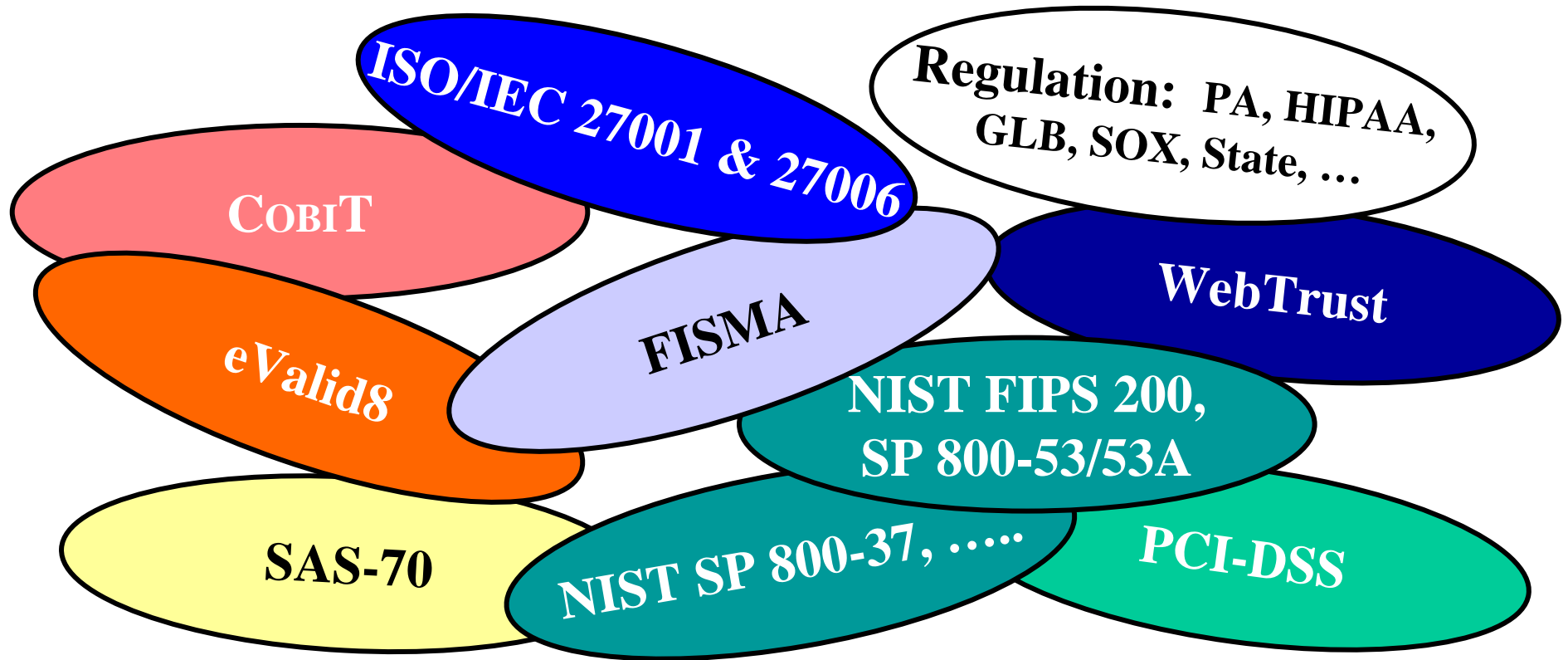
- many of these are complementary, addressing different 'space' or levels.
- need an holistic framework
- Federal government has a strong position





where's our focus?

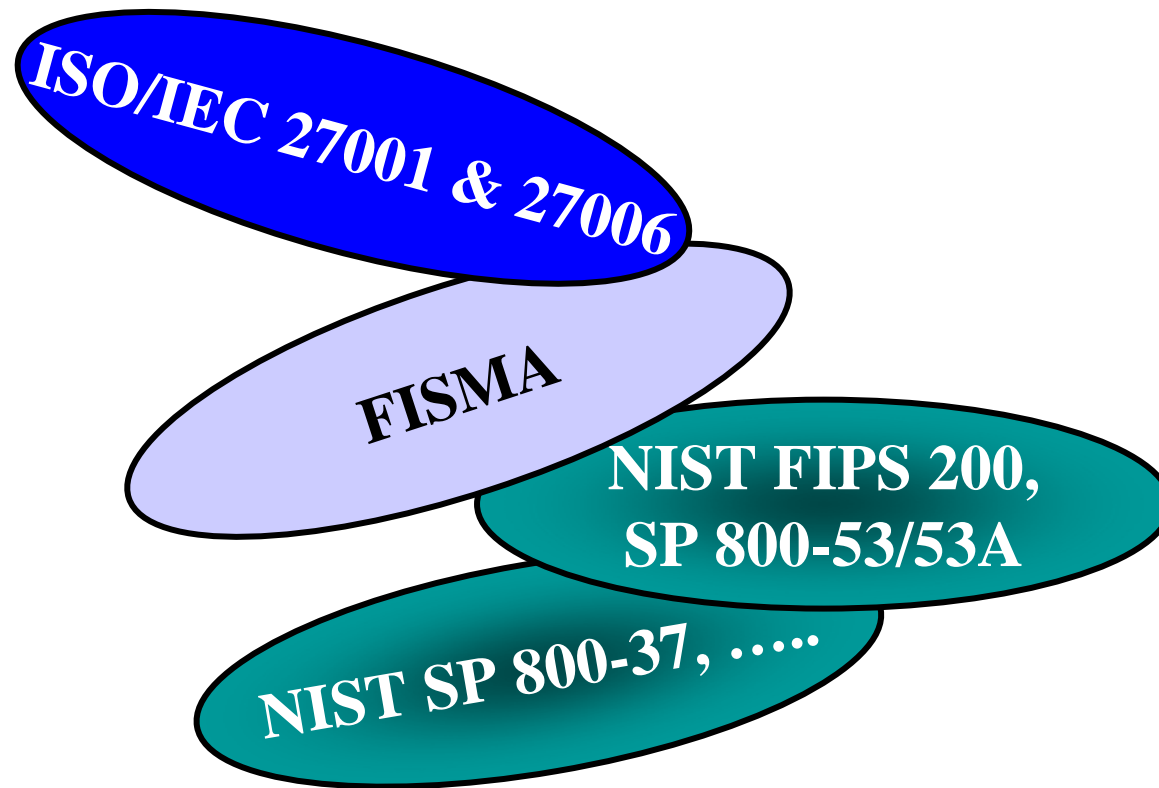
- there are two serious contenders
- this paper deals with their alignment and the drivers for that to happen





where's our focus?

- there are two serious contenders
- this paper deals with their alignment and the drivers for that to happen





what are the benefits?

- **FISMA has lower value/recognition in the commercial sector**
- **Even more so, concerning international recognition**
- **If FISMA requirements can be met, ISMS Certification carries wider recognition**
- **ISMS has a more workable approach to showing compliance with other regulations, standards, &c. (more open, flexible)**



what are the benefits?

- **reduction of management and technical complexity, economies in time and money**
- **combining will reduce the total workload where both FISMA and ISMS are required**
- **dual qualification of assessors not required**
 - **minimises set-up costs for new scheme**
 - **minimal/no additional training costs**
 - **lower cost per assessment**



broad scope

FISMA

- Federal law (2002), applicable to Federal departments' & agencies' systems and their suppliers/ contractors
 - mandatory compliance, mandatory 'C&A'
 - supported by various NIST publications which define requirements, controls, assessment
-

ISO/IEC 27001

- an international standard, generally-accepted best practice infosec management
- elective conformity, elective certification
- establishes the process requirements and controls, supported by various ISO publications which address implementation guidance, code of practice for applying controls, audit requirements



equivalencies

Regulation Requirements Guidance Certification/Audit

FISMA

↓
FISMA
OMB A-130

↓
FIPS 199
FIPS 200
SP 800-53
SP 800-XX

↓
SP 800-53A

↓
SP 800-37



ISO/IEC 27001

n/a

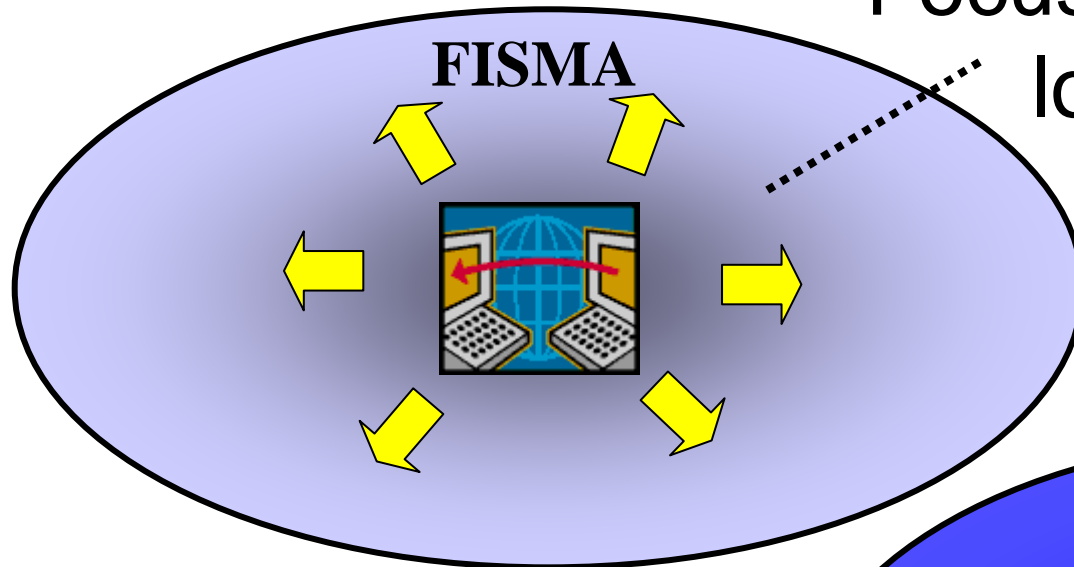
27001:2005 27002:2007
27003:2007?
270XX:200x?

27006:2007



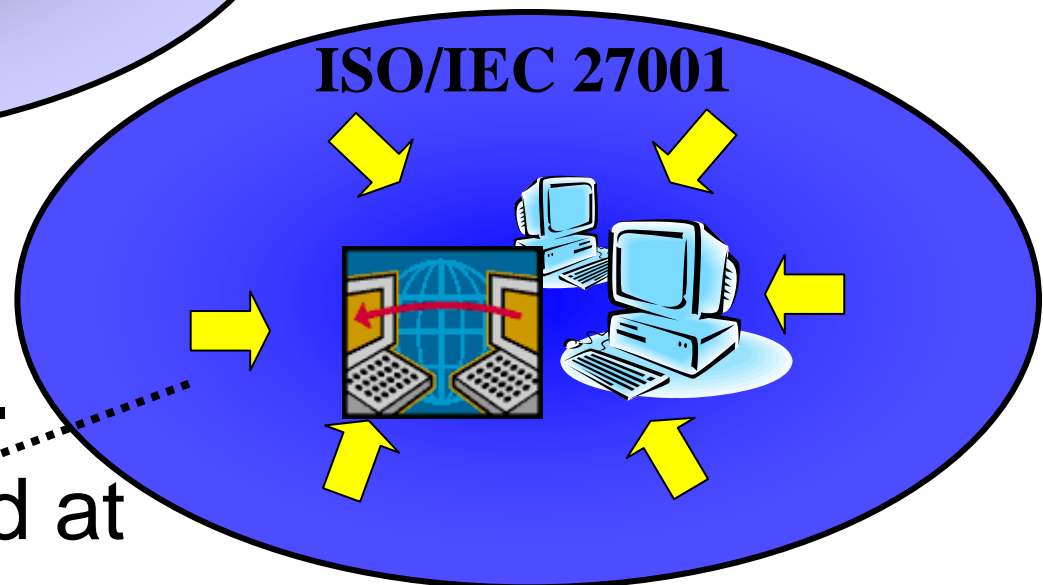
(non-equivalence!)

differences - foci



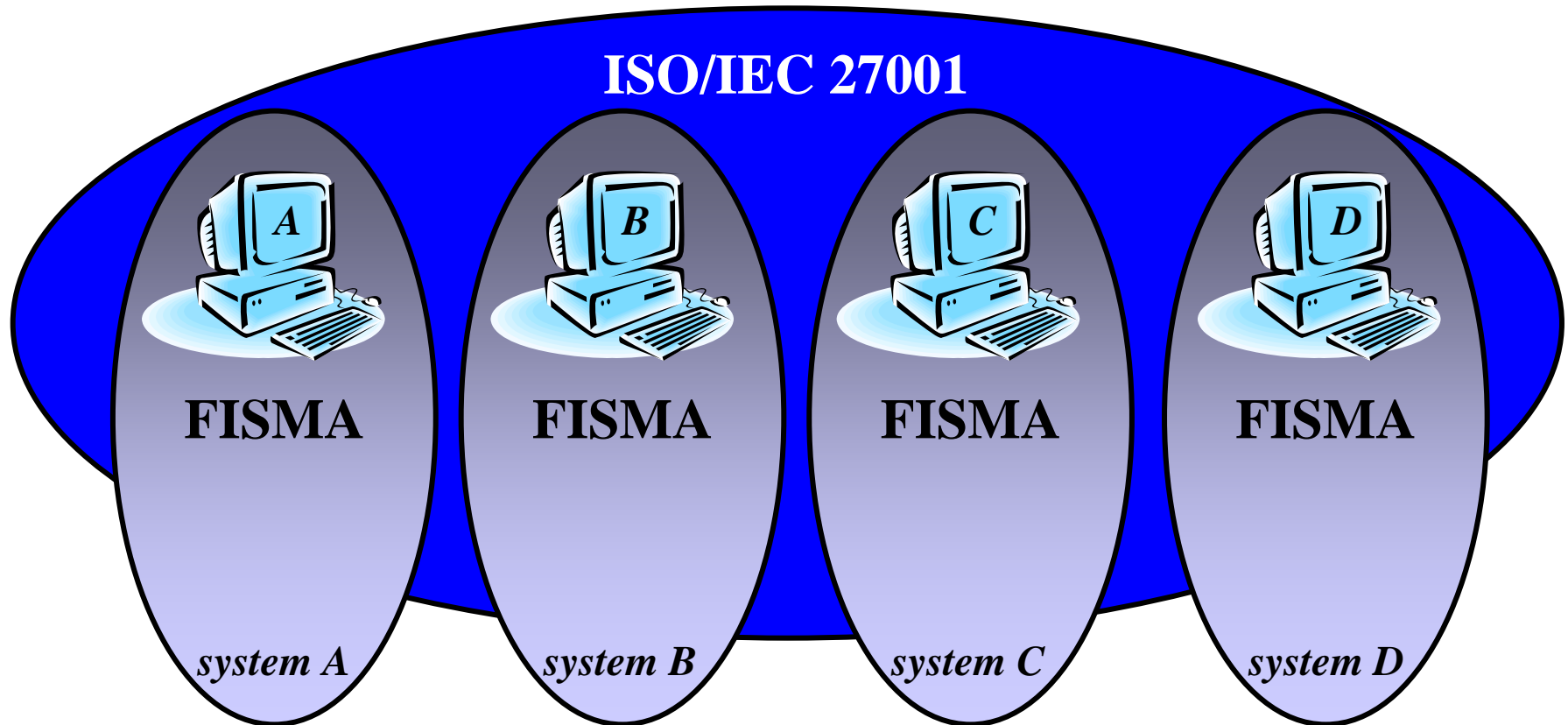
Focuses on a **system**, looks outward at its **management environment**

Focuses on the **security management**, looks inward at the **systems within scope**





differences - coverage





differences - process

FISMA

Categorize system, assess risks,
select and apply controls

**Independent assessment
& certification**

mandatory

Accept risk, issue ATO
(C&A process)

Operate system

Monitor system

ISO/IEC 27001

Categorize system, assess risks,
select and apply controls

Accept risk, issue ATO

Operate system

Independent assessment
& certification

optional

Monitor system



differences - process

FISMA

ISO/IEC 27001

Categorize system, assess risks,
select and apply controls

Categorize system, assess risks,
select and apply controls

*Designated
Assessor*

**Independent assessment
& certification**

Accept risk, issue ATO

*Accredited
Certification
Body*

Operate system

Accept risk, issue ATO
(C&A process)

**Independent assessment
& certification**

Operate system

Monitor system

Monitor system



key issues

- understand the relationship between the respective management/process requirements, and between the required controls
- determine which FISMA controls really are IT system-specific, which more management focused
- establish a process flow which resolves both paradigms
- address the inherent one-for-all (27001) vs. one-each (FISMA) approach
- accommodate FISMA only and ISMS only options (e.g. some steps driven by need)
- prove the alignment concept with a real system certification:
 - We have a volunteer: **the Federal PKI Operational Authority**

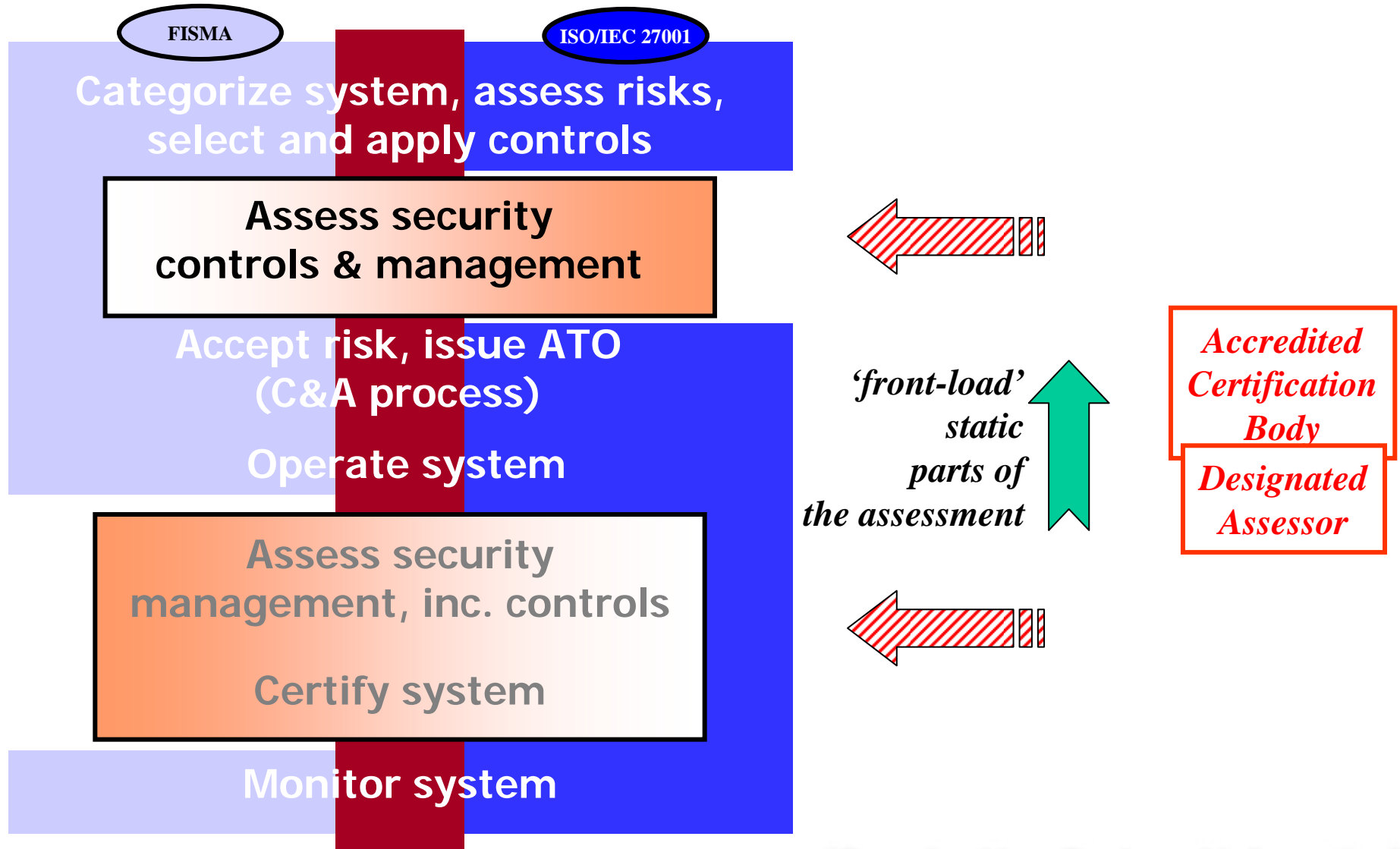


work to date

- white papers addressing the application of ISO/IEC 27001 to demonstrating conformance with other standards, regulation (Zygma)
 - HIPAA compliance
 - Generic model, concept of Extended Control Set
 - ISMS/FISMA alignment
- contribution to 27000-family, through ISO JTC1/SC27 (Zygma)
- mapping between FPKI FBCA Policy and SP 800-53 (Enspier)
- mapping between ISO/IEC 27001 and SP 800-53 (Zygma)
 - Likely outcome: SP 800-53 Addendum, 27001 mapping all in new Appendix
- FPKI-OA ISMS being developed (Zygma)

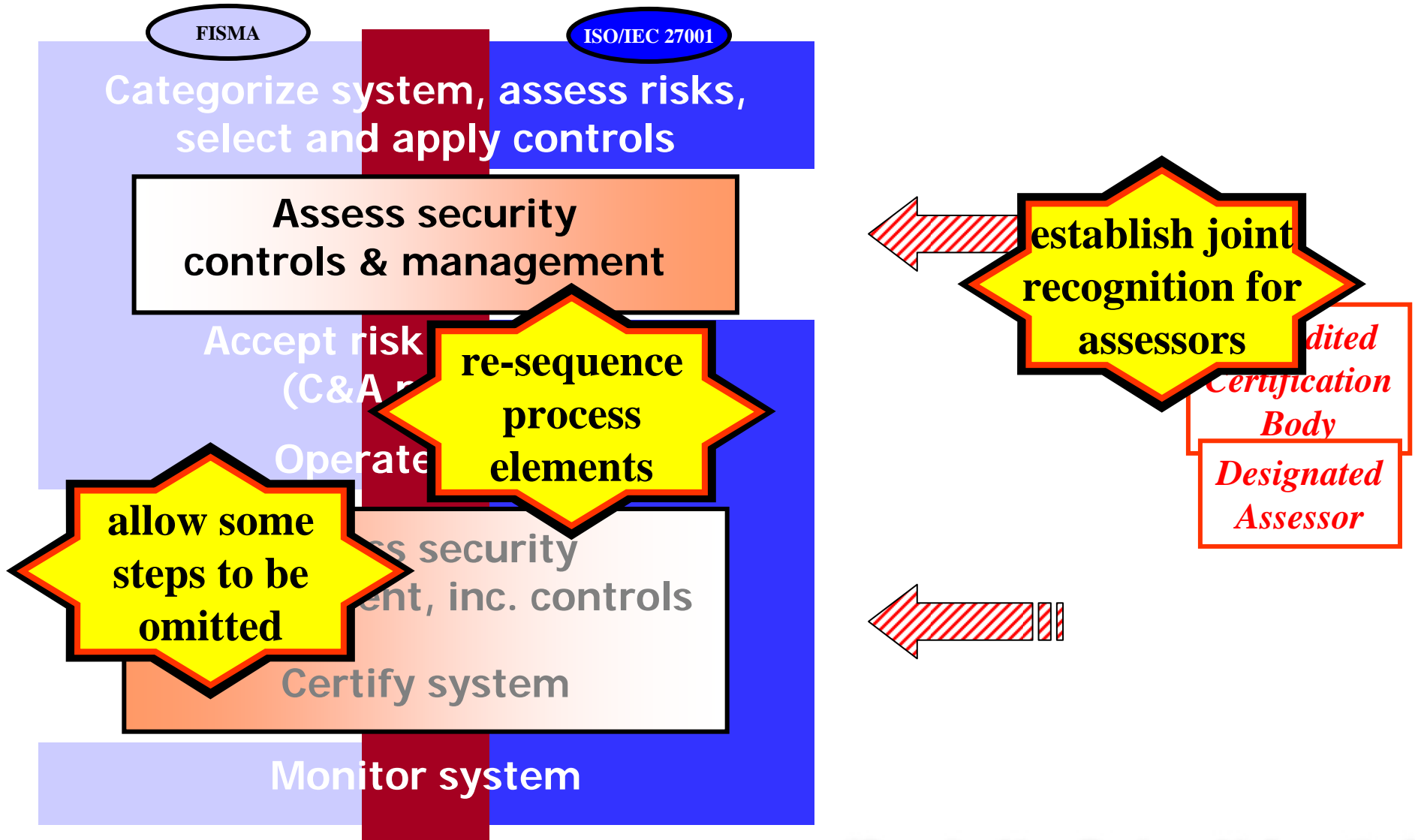


aligning processes



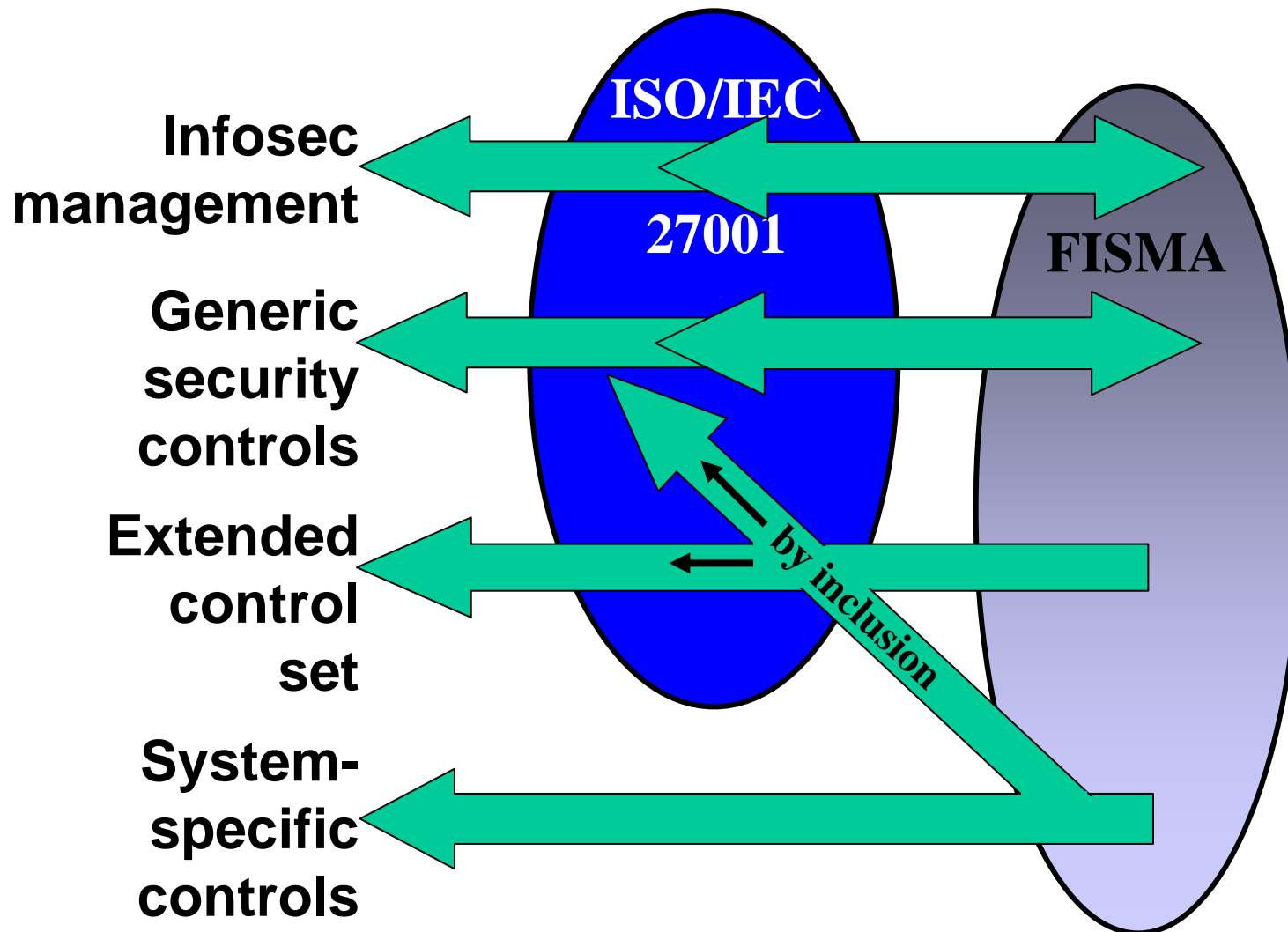


aligning processes



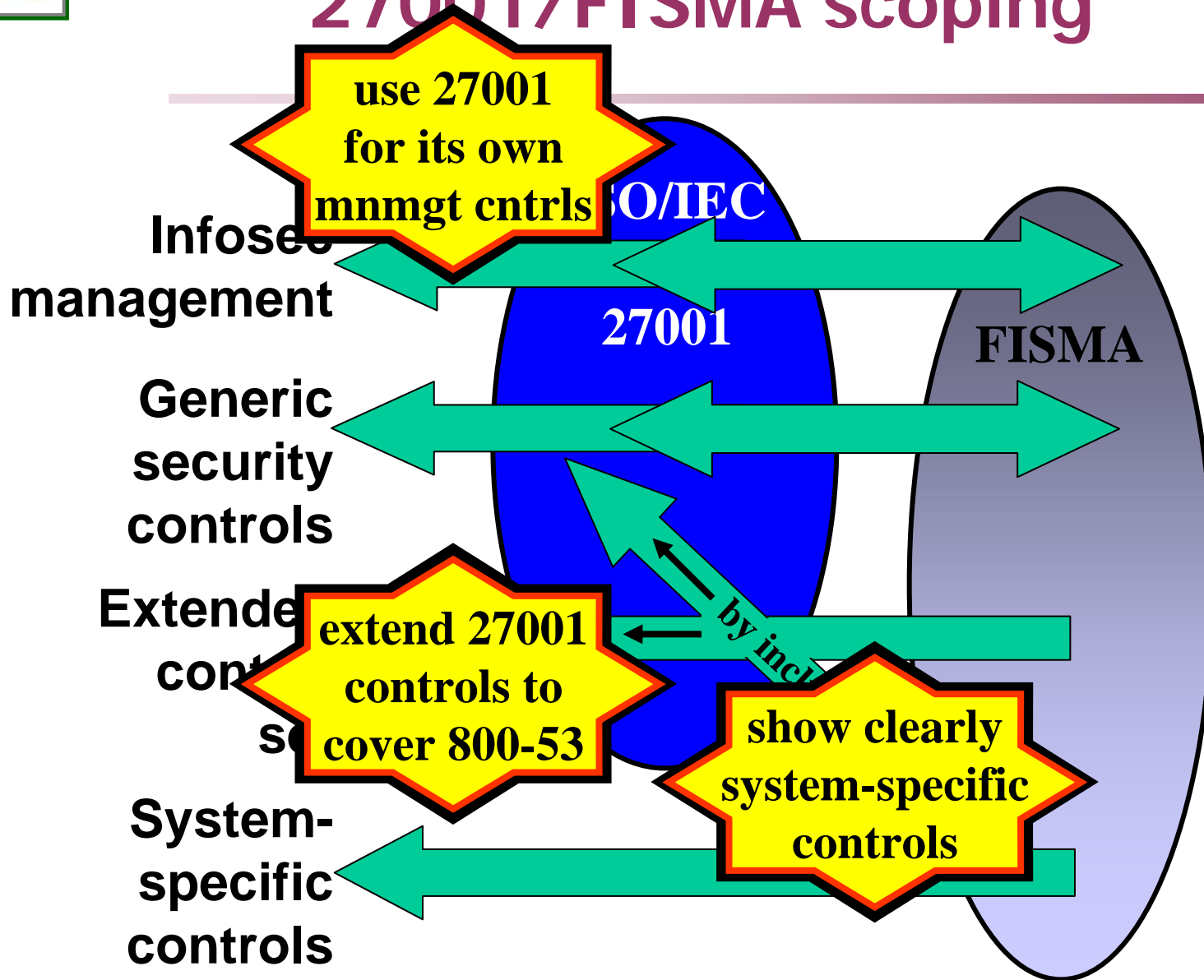


27001/FISMA scoping



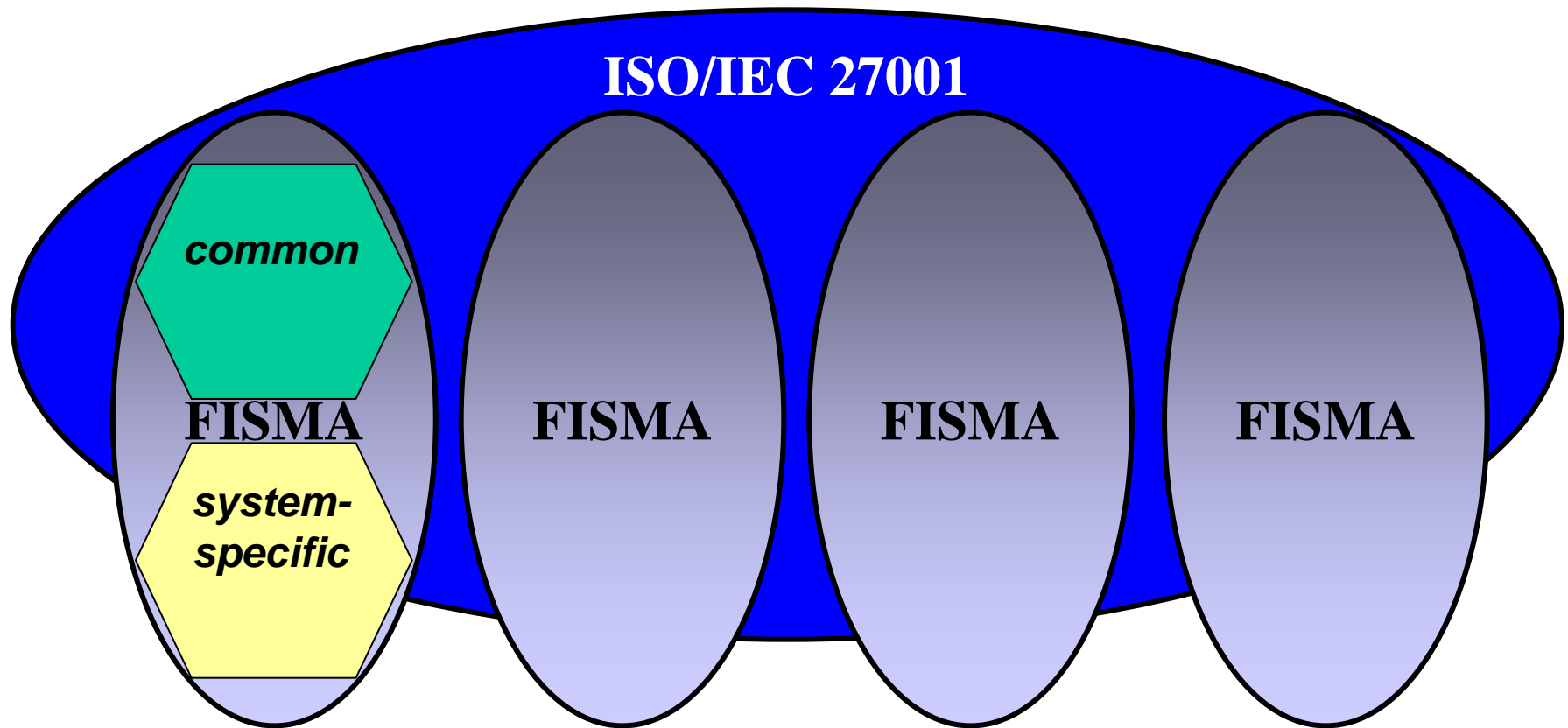


27001/FISMA scoping

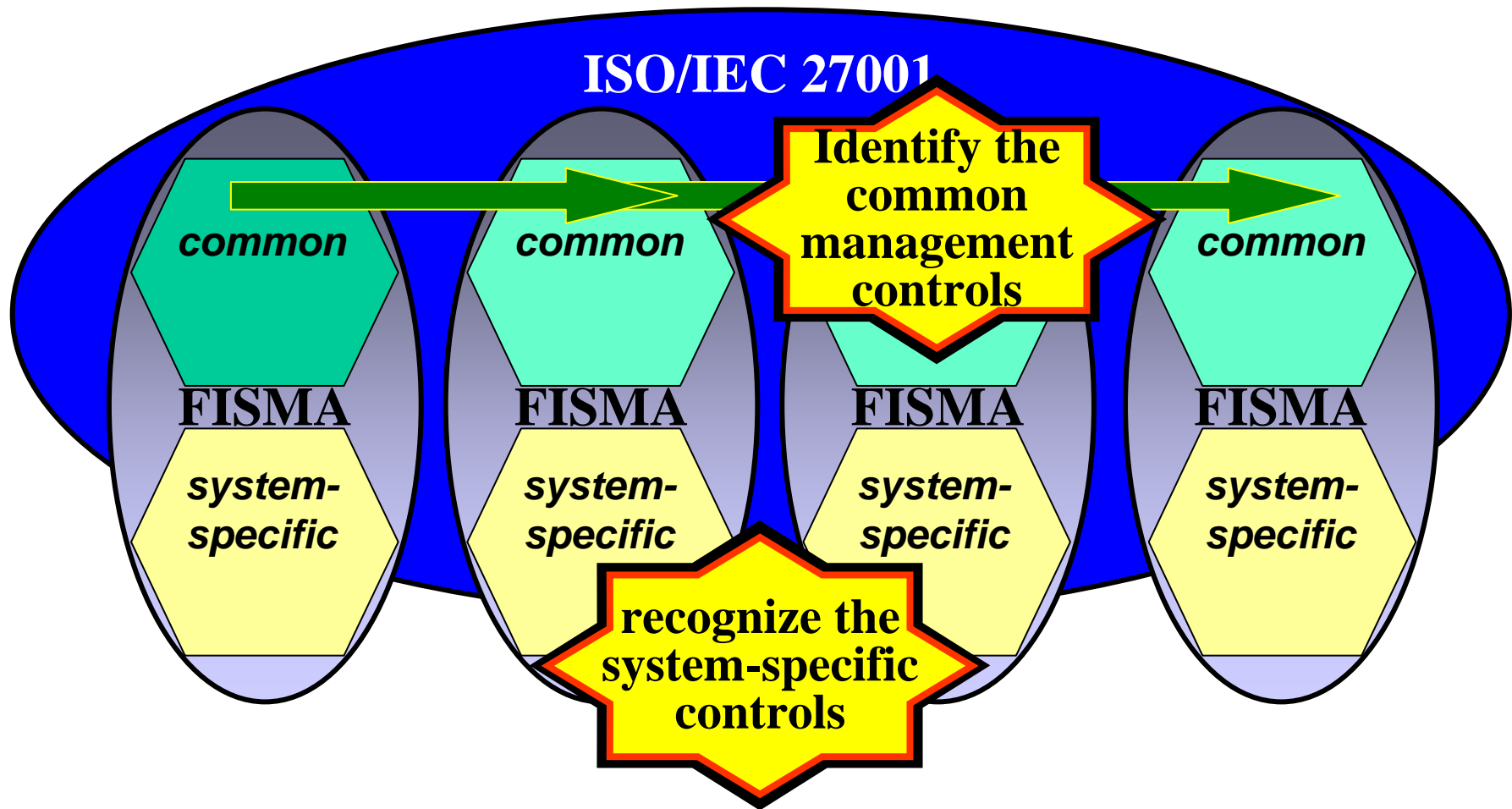




FISMA - resuability

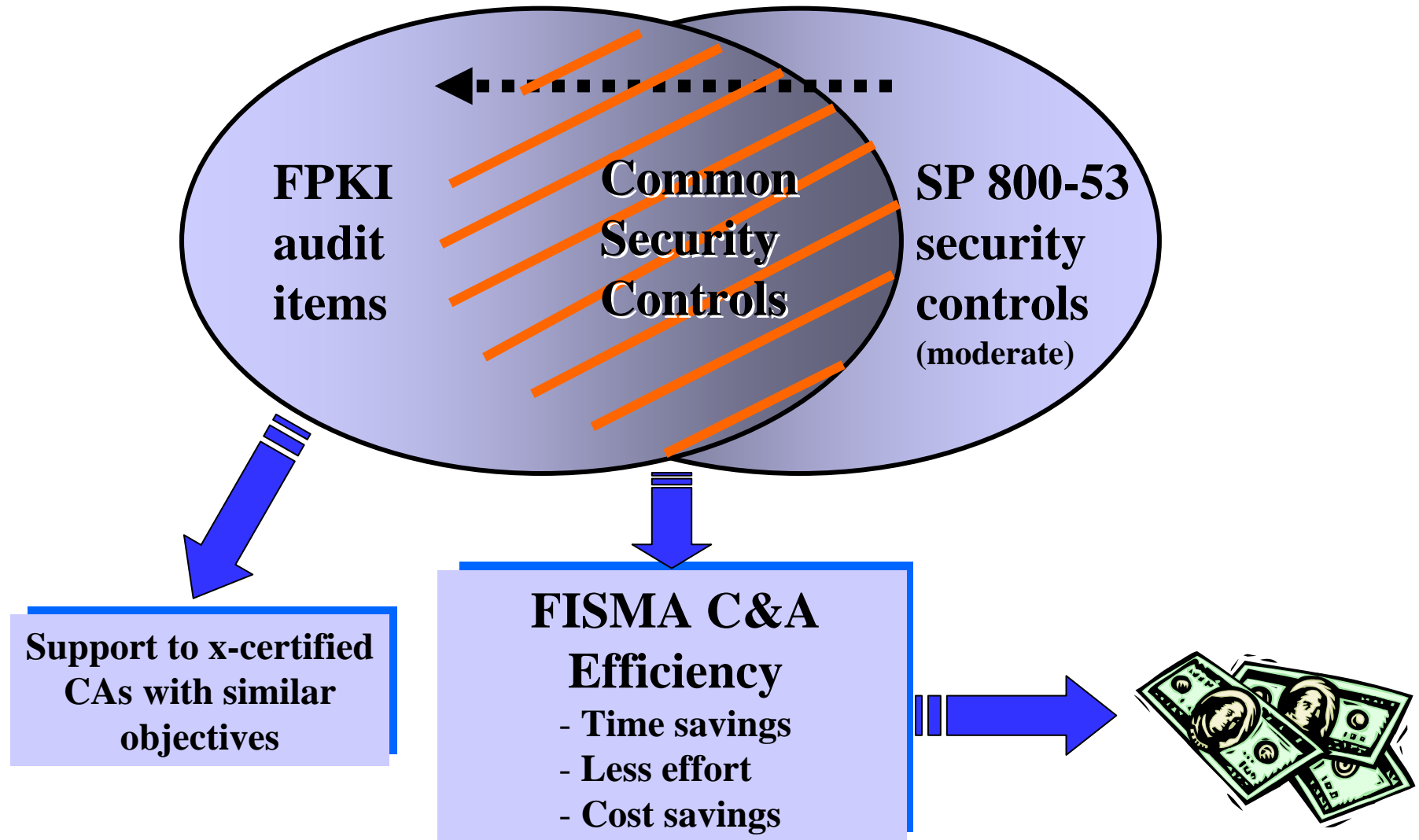


FISMA - resuability



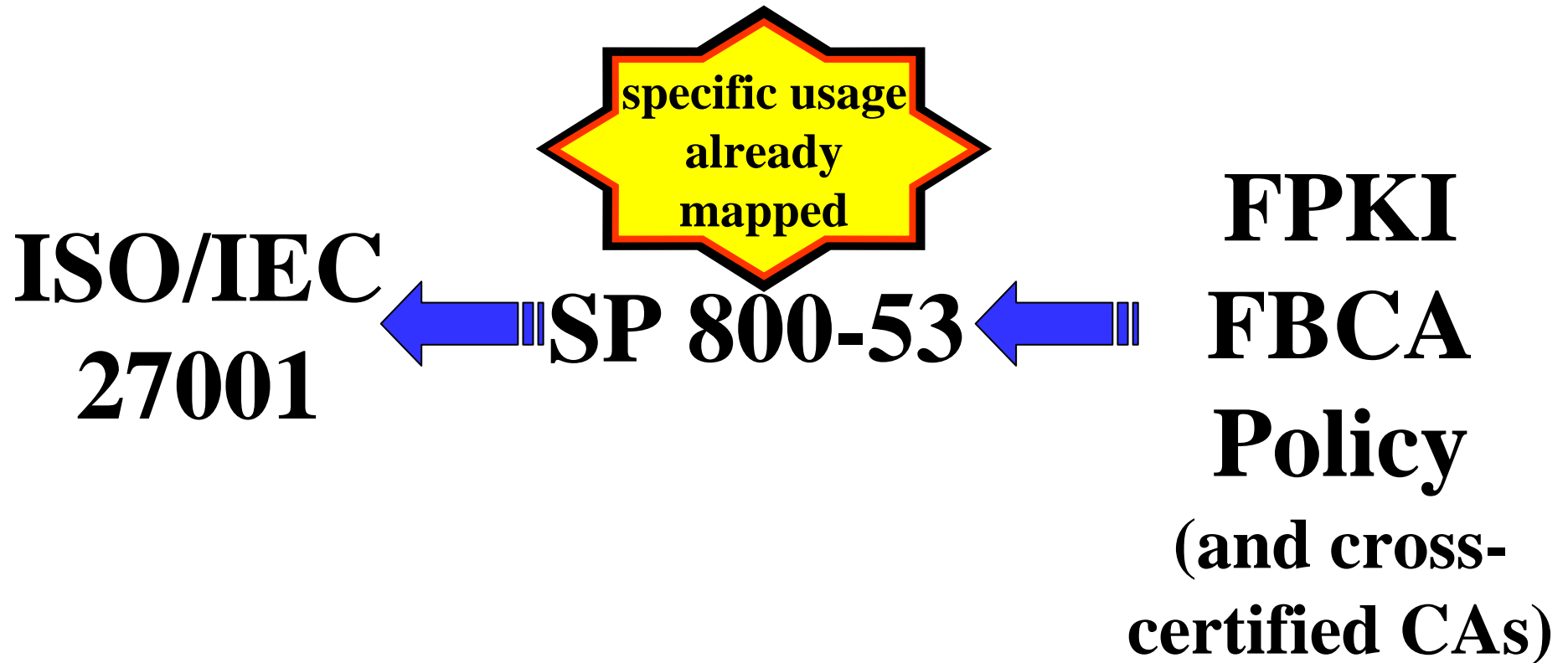


FBCA Policy / SP 800-53 mapping





FPKI OA proofing





summary - next steps

- establish joint recognition for assessors – fine-tune the ISO process
- minimise assessment overhead – recognise where re-sequencing is not detrimental to the principles of each model (e.g. 'desk' review)
- accommodate FISMA only and ISMS only options (e.g. some steps driven by need) – do not combine, just align
- identify SP 800-53 elements which could be commonly-applied, explicitly recognise that in the standard
- create an Extended Control Set (if required) which is SP 800-53 -specific (individual systems may always need additional, tailored, controls)
- consider additional controls within SP 800-53, to give broader security management perspectives (or reference ISO/IEC 27001??)
- prove concepts by practical implementation (FPKI OA C&A - 2008)



questions?



to follow-up:

Contacts:

Richard G. WILSHER

Founder & CEO

the *Zygma* partnership LLC

+1 714 965 99 42 (office)

+1 714 797 99 42 (mobile)

RGW@*Zygma*.biz