

A faint, light gray world map serves as a background for the title text.

“BS 7799-2 and the CC” Supporting the Business of Software Development

5th ICC, Berlin. 30th September, 2004

Fiona Pattinson

Agenda



Risk Management : Context , Systems

BS 7799-2 (an ISMS) supports systemic assurance by providing a framework supporting the SAR's demanded by a CC product evaluation

And...

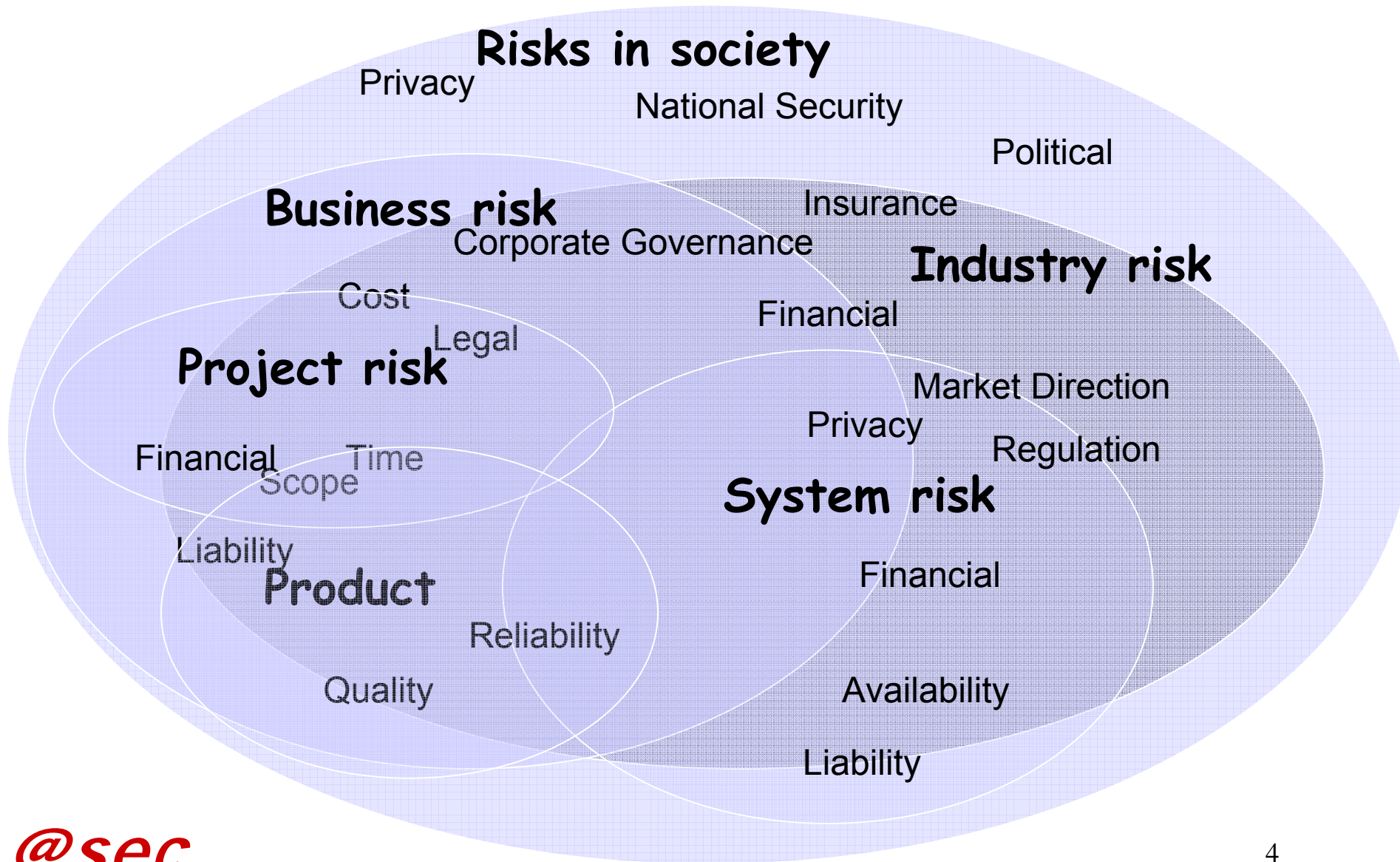
By providing a systemic assurance framework in which CC evaluated products can be used effectively



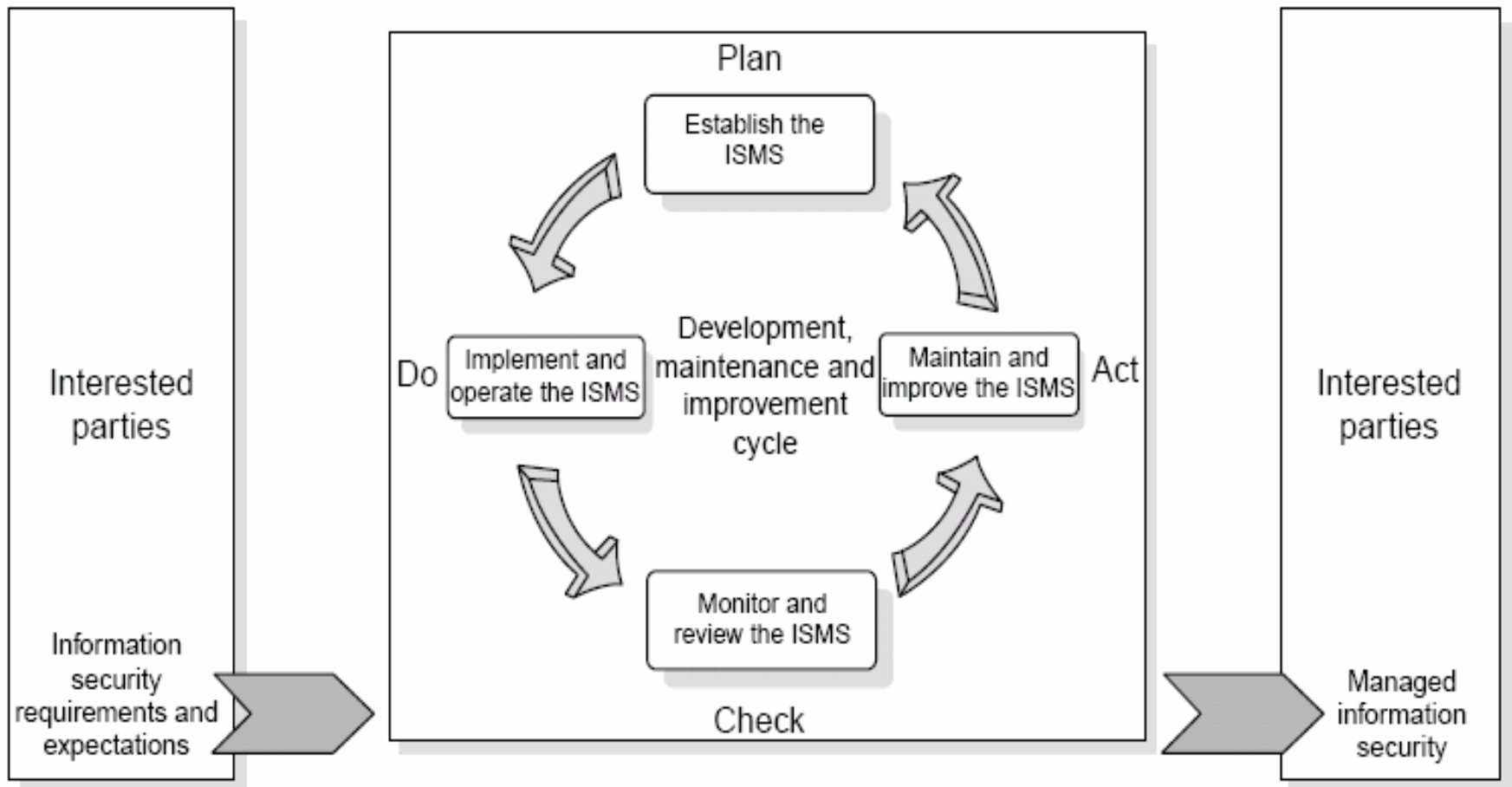
Definition: “System”

- For this presentation “system” does not mean a computer system
- Does mean the community
 - The people, computers and their environment
 - May be one or more computer-systems
 - May be one or more organizations

Risk management context



What is BS 7799-2?



What is Common Criteria?



- Product or component oriented
- Procedurally oriented
- Assurance based
- Boundary is defined by the “Target of Evaluation” (TOE)
- Significant software component
- A few IT system evaluations



@sec

the information security provider

Software development



Security IS a Quality Factor

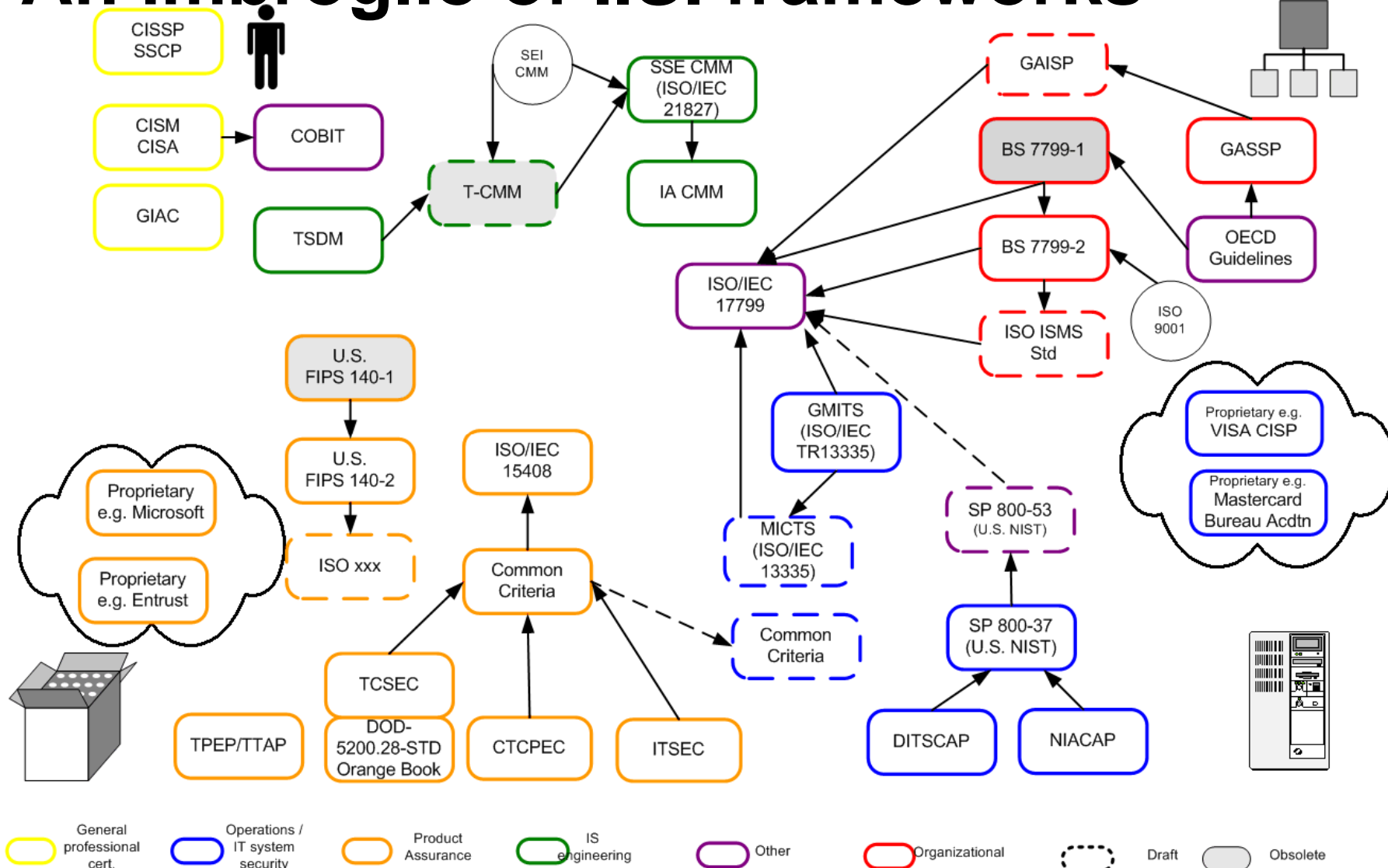
- Customer satisfaction, Customer expectations
- Frameworks quagmire: CMMI, SSE CMM, Agile,
- Service Provision: patches, warranties, maintenance
- Product risk management
- Systems, Systems of Systems
- Outsourcing & Supplier Management
- Legal / regulatory Issues :Trade Control & Compliance



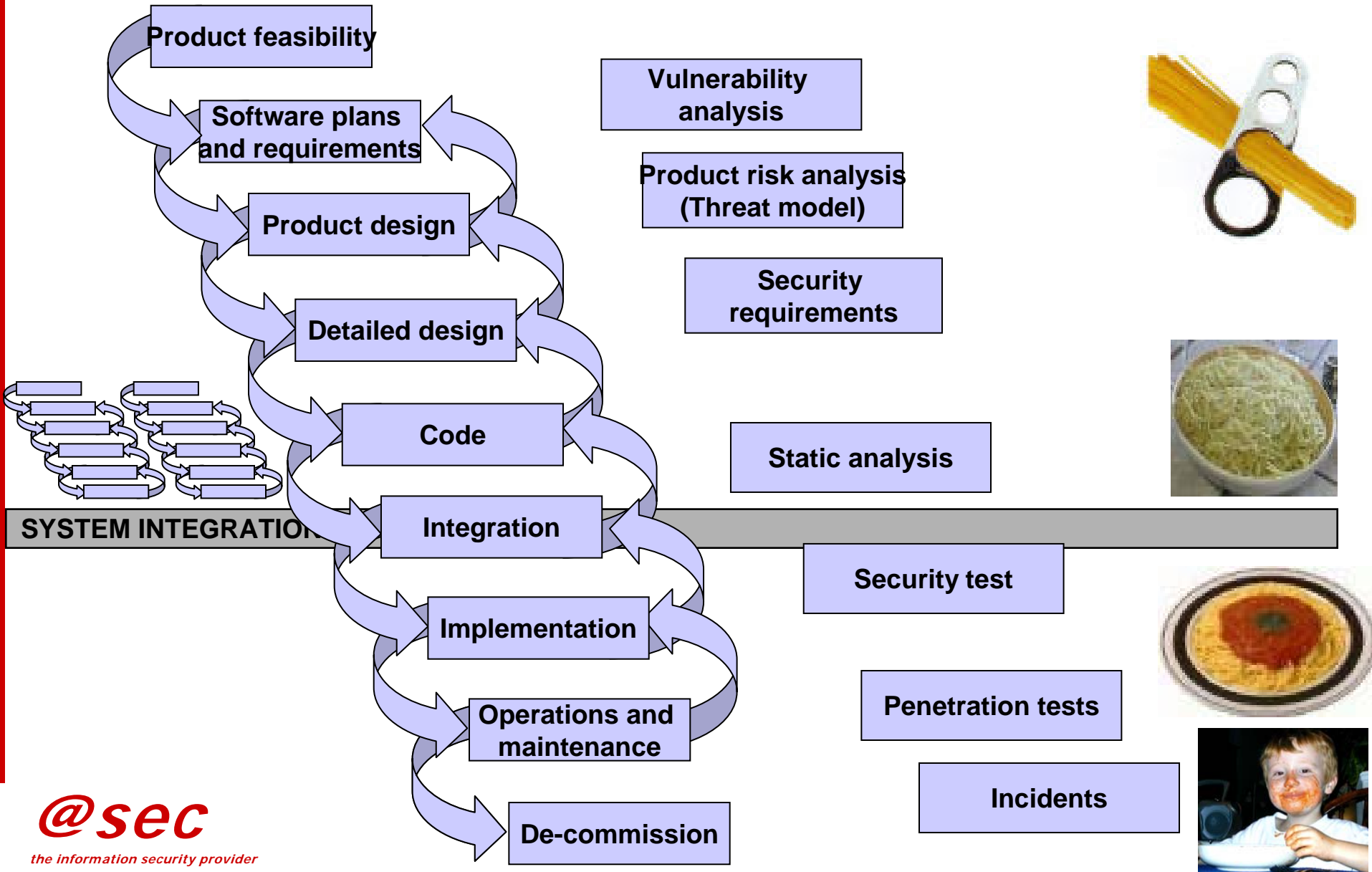
@sec

the information security provider

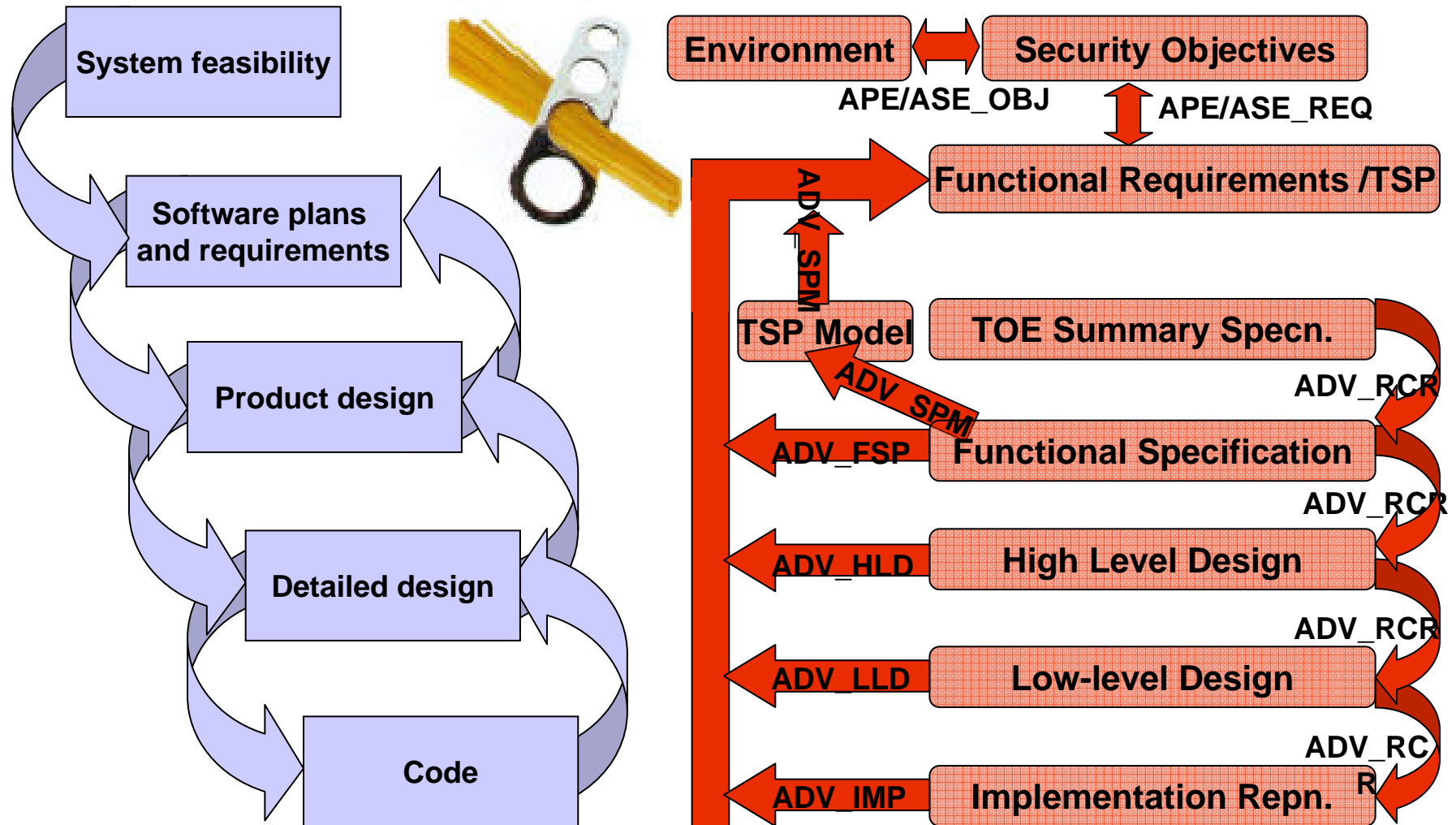
An imbroglio of I.S. frameworks



Development & security testing



ADV Development assurance

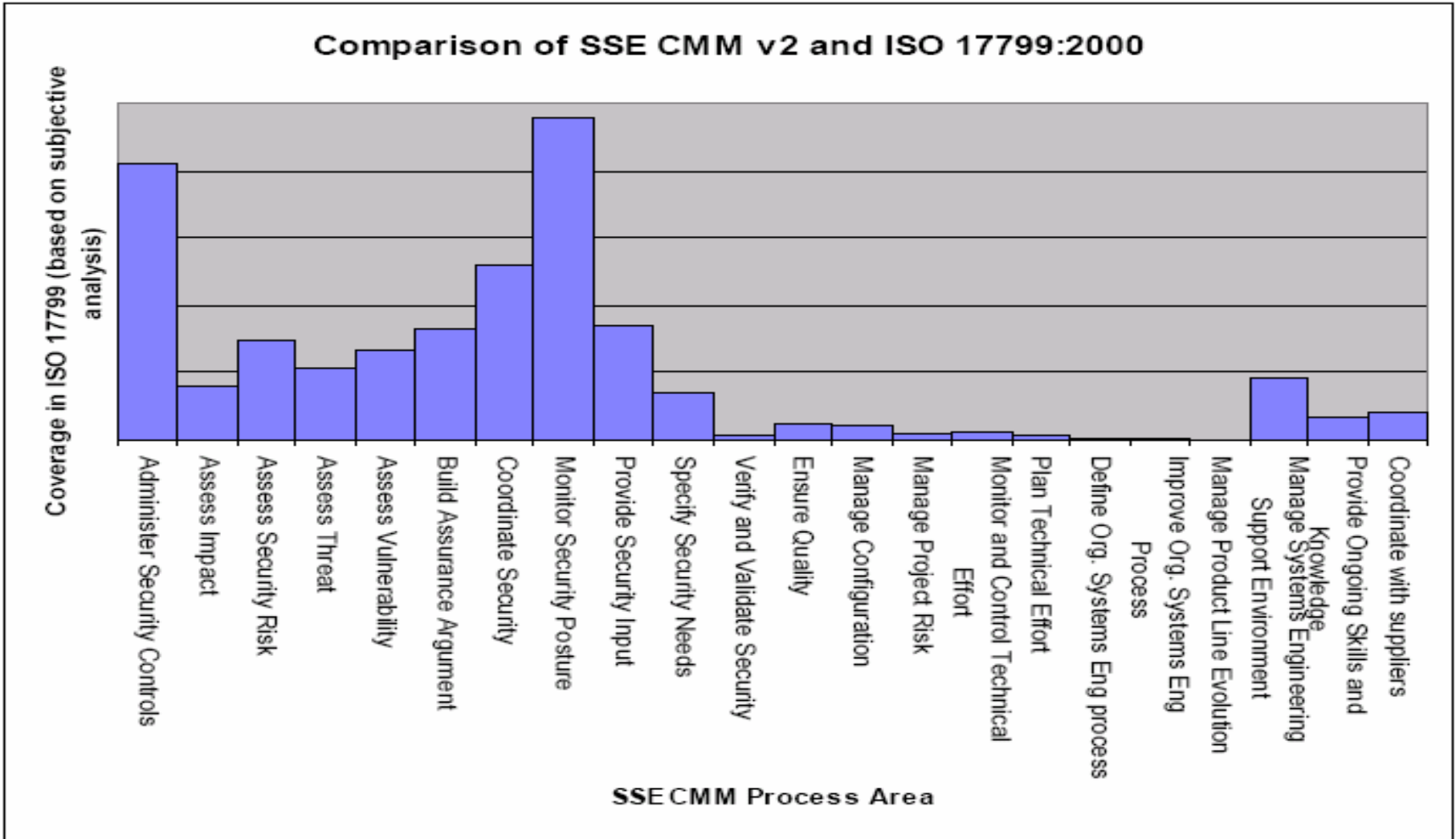


SYSTEM INTEGRATION =>

@sec

the information security provider

SSE CMM and ISO/IEC 17799



Placing products in the real world

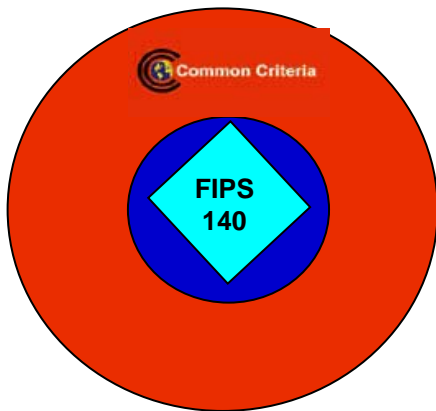


Were the ingredients fit to eat?

Was it prepared properly?

Can I use this to make a meal?


It's a little bland on it's own





How does BS 7799-2 support the CC?


- Through providing a process based framework for supporting the Security Assurance Requirements (SAR) and selecting safeguards commensurate with the risk:
 - ACM : Configuration Management
 - ALC : Lifecycle Support
 - ADO : Delivery and Operation
 - ADV : Development
 - AGD : Guidance Documents
 - ATE : Tests
 - AVA : Vulnerability Assessment


How does BS 7799-2 support the CC?

 **ALC_DVS.1.1D** The developer shall produce development security documentation.

 **ALC_DVS.1.1C** The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

 **ALC_DVS.1.2C** The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

 **ALC_DVS.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

 **ALC_DVS.1.2E** The evaluator shall confirm that the security measures are being applied.

How does BS 7799-2 support the CC? ICC

- Systemic processes NOT for a product instance
- Uses a good risk management methodology to
 - Identify applicable threats and vulnerabilities
 - Assess the risks
 - Choose appropriate controls (ISO/IEC 17799 +)
 - Apply them
- Ensures documentation
- Ensures measurement of effectiveness
- When in the certification scheme ensures, and provides evidence that this is the ongoing situation. (Not just one site visit.)

How does the CC support BS 7799-2? ICC



How does the CC support BS 7799-2? ICC

- Threats are an input to the organization's ISMS
- Organizational Security Policies are a requirement to the organization's ISMS
- In operation Assumptions are NOT a given and must be provided and monitored by the ISMS to achieve the claimed assurance.

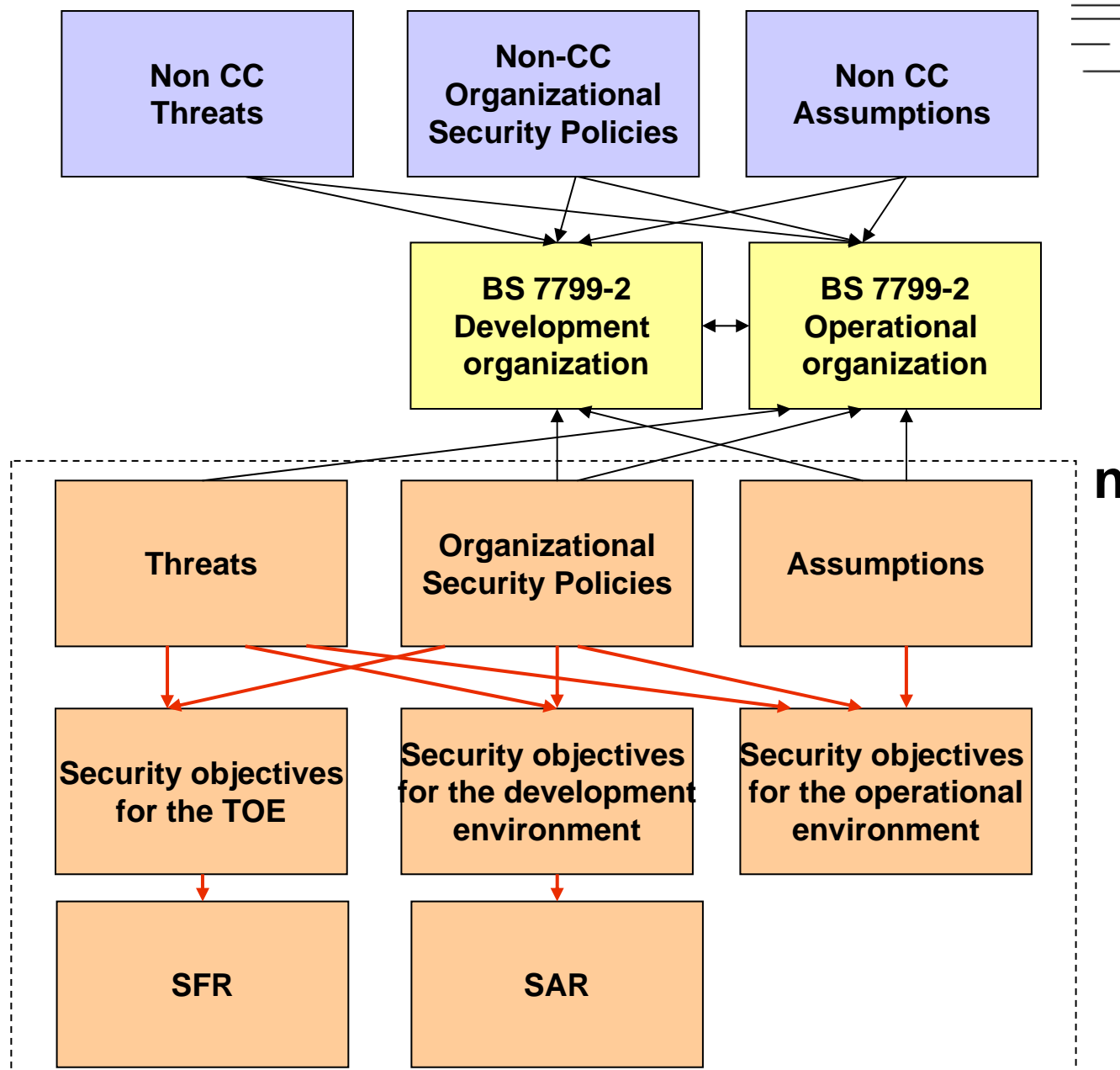


Common Criteria and systems



- Common Criteria does recognize that the product that is under evaluation is likely to be part of a larger system.
- One way in which CC conveys this is through assumptions, which communicate a vulnerability to the product purchaser (through the ST) or to the administrator or user through the guidance documents.
- Problem areas exist in composite systems, where the assurance of a composite system is not equivalent to those of its parts.





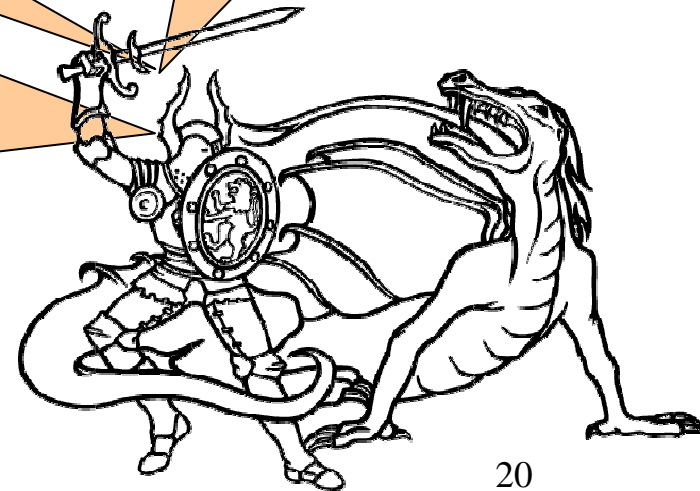
Assumptions := system vulnerabilities ICC

A.PROTECT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities which will prevent unauthorized physical access.

A.NO_EVIL_ADM

The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation

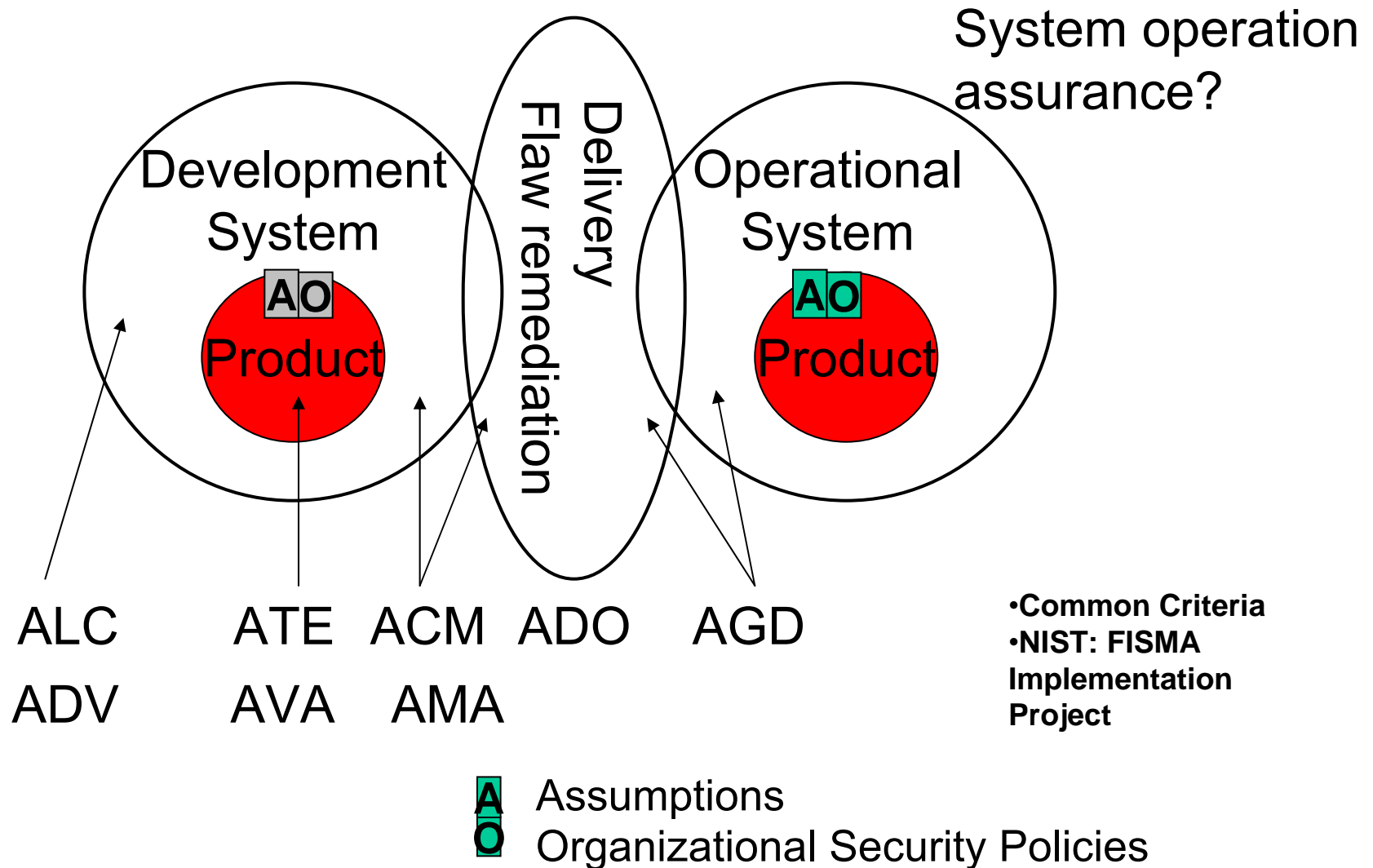


Organization Security Policies



- Examples of OSPs are:
 - – All products that are used by the Government must conform to the National Standard for password generation and encryption
 - – All products that are used by the branches of the Bank, must be CC certified with the EAL 4 + ADV_IMP.2 assurance package
 - – All system administrators that have access to the Department File Servers must be vetted to the level of Department Secret

Moving into operation



Conclusion

- Common Criteria is a good tool for product assurance
- It's only PART of the picture for the systemic view
- An ISMS (eg BS 7799-2) helps co-ordinate and maintain assurance in the “community”
- An ISMS framework in development brings effectiveness to CC development by providing a consistent and maintained environment
- An ISMS framework in operation brings effectiveness to CC deployment by supporting effective and efficient provision of a correct environment



Quality is Security: Security is Quality

Bibliography

- Alistair Cockburn and Jim Highsmith. **Writing Effective Use Cases**: Addison Wesley Longman Inc, 2001.
- Aristotle (edited by Richard McKeon). **The Basic Works of Aristotle**. *Organon* pp 7-217 : Random House Inc, 1941.
- The Common Criteria Sponsoring Organizations. "**Common Criteria for Information Technology Security Evaluation Version 2.2**" 2004.
- The Common Criteria Sponsoring Organizations,. "**Common Criteria for Information Technology Security Evaluation Version 2.4**" 2004.
- Boehm, B.W. and DeMarco, T. "**Software Risk Management**." *Software*, May/June (1997).
- Brewer, David. "**ISO/IEC 17799 Information Security Management Application to Smart Cards**." Paper presented at the *Smart Card Security Conference*, Tokyo 2001.
- Humphreys, Ted. "**The Newly Revised Part 2 of BS 7799**." 2002.
- ISMS-IUG. **International Register of BS 7799 Accredited Certificates**. Available from <http://www.xisec.com/Register.htm>.
- Karapetrovic, Stanislav and Jonker, Jan. "**Integration of Standardized Management Systems: Searching for a Recipe and Ingredients**." *Total Quality Management & Business Excellence* 14, no. 4 (2003): 451-60.
- Kocher, Paul; McGraw, Gary; Lee, Ruby and Raghunathan, Anand. "**Security As a New Dimension in Embedded System Design**." Paper presented at the *Annual ACM IEEE Design Automation Conference*, San Diego, CA, USA 2004.
- Sheard, Sarah A. "**Evolution of the the Frameworks Quagmire**." *Computer* 34, no. 7 (2001).
- FISMA Implementation Project: <http://csrc.nist.gov/sec-cert/>
- Tutorial on NIST Special Publication 800-37: **Guide for the Security Certification and Accreditation of Federal Information Systems** Version 1.2, (May 24, 2004). Available from <http://csrc.nist.gov/sec-cert/ca-library.html>
- ISMS-IUG. **International Register of BS 7799 Accredited Certificates**. Available from <http://www.xisec.com/Register.htm>.