



Virginia Information Technologies Agency

Exceptions, Common Controls, and the Cloud

John Craft
Commonwealth Security Architect



Security

- Good security
 - Proactive
 - Common defense in depth
 - Culture of security
- Bad security
 - Reactive
 - Siloed
 - Silent

What is a security exception?





Common exception drivers

- Technical limitations
- Regulatory or legal requirements
- Business needs
- Personnel / staffing limitations
- Budgetary limitations*



SEC501 definition

A deviation from a specific requirement of commonwealth security standards, policies, or configuration baselines.

Example: An agency needs to continue to run Windows Server 2003 after 7/14/15 in deviation from SI-2-COV of SEC 501-09.



But is that all?

Also a formal acknowledgement of risk by the Agency Head

- Code of Virginia § 2.2-603(F) states: “the director of every agency and department in the executive branch of state government, including those appointed by their respective boards or the Board of Education, shall be responsible for securing the electronic data held by his agency or department and shall comply with the requirements of the Commonwealth's information technology security and risk-management program as set forth in § [2.2-2009](#).”



Why must the CISO approve?

- Risk must often be assessed from an enterprise perspective
- More complete knowledge of available enterprise controls
- Evaluation against the established enterprise risk threshold



What is expected?

- Business need / Justification
- Scope and extent
- Compensating controls
- Identification of risks and residual risks
- Specific duration – not to exceed one year
- Agency Head approval



Templates

- VITA CSRM has templates for many of the common exception requests
- A blank template is located at:

http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Word_versions/Blank_Exception_form.doc



Blank Template

COV Information Security Policy & Standard Exception Request Form
Agency Name: _____ Contact for Additional Information: _____

Policy/Standard requirement to which an exception is requested: _____

Note: This request is for an exception(s) to a component of the Commonwealth policy and/or standard(s) and approval of this request does not in any way address the feasibility of operational implementation. You are encouraged to check with your technical support staff prior to submitting this request.

1. Provide the **Business or Technical Justification:**

2. Describe the scope including quantification and requested duration (not to exceed one (1) year):

3. Describe all associated risks:

4. Identify the controls to mitigate the risks:

5. Identify all residual risks:

I have evaluated the business issues associated with this request and I accept any and all associated risks as being reasonable under the circumstances.

Printed name Agency Head	Signature	Date
--------------------------	-----------	------

Justification

- The business or technical need driving the request. This well defined and includes pertinent ancillary artifacts, such as:
 - Work requests
 - VCCC / helpdesk tickets
 - Project plans
 - Vendor documentation
- Cost is rarely considered a compelling justification

Scope and duration

- Exception should document details:
 - Number of systems impacted
 - Applications impacted
 - Accounts impacted
 - Data sensitivity classification
- Duration should be specified
 - Not to exceed one year
 - Exception should be remediated before expiration; if not, an extension or new request should be submitted

Compensating Controls

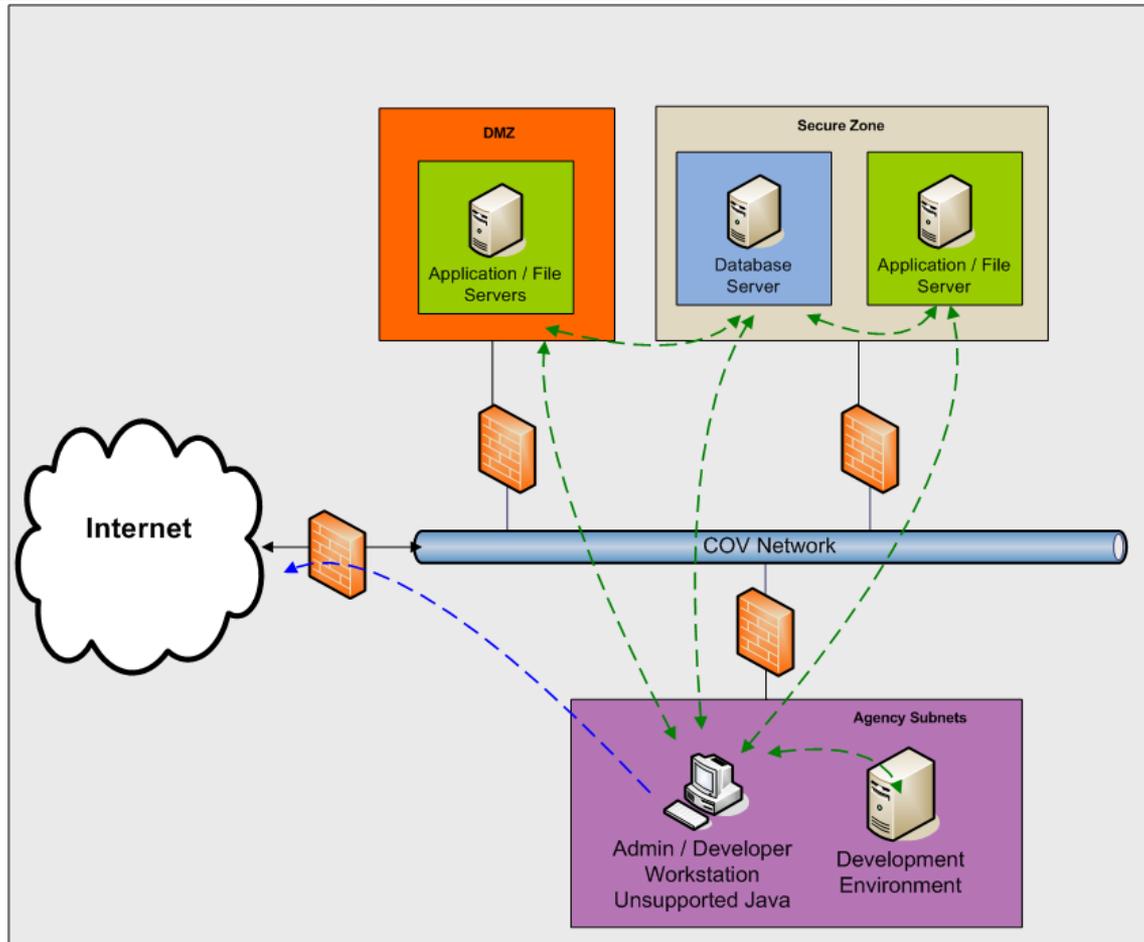
- Controls implemented to satisfy the requirements of approved security standards, policies, and baselines when those requirements cannot be met.
- Compensation controls should:
 - Be commensurate with the risk of not adhering to the original requirement;
 - Meet the intent of the original requirement; and
 - Provide similar defense as the original requirement.



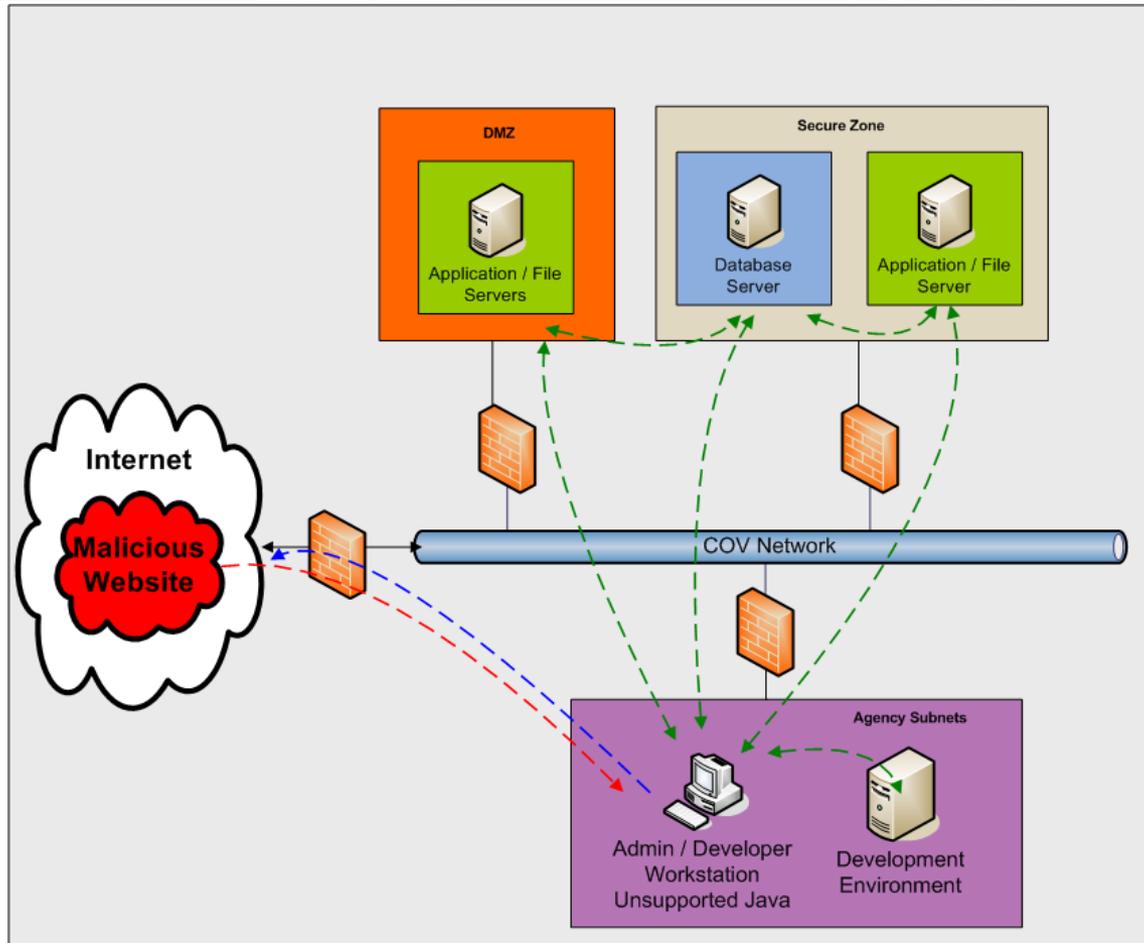
Risks

- Identify risks associated with the requested security exception
- Compensating controls should be matched to identified risks
- Residual risks are those risks not completely mitigated by compensating controls
 - Compensating controls rarely completely mitigate risk

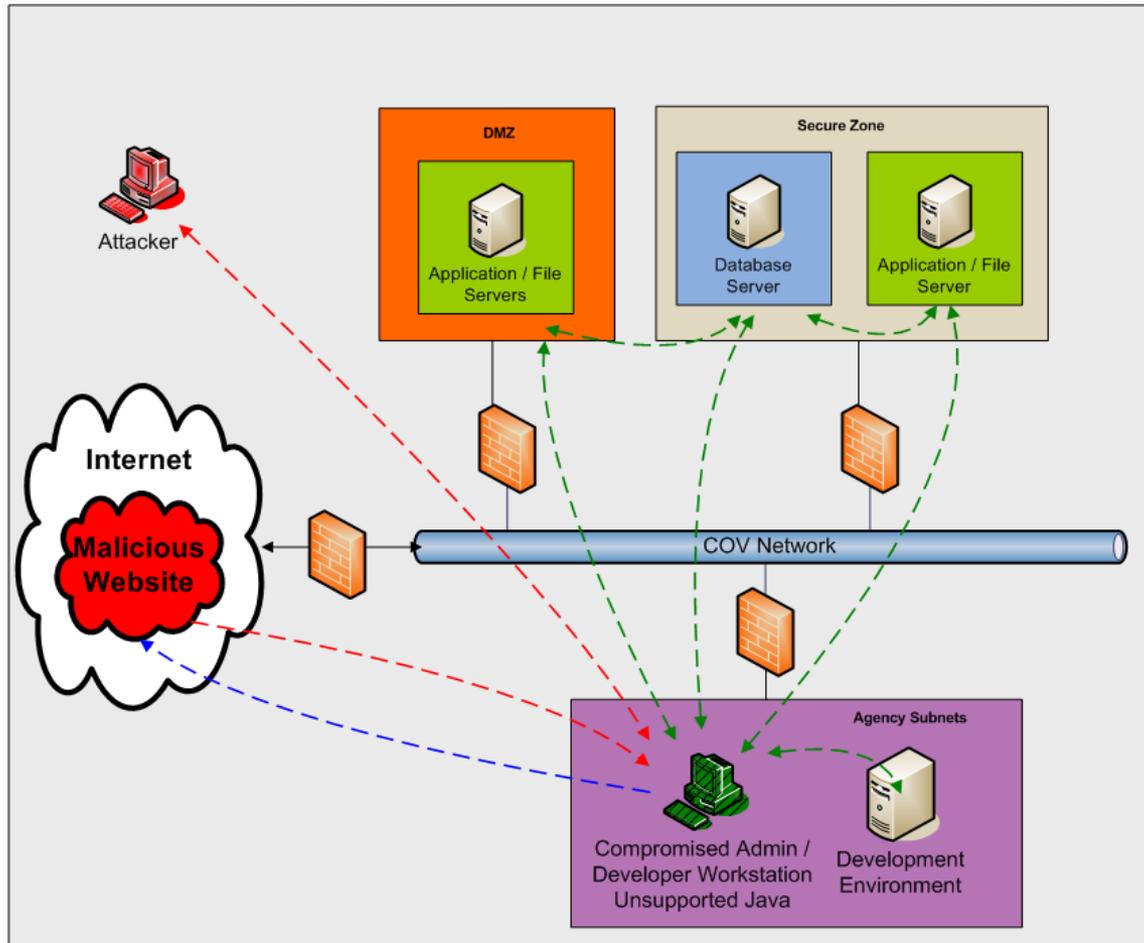
Basic Compromise Example



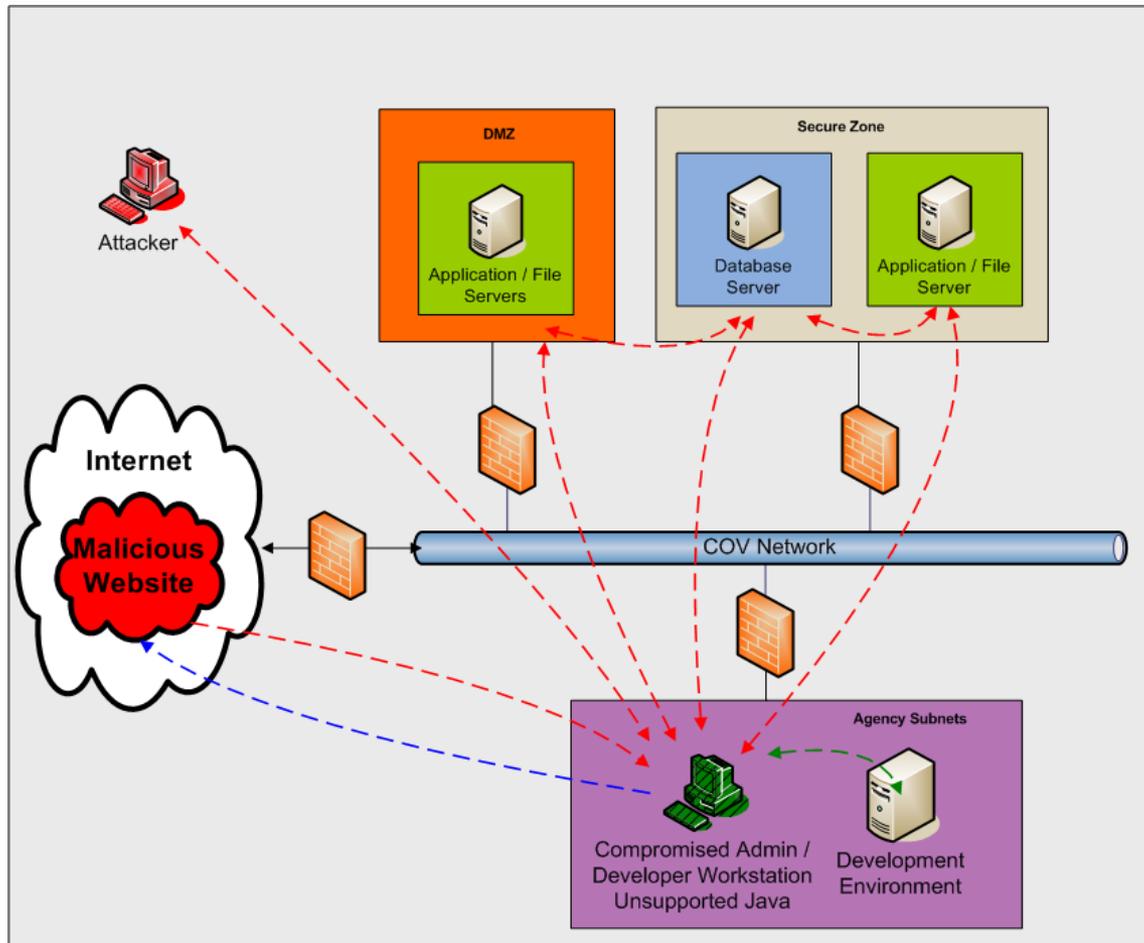
Basic Compromise Example



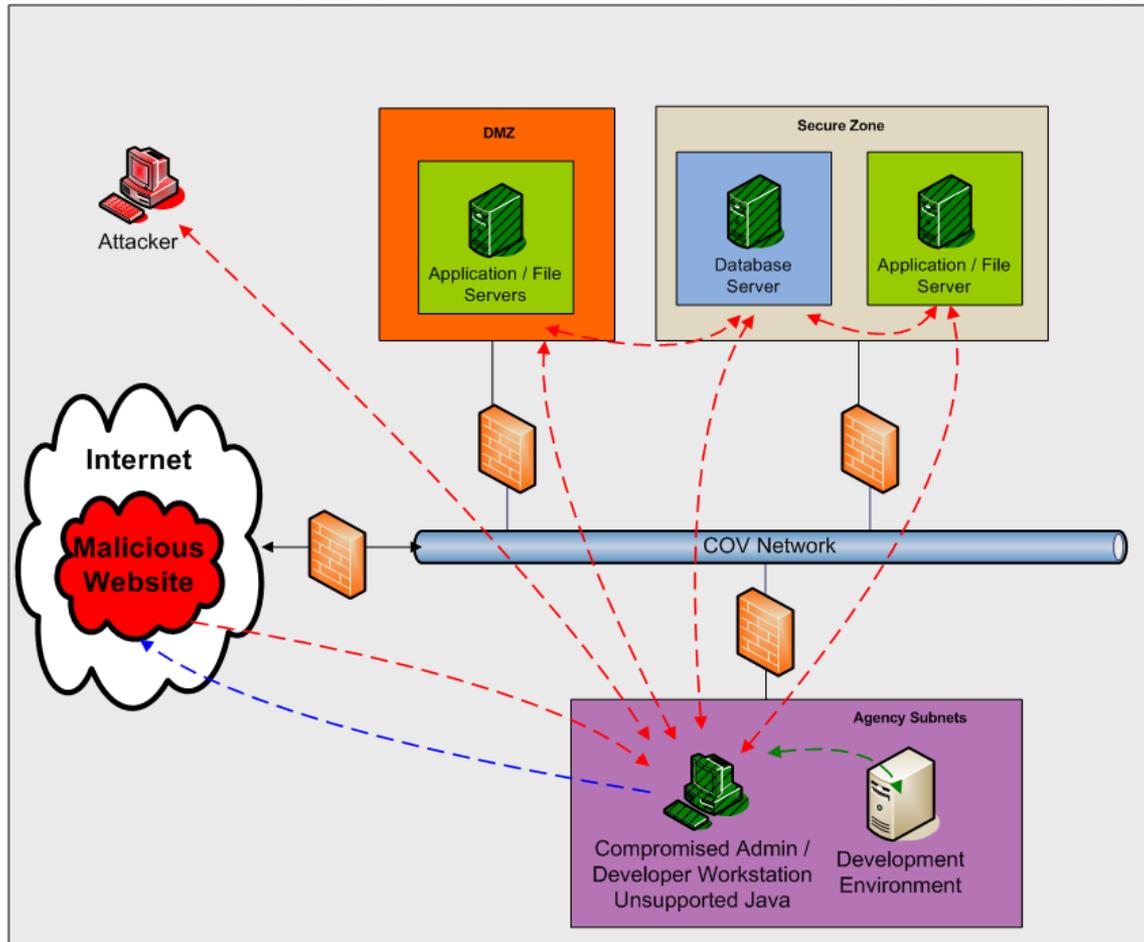
Basic Compromise Example



Basic Compromise Example



Basic Compromise Example





Things to think about

- What other resources do my at-risk resources have access to?
- What is the privilege context of the resource?
- What is the comprehensive risk before controls?
- What controls will be the most effective?
- Where do controls best fit into my architecture?
- What risks do the controls not address?



Common compensating controls

- Application control (WWLS)
 - End-of-support software
 - Shared systems
- Host-based Intrusion Prevention System (HIPS)
 - End-of-support frameworks (.NET) associated with approved processes
 - Unsupported transactional systems (databases)



Common compensating controls

- Managed firewall
 - End-of-support software / systems
 - Shared systems
 - Systems that cannot have other technical controls installed
- Enhanced logging and monitoring
- Enhanced physical security
- Enhanced scanning operations



Submission requirements

- Submission must come from the Agency Head or the Agency ISO
- Submission must be approved by the Agency Head
 - This can be via email



The Cloud

- Hosted Environment Information Security Standard (SEC525-01) has been published on the VITA website
 - http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/HostedEnvironmentInformationSecurityStandardSEC52501.pdf
- Based on SEC 501, FEDRAMP, and Cloud Security Alliance (CSA)
- Effective as of 3/22/16



Cloud Drivers and Detractors

- Advantages
 - Efficiency
 - Speed
 - Elasticity
 - Cost *
- Disadvantages
 - Loss of control
 - Multi-tenancy
 - Cost *



Key control awareness

- Liability language commensurate with data sensitivity and risk (1.7)
- No sensitive data stored outside of the commonwealth (1.8)
- 30 minute lockout after 3 consecutive invalid logon attempts in 15 min period (AC-7)
- 15 minute session lock (AC-11)
- 15 minute timeout / disconnect for remote sessions (AC-17-COV, SC-10)
- Weekly review and analysis of audit records (AU-6)
- Many review and analysis requirements changed from annual to monthly / quarterly



Key control awareness

- Authenticator management (IA-5)
 - 60 day password expiration (42 for admin accounts / sensitive systems)
 - 12 character minimum password length
 - Must use all 4 character types
- Automated incident response capability for sensitive systems (IR-6 & IR-7)
- Quarterly IPS / IDS reporting (IR-6-COV)
- Vulnerability scans at least every 30-days with remediation of identified vulnerabilities within 30 days (RA-5)
- Application and data storage instances cannot be hosted on the same hypervisor (SA-3-COV-2)



Key control awareness

- SA-4, SA-4-COV-1, SA-9, SA-9-COV-1, SA-9-COV-1: All very important acquisition requirements
 - Geographic location of data requirements
 - Data escrow requirements
 - Contractual control requirements
- All cryptographic keying material must remain under exclusive control of the commonwealth (SC-12-COV)
- Required encryption for the protection of sensitive data at rest (SC-28)
- Install security-relevant updates within 60 days of release by the vendor (SI-2-COV)
- SI-6 and SI-7: security functionality and software / information integrity verification requirements



Thank you for attending!

Questions?