Red Hat Security Update

SHAWN WELLS
Unclass: shawn@redhat.com
JWICS: wellshaw@nro.ic.gov
(+1) 443-534-0130

In the next hour . . .

- Factual information to answer security compliance questions

- Learn how to use Red Hat security compliance as a competitive advantage during sales cycle

- Understand where Red Hat technologies & services fit into certification and accreditation stages of the deal

Understanding Common Criteria

- Internationally standardized evaluation process to validate commercial technologies **perform as advertised**

Understanding Common Criteria

- Internationally standardized evaluation process to validate commercial technologies perform as advertised

- NSTISSP No. 11: Mandates government agencies ***only*** procure software which has been FIPS and Common Criteria certified. Effective since 1-JULY-2002.
  - No waiver process!
  - Products “In Evaluation” may receive conditional Deferred Compliance Authorization (DCA), which will be revoked if technology fails to pass Common Criteria

Understanding Common Criteria

- Internationally standardized evaluation process to validate commercial technologies perform as advertised

- NSTISSP No. 11: Mandates government agencies only procure software which has been FIPS and Common Criteria certified. Effective since 1-JULY-2002.
  - No waiver process!
  - Products “In Evaluation” may receive conditional Deferred Compliance Authorization (DCA), which will be revoked if technology fails to pass Common Criteria

- ***Reviews development processes*** in addition to capabilities

	Red Hat Enterprise Linux 6 with KVM	Red Hat Enterprise Linux 5.6 with KVM	IBM z/VM Version 5 Release 3 (for IBM System z Mainframes)	VMWare vSphere 5.0	VMWare ESXi 4.1	Microsoft Windows Server 2008 Hyper-V Role with HotFix KB950050
Certification Date	2012-10-08	2012-04-20	2008-08-06	2012-05-18	2010-12-15	2009-07-24
Certification Number		BSI-DSZ-CC -0724-2012	BSI-DSZ-CC -0472-2008	383-4-189-CR	383-4-145 383-4-147	BSI-DSZ-CC -0570-2009
EAL Level	EAP4+	EAP4+	EAP4+	EAP4+	EAP4+	EAP4+
CAPP	YES	YES	YES	NO	NO	NO
RBAC	YES	YES	NO	NO	NO	NO
LSPP	YES	YES	YES	NO	NO	NO

CAPP: Users control who access' their data
RBAC: Users classified into roles ("BackupAdm," "AuditAdm"...)
LSPP: Compartmentalizes users and applications from each other. Enables MLS.

Common Criteria, NIST, STIG, USGCB

Common Criteria tells the government software can be “trusted”

Common Criteria, NIST, STIG, USGCB

Common Criteria tells the government software can be “trusted”

NIST publishes a catalog of security best practices
(“You must use secure passwords!”)

Common Criteria, NIST, STIG, USGCB

Common Criteria tells the government software can be “trusted”

NIST publishes a catalog of security best practices
(“You must use secure passwords!”)

Agencies select practices they agree with, and refine them
(“NSA secure passwords must be 100 characters”)

Common Criteria, NIST, STIG, USGCB

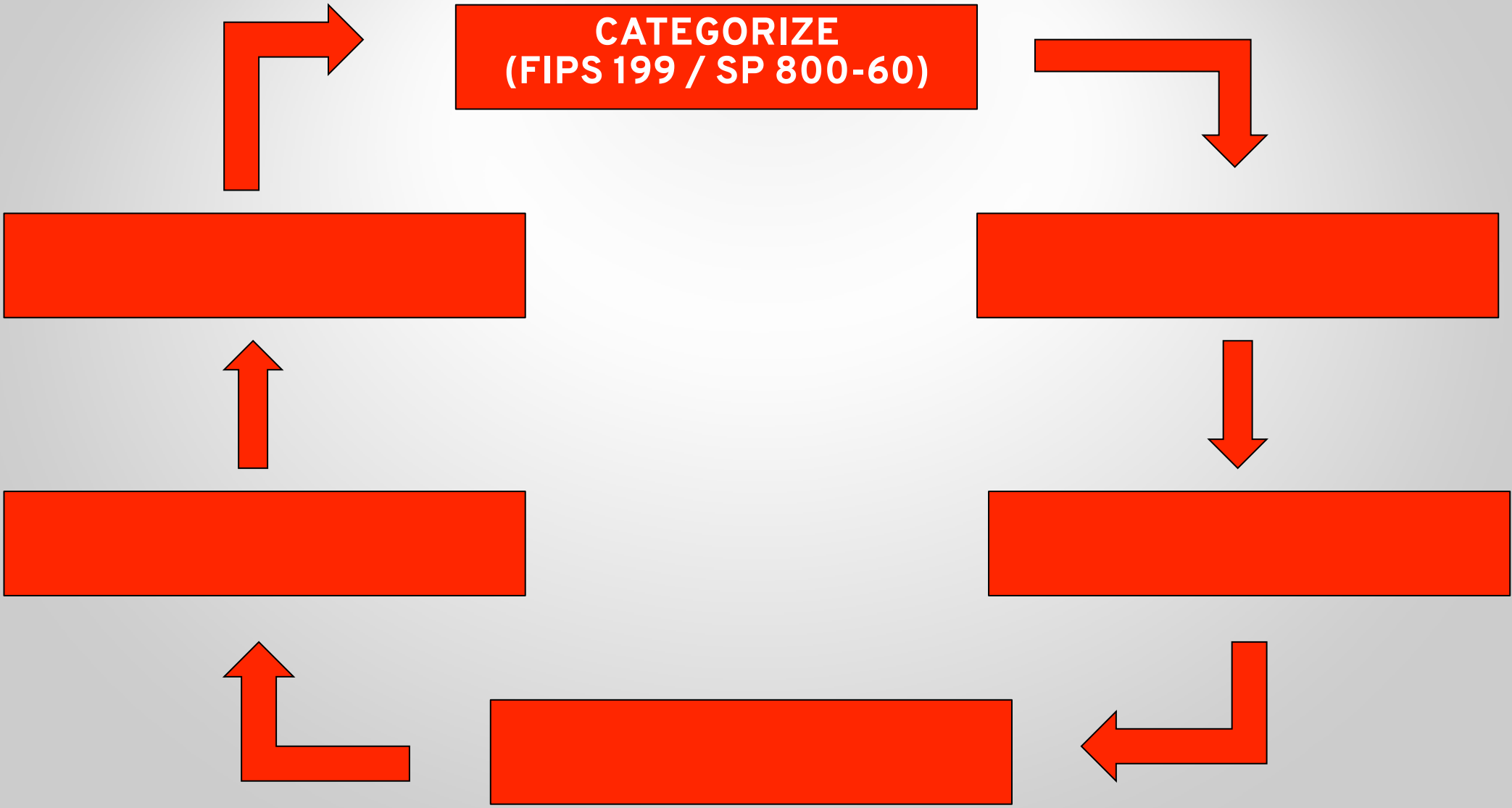
Common Criteria tells the government software can be “trusted”

NIST publishes a catalog of security best practices
(“You must use secure passwords!”)

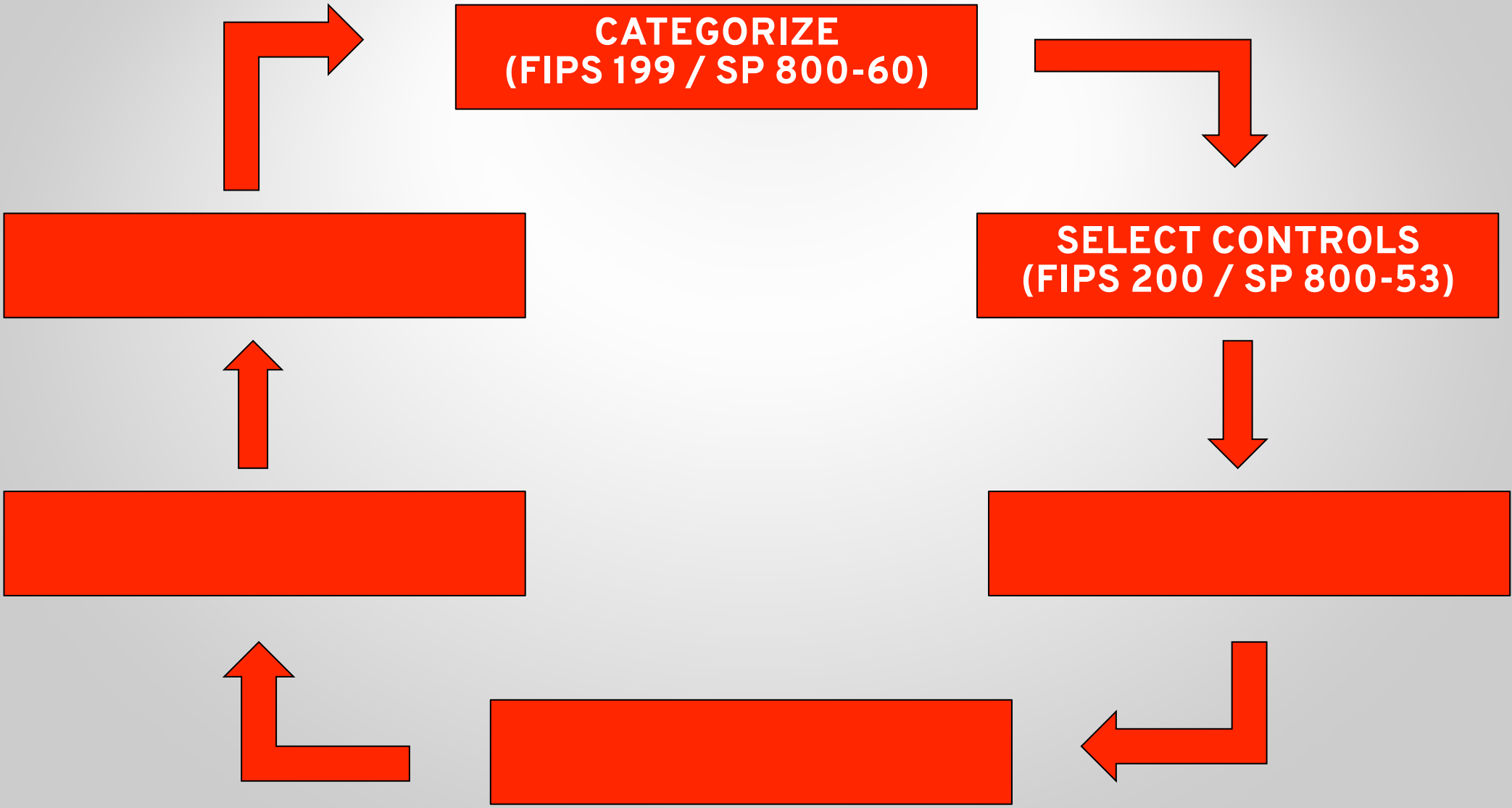
Agencies select practices they agree with, and refine them
(“NSA secure passwords must be 100 characters”)

Agencies aggregate refined values into Agency baselines
(e.g. STIG for DOD, USGCB for Civilian)

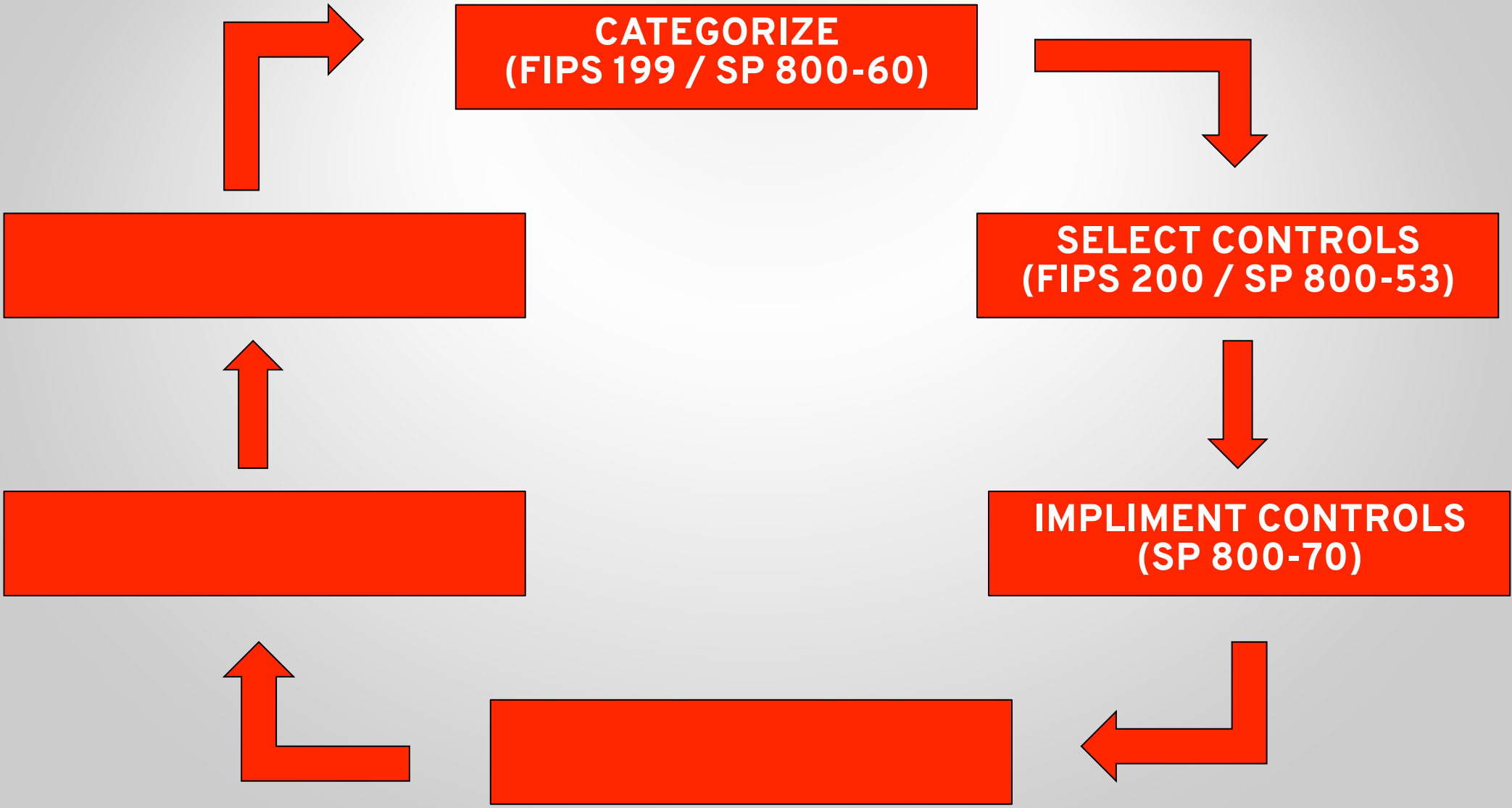
What is the C&A process?



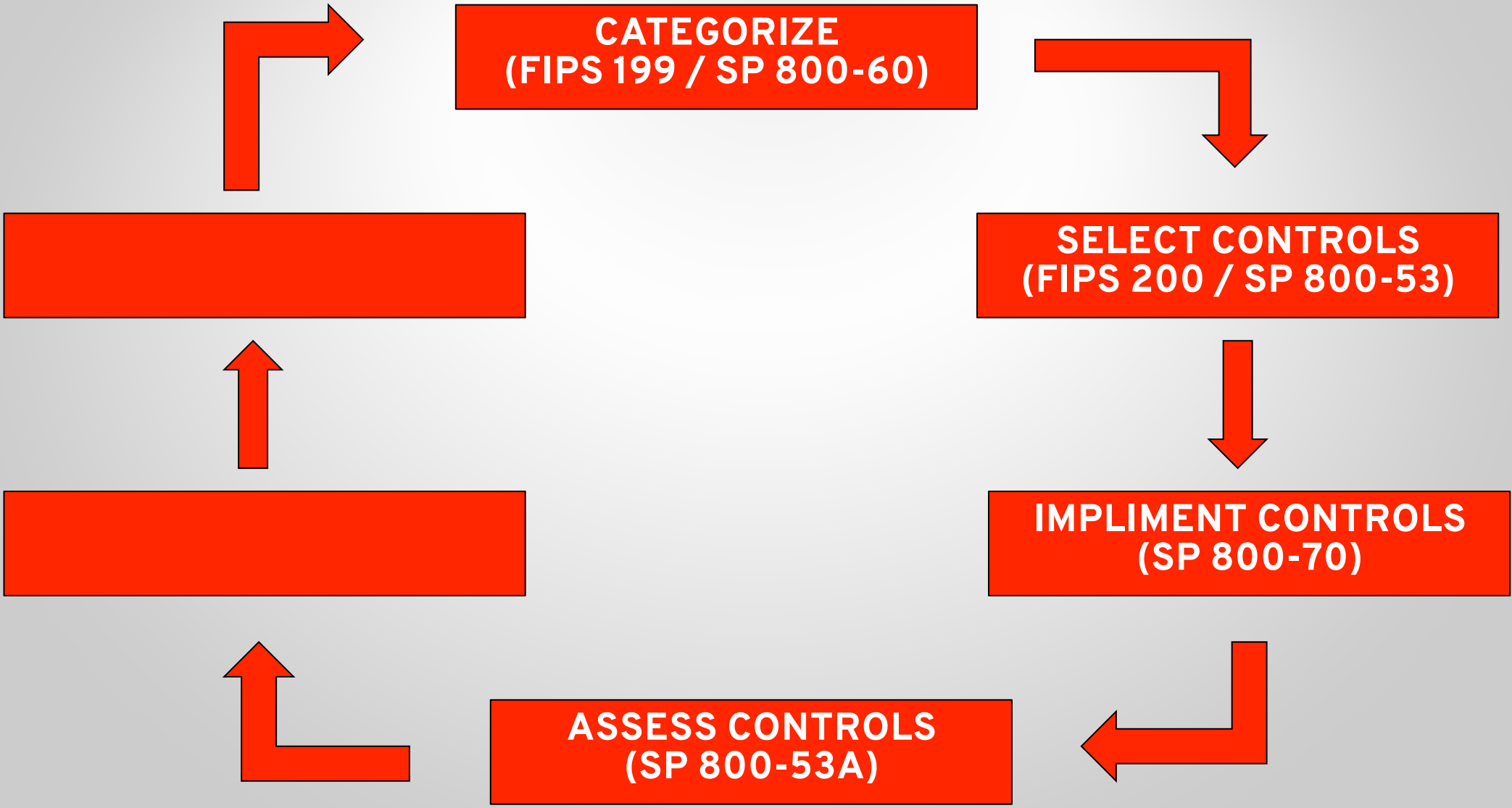
What is the C&A process?



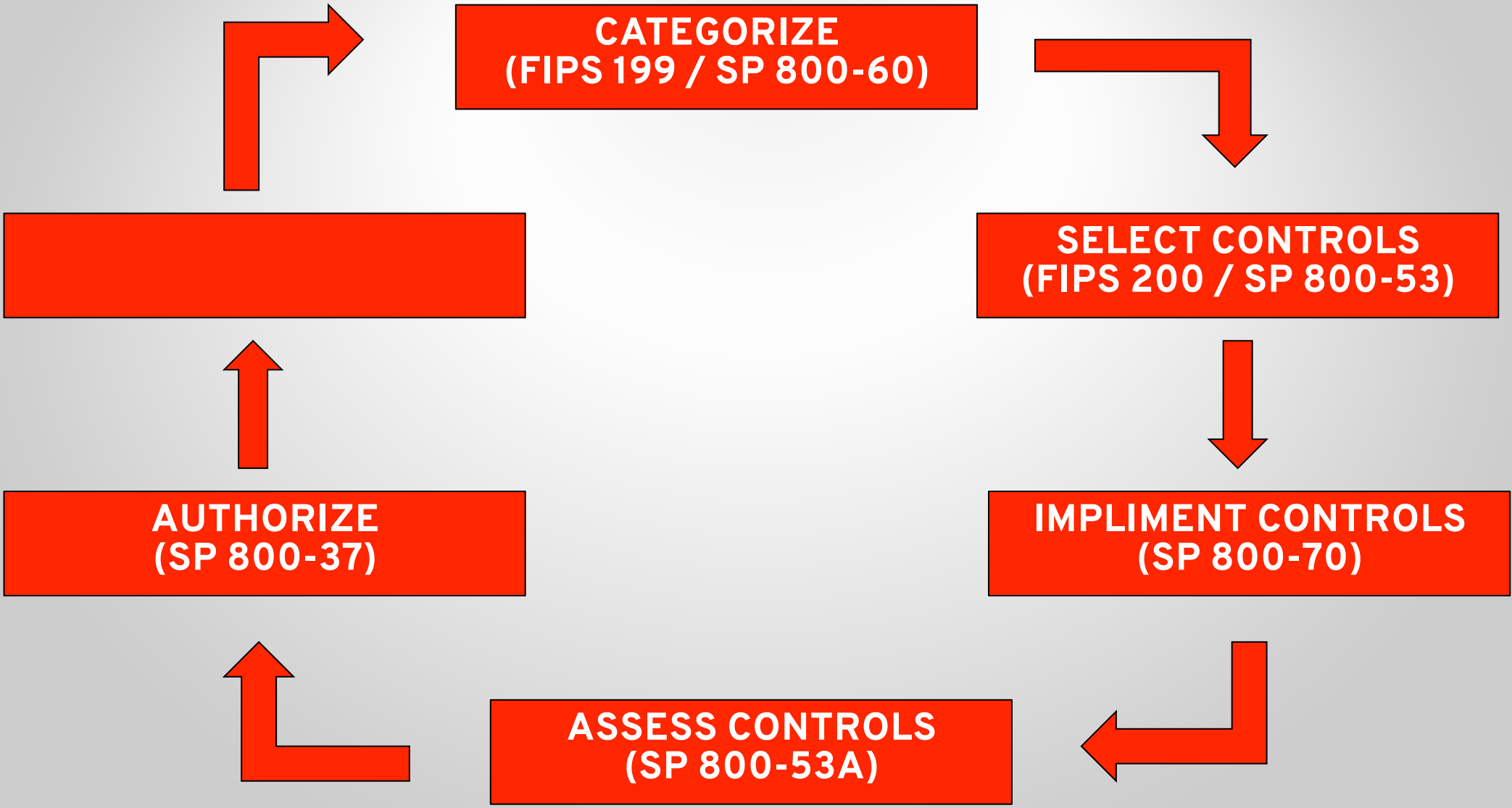
What is the C&A process?



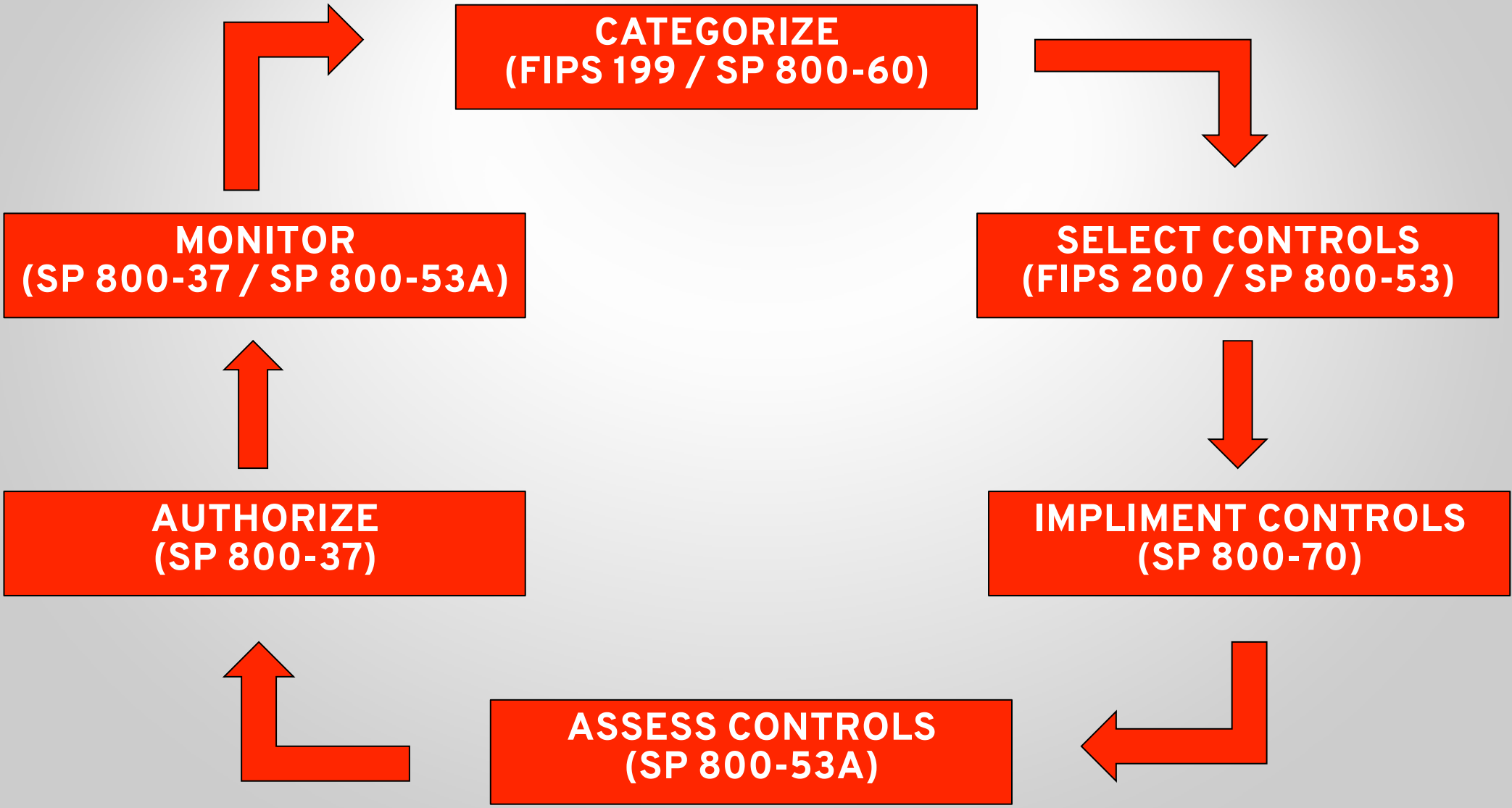
What is the C&A process?



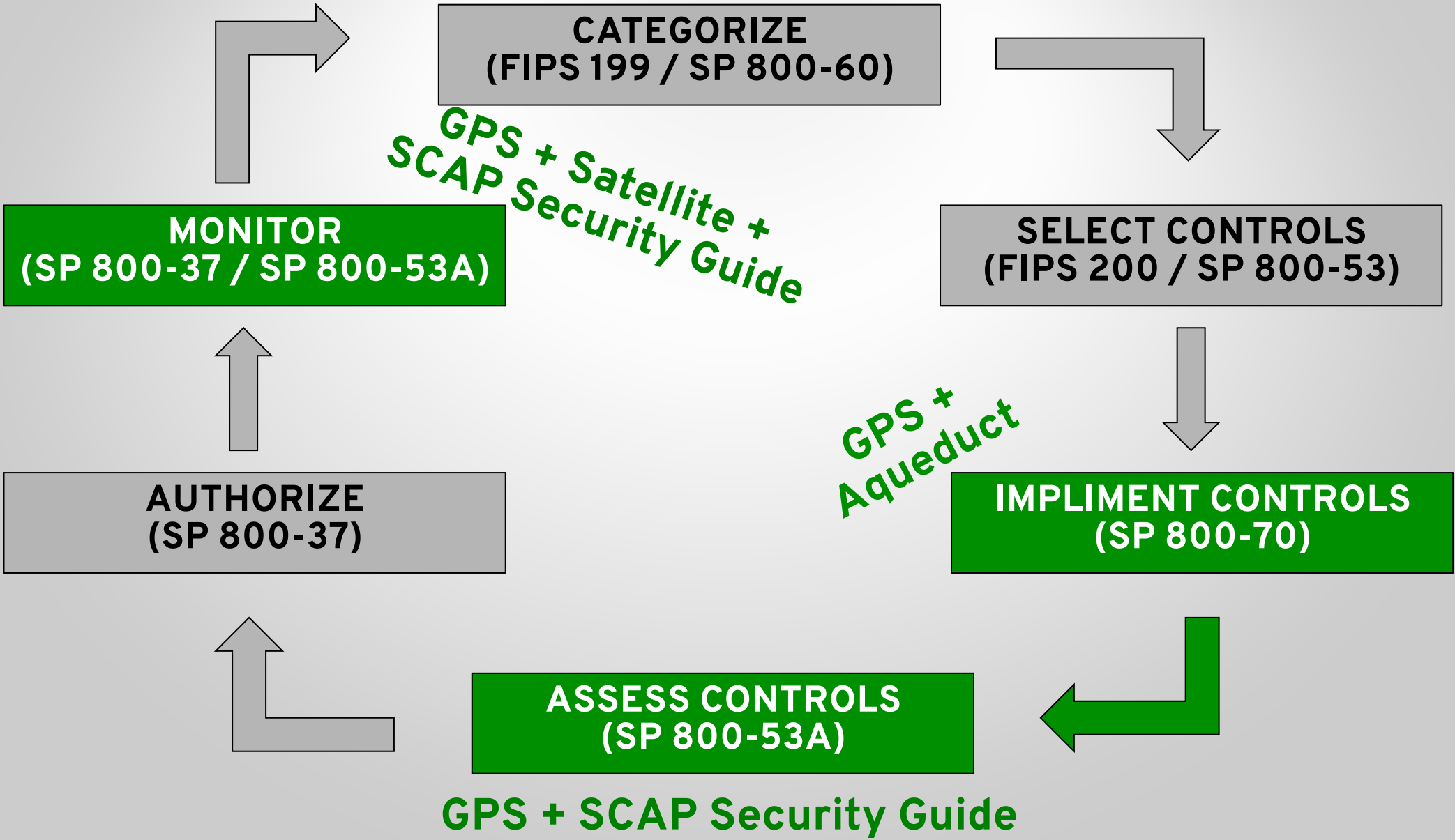
What is the C&A process?



What is the C&A process?



What is the C&A process?




I DON'T ALWAYS TEST MY CODE
BUT WHEN I DO, IT'S DURING LIVE DEMOS
memegenerator.net