ID18939561

CPA SECURITY CHARACTERISTIC

CPA-SC SERVER VIRTUALISATION 1.21.DOCX

Version 1.21

© Crown Copyright 2016 – All Rights Reserved

Document History

Version	Date	Description
1.1	September 2011	First published version.
1.21	May 2012	Augmented Grade mitigations added

This Security Characteristic is derived from the following files

File Name	Version
Server Virtualisation - v1.21.cxl	1.21
Virtualisation - Common - v1.21.cxl	1.21
Common Libraries - v1.6.cxl	1.6

Soft copy location

DiscoverID 18939561

This document is authorised by:

Deputy Technical Director (Assurance), CESG

This document is issued by CESG

For queries about this document please contact:

CPA Administration Team
CESG
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX
United Kingdom

Tel: +44 (0)1242 221 491
Email: cpa@cesg.gsi.gov.uk

The CPA Authority may review, amend, update, replace or issue new Scheme Documents as may be required from time to time.

CONTENTS

REFERENCES

[a] CESG IA Good Practice Guide No 12 – Use of Virtualisation Products for Data Separation: Managing the Security Risks – Issue 1.2 – August 2010 (Not Protectively Marked). Available at: https://cesgiap.gsi.gov.uk. An updated issue, based on CPA, is currently in production.

[b] The Process for Performing Foundation Grade CPA Evaluations, v1.3, August 2011, CESG. Available at http://www.cesg.gov.uk.

[c] HMG IA Standard No 1 – Technical Risk Assessment – Issue 3.6 – October 2010 (Unclassified)

[d] NIST Special Publication 800-22 Revision 1a – A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications – Revised April 2010. Available at http://csrc.nist.gov.

[e] CESG IA Good Practice Guide No 13 – Protective Monitoring for HMG ICT Systems – Issue 1.5 – August 2010 (UNCLASSIFIED). Available at: https://cesgiap.gsi.gov.uk.

[f] CESG IA Implementation Guide No 3 – User Authentication Systems – Issue 1.0 – May 2011 (UNCLASSIFIED). Available at: https://cesgiap.gsi.gov.uk.

I. OVERVIEW

1. This document is a CPA Security Characteristic – it describes requirements for a particular type of assured product for evaluation and certification under CESG's Commercial Product Assurance (CPA) scheme.

A. Product Aims

2. The primary purpose of a virtualisation product is to provide the ability to run multiple instances of a commercial operating system on a single piece of hardware. Products providing virtualisation offer separation between operating system instances and an interface to allow the sharing of system resources.

3. A virtualisation product only needs to be assured when it is being used to run virtual machines from different security domains on the same platform (i.e. the virtualisation product forms part of the security boundary).

4. In this context, a 'security domain' refers to one or more virtual machines sharing a common threat model. Generally, this is the same as saying that they share the same protective marking though, as noted in reference [a], there can be situations where system architects or data owners want separate security domains at the same protective marking.

5. Security domains are described as 'Red' or 'Black' (or, similarly, 'Red side' or 'Black side'), based on terms commonly used in the design of cryptographic systems. The Red side contains the more sensitive data (such as RESTRICTED material), while the Black side contains the less sensitive data (such as UNCLASSIFIED material). This document assumes that an attacker will compromise the Black side and that attacks will be against the Red side from the Black side; however, this doesn't rule out data exfiltration from misuse of the Red side. Any security procedures produced as a result of an assessment based on this Security Characteristic should reflect this.

6. By extension, this document will refer to Red and Black virtual machines, network cards, networks, data, etc, according to which security domain they are in.

7. The assumption is that the virtualisation product is separating (and hence protecting) virtual machines in the Red security domain from attacks coming from a (compromised) Black security domain. However, it is also assumed that a virtualisation product provides symmetric protection unless otherwise noted; CESG advice should be sought in cases where symmetrical protection is a requirement (for example, where the two security domains are RESTRICTED and PROTECT MEDICAL and the data owners are particularly concerned about attacks in both directions) and the product does not offer symmetric protection.

8. In some cases, a virtualisation product might be set up to have more than two security domains (such as UNCLASSIFIED, PROTECT STAFF, and RESTRICTED). Detailed guidance on these cases cannot be given in a document such as this, but a

rough guide would be to treat the intermediate security domains as being on the Red side of anything less sensitive, and on the Black side of anything more sensitive, so they are appropriately protected from the other security domains. In other words, any pair of security domains considered in isolation should be treated as Black and Red with respect to each other.

9. Despite the above, the host software is not considered to be its own security domain; instead, it is treated separately, to make the document clearer.

10. This document contains the mitigations for server virtualisation. This is typically distinguished by a need for unattended running and remote access by multiple users. There is a companion document available for client virtualisation, and a virtualisation product can be certified against either or both. In the case of a virtualisation product that is not clearly one or the other (such as one that involves frequent interactive access, like a client, as well as unattended running and remote access, like a server), it will need to be certified against both Security Characteristics.

11. In the event of doubt, it is recommended that the requirements for both types of virtualisation are read, even for a product that is intended for only one type of virtualisation, as this can provide useful guidance.

B. Typical Use Cases

12. The typical use case for server virtualisation is the consolidation of multiple physical servers in different security domains onto a single platform. By using virtualisation to reduce the number of physical servers, cost savings can be made, both in the number of machines that need to be bought, as well as in running and maintenance costs. This will usually involve server-grade hardware, with some or all storage provided by a remote storage device (such as a SAN), and server administration performed using remote tools. There may be multiple users accessing the platform at the same time.

Excluded Use Cases

13. For the moment, cross-domain solutions (where a virtual machine is connected to more than one security domain) are specifically excluded.

14. Data sharing is similarly excluded, though it remains acceptable to use existing approaches to transfer data (for example, passing data from one security domain to an external cross-domain solution, and then returning it to the other security domain). The specific example of writing to removable media, unmounting that media, and then remounting it in the other security domain, is permitted provided the data owners have evaluated the risks of importing malware or leaking data, and have agreed how they are going to handle the risks.

C. Expected Operating Environment

15. It is assumed the hardware and the virtualisation product are enterprise-managed and supported. This can be interpreted flexibly: for example, it does not

preclude the management and support being done by another department under agreement.

D. Compatibility

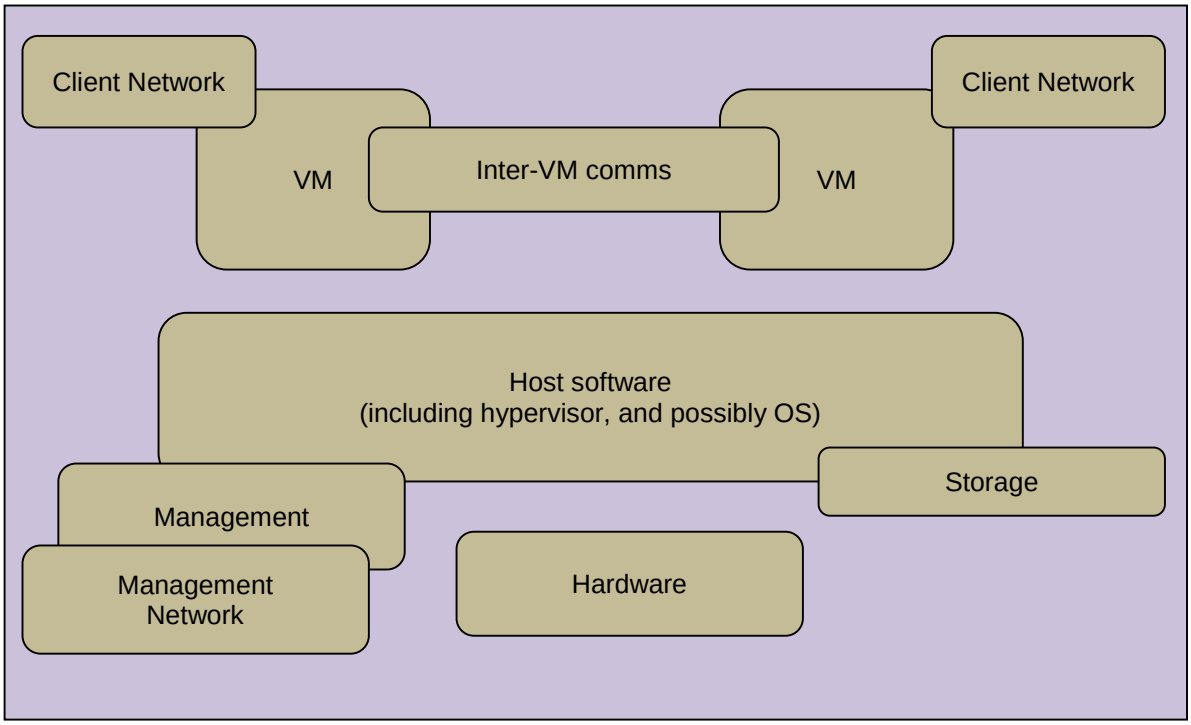
16. These Security Characteristics are intended for products running on a 32-bit or 64-bit x86 platform that supports hardware virtualisation extensions for both the processor (for example, Intel VT-x or AMD-V) and the memory (for example, Intel EPT or AMD RVI). Products aimed at other hardware platforms may still be able to make use of these Security Characteristics with appropriate changes.

17. It is expected that any product implementing server virtualisation will not require the use of a special operating system in the virtual machines. In other words, it must support one or more Guest OSes currently used within the public sector, and must not impose undue restrictions on moving to newer OSes.

E. Interoperability

18. This document should be read in conjunction with CESG Good Practice Guide no. 12 (reference [a]), which provides over-arching guidance on the use of virtualisation. The current version of the Good Practice Guide, issue 1.2, pre-dates the CPA scheme, but it will shortly be updated.

F. High Level Functional Components



19. The above diagram shows the host software (a hypervisor in the case of bare metal virtualisation, but potentially also including an operating system in the hosted case) running on top of the physical host (the hardware). There is storage (such as a local hard disk, or a SAN), and some form of management software (either on the

same platform, or attached to a management network). Virtual machines (VMs) run on the host software, connect to each other through other communication links (labelled ‘Inter-VM comms’), and will have connections to their own networks.

20. The generic term for the part of the host software that runs the virtual machines is a Virtual Machine Manager, or VMM, with a ‘hypervisor’ being a minimal VMM used in some bare metal implementations. However, mixing VMM and VM in the same document, together with some commercial uses of VMM to mean something slightly different, make using VMM potentially confusing. As a result, in common with GPG12 (reference [a]), this document uses ‘hypervisor’ to refer to all forms of host software used to run virtual machines, even though this is not strictly correct.

21. Certain virtualisation products transfer some of the functionality of the host software to one or more special-purpose VMs (for example, a ‘driver VM’ may be used to manage device access, and hence the device drivers, for some of the host devices). Since these special purpose VMs are being used to provide functionality for the host software, for the purposes of this document such VMs are treated as part of the host software. Specifically, mitigations that refer to VMs or Guest OSes do not include these special-purpose VMs, whereas they are included in mitigations that refer to the host software or services (as appropriate).

22. For example, a special-purpose VM used for introspective scanning of other VMs is not covered by the requirements on inter-VM connectivity, but is covered by the requirements on providing services to VMs in multiple security domains.

G. Future Enhancements

23. CESG welcomes feedback and suggestions on possible enhancements to this Security Characteristic.

24. Future enhancements to this Security Characteristic may include support for virtualisation-aware devices such as network cards.

II. SECURITY CHARACTERISTIC FORMAT

25. All CPA Security Characteristics contain a list of mitigations which are split into three requirement categories: development, verification and deployment requirements. Within each of these sets the mitigations can be grouped based on areas of the product (as illustrated in the High Level Functional Component Diagram above), such as bulk encryption or authentication, or they may be overarching requirements which apply to the whole product. Reference [b] describes how evaluation teams should interpret Security Characteristics.

26. The three types of mitigations are denominated as follows:

- **DEV** – These are mitigations that are included by the developer during the design or implementation of the product. These are validated via a review of the product's design or implementation during a CPA evaluation.

- **VER** – Verification mitigations are specific mitigations that the evaluator must test during the assessment of the product.

- **DEP** – Deployment mitigations are points that must be considered by users or administrators during the deployment of the product. These mitigations are incorporated into the security procedures for the product.

27. Each mitigation includes informational text in italics, describing the threat that it is expected to mitigate. It also lists at least one specific mitigation, which describes what must actually be done to achieve that requirement. In some cases there is additional explanatory text which expands upon these requirements.

28. In the requirements listed below, the following terminology can be used:

- 'Must', 'Mandatory' and "Required" are used to express a mitigation that is essential. All mitigations and detailed mitigations are mandatory unless there is an explicit caveat, such as 'if supported by the product'.

- 'Should' and 'Strongly Recommended' are used whenever a requirement is highly desirable, but is not essential. These are likely to become mandatory in future iterations of the Security Characteristic.

- 'Could' and 'Recommended' are used to express a non-mandatory requirement that may enhance security or functionality.

29. For example:

DEV.M1: [A mitigation]

This mitigation is required to counter [a threat]

At Foundation Grade the product must [**do something**].

This can be achieved by [**explanatory comment**].

At Augmented Grade the product is required to [**do something**]

This can be achieved by [**explanatory comment**].

30. An Augmented grade requirement may say that 'the {product, evaluator, deployment} need not do anything additional'. This normally indicates that the Foundation grade mitigation is considered sufficient at Augmented grade; however, CESG reserve the right to re-examine any such mitigation based on the higher standard of evidence required at Augmented grade. For example, a mitigation that was accepted at Foundation based on black box testing may have its source code examined for security flaws.

31. Because the requirements are generic and virtualisation is a complex subject, some of the requirements may not apply to every possible product. For example, DEV.1.M340 refers to ASLR: this is usually a valuable security technique, but it offers little value to code that doesn't use libraries, which is typical of a type 1 hypervisor. CESG does not expect ASLR to be applied where it would provide no security benefit. On the other hand, some of the supporting software for the hypervisor could benefit from ASLR, as could a type 2 hypervisor, in which case it should be used.

III. REQUIREMENTS

A. Design Mitigations

DEV.M203: Limit availability of potential covert channels

This mitigation is required to counter the exploitation of a covert channel.

At Augmented Grade the product is required to seek to minimise covert channels.

A covert channel is any mechanism that can be subverted to transfer information in a way that violates the security policy. This includes, among other things, timing attacks, and passing data in the unused fields of protocols. This covers both data exfiltration, and being able to deduce useful information by passive observation.

There is no assumption that the developer will successfully find and block every possible covert channel; the requirement is for the developer to show they have considered this form of attack and taken steps to prevent the more obvious ones (for example, ensuring that unused fields in protocols are set to a specific default value).

DEV.1 - Design >> Host software

DEV.1.M41: Crash reporting

This mitigation is required to counter exploitation of a software implementation error

At Foundation Grade the product is required to ensure crashes are logged.

Where it is possible that sensitive data may end up in the crash data, this must be handled as red data and must only be available to an administrator. Crash data from both the product and the underlying operating system must be considered.

At Augmented Grade the product need not do anything additional.

DEV.1.M42: Heap hardening

This mitigation is required to counter exploitation of a software implementation error

At Foundation Grade the product is required to use the memory management provided by the operating system. Products should not implement their own heap.

At Augmented Grade the product need not do anything additional.

DEV.1.M43: Stack protection

This mitigation is required to counter exploitation of a software implementation error

At Foundation Grade the product is required to be compiled with support for stack protection in all libraries, where the tool chain supports it.

If more recent versions of the tool chain support it for the target platform then they should be used in preference to a legacy tool chain.

At Augmented Grade the product need not do anything additional.

DEV.1.M44: Data validation on untrusted input

This mitigation is required to counter exploitation of a software implementation error

At Augmented Grade the product is required to perform validation on data derived from untrusted sources.

The checks should consist of common best practice, including range checks for integers and length checks for strings/buffers. All data from external sources should be assumed invalid until checked.

DEV.1.M159: Update product

This mitigation is required to counter exploitation of a software logic error

This mitigation is required to counter exploitation of a software implementation error

At Foundation Grade the product should support the use of software updates.

At Augmented Grade the product need not do anything additional.

DEV.1.M179: Use CPU virtualisation extensions on the host

This mitigation is required to counter raising privilege in the Guest OS by the exploitation of a bug in software virtualisation techniques

At Foundation Grade the product is required to use hardware support for virtualisation.

This includes, for example, Intel VT-x and AMD-V. Note that this is part of the hardware requirements, meaning that only platforms that provide hardware support may be used.

At Augmented Grade the product need not do anything additional.

DEV.1.M180: Use CPU virtualisation memory handling extensions on the host

This mitigation is required to counter the exploitation of a bug in memory handling

At Foundation Grade the product is required to use hardware support for virtualisation memory handling.

This includes, for example, Intel Extended Page Tables and AMD Rapid Virtualisation Indexing. Note that this is part of the hardware requirements, meaning that only platforms that provide hardware support may be used.

At Augmented Grade the product need not do anything additional.

DEV.1.M184: Protect SMM access

This mitigation is required to counter the exploitation of SMM.

At Foundation Grade the product is required to prevent VMs accessing SMM on the host.

This includes preventing a VM from triggering an SMI on the host.

At Augmented Grade the product need not do anything additional.

DEV.1.M190: Protect DMA access

This mitigation is required to counter the exploitation of DMA access.

At Foundation Grade the product is required to prevent VMs from directly performing DMA.

This simply means that a virtual machine must not be able to directly program DMA on the host. This is to stop a virtual machine using DMA to gain access to host memory it is not authorised to access. It is acceptable for the virtual machine to trigger existing DMA provision on the host.

At Augmented Grade the product is required to prevent VMs from programming devices to perform DMA.

The additional requirement for Augmented Grade is that it also restricts the ability of a VM to get a device to perform DMA on its behalf. As with Foundation grade, this refers to the VM being able to fully control the DMA, not triggering existing DMA on the devices.

DEV.1.M191: A VM must have no access to the I/O of another VM

This mitigation is required to counter an attacker gaining access to the I/O of a VM.

At Foundation Grade the product is required to prevent a VM from directly accessing any input or output of another VM.

At Augmented Grade the product need not do anything additional.

DEV.1.M240: Deny access to sensitive information on a context switch

This mitigation is required to counter an attacker retrieving information about the previous context on a context switch.

At Foundation Grade the product is required to prevent VMs from reading sensitive information about other VMs.

This includes memory, CPU (and other) caches, stacks, etc.

At Augmented Grade the product need not do anything additional.

DEV.1.M253: No old information about a device must remain after it is reassigned to a different security domain

This mitigation is required to counter the exploitation of device reassignment.

At Foundation Grade the product is required to clear any sensitive information related to a device when it is re-assigned.

This includes memory, CPU (and other) caches, stacks, etc. It does not include data in persistent storage (such as that stored on a disk), because access to that is covered by other requirements.

At Augmented Grade the product need not do anything additional.

DEV.1.M267: Provide an automated configuration tool to enforce required settings

This mitigation is required to counter exploitation of an accidental misconfiguration

At Foundation Grade the product is required to be provided with a configuration tool, or other method, for an administrator to initially set it up into a suitable configuration.

If the product requires more than 12 options to be changed or set by an administrator to comply with these Security Characteristics, the developer must supply a tool or policy template which helps the administrator to achieve this in fewer steps.

At Augmented Grade the product is required to provide a tool, or other method, for an administrator to verify that their configuration conforms to CPA Augmented.

If the product requires more than 12 options to be checked by an administrator to comply with these Security Characteristics, the developer must supply a tool which helps the administrator to achieve this requirement.

DEV.1.M273: Implement access controls on memory

This mitigation is required to counter the unauthorised reading of data from memory.

This mitigation is required to counter the unauthorised modification of data in memory.

This mitigation is required to counter an attack from the Black VM to the Red VM.

At Foundation Grade the product is required to employ access controls to prevent unauthorised access to memory.

At Foundation grade, this refers to normal platform access controls (such as different memory spaces), such that VMs have no direct access to the memory of other virtual machines or the hypervisor.

At Augmented Grade the product need not do anything additional.

DEV.1.M321: Data Execution Protection

This mitigation is required to counter exploitation of a software implementation error

At Foundation Grade the product is required to support Data Execution Protection (DEP) when enabled on its hosting platform and must not opt out of DEP.

If the product is to be specifically deployed on a platform that does not support either Software DEP or Hardware-enforced DEP, there is no requirement for DEP compatibility.

At Augmented Grade the product need not do anything additional.

DEV.1.M340: Address Space Layout Randomisation

This mitigation is required to counter exploitation of a software implementation error

At Foundation Grade the product is required to be compiled with full support for ASLR, including all libraries used.

ASLR may be disabled for specific aspects of the product, provided there is justification of why this is required.

At Augmented Grade the product need not do anything additional.

DEV.1.M350: A device driver does not share or transfer data belonging to different security domains

This mitigation is required to counter the exploitation of shared drivers.

At Foundation Grade the product is required to apply access controls on any shared device driver to keep data from one security domain from being access by another.

At Augmented Grade the product is required to use different instances of device drivers for each security domain.

DEV.1.M353: Ensure product security configuration can only be altered by an authenticated system administrator

This mitigation is required to counter unauthorised alteration of product's configuration

At Foundation Grade the product is required to ensure that only administrators are able to change the product's security enforcing settings .

The only security enforcing setting a user should be able to change is their passphrase.

At Augmented Grade the product need not do anything additional.

DEV.1.M355: Secure software delivery

This mitigation is required to counter installation of malware on host

This mitigation is required to counter installing compromised software using the update process

At Foundation Grade the product should be distributed via a cryptographically protected mechanism, such that the authenticity of software can be ensured.

Initial code for the product, and any subsequent updates, must be distributed in such a way that tampering is cryptographically detectable. The recipient of the software must be able to ensure the identity of the originator (i.e. vendor).

At Augmented Grade the product is required to be distributed via a cryptographically protected mechanism.

All installation files, executable binaries and configuration data must be signed using Operating System provided mechanisms.

DEV.1.M356: Protect host services access

This mitigation is required to counter the exploitation of a host service.

At Foundation Grade the product is required to ensure VMs can only access authorised host services.

'Host services' includes Guest OS services handled by the host, and all interfaces between a VM and the host (such as hypercalls).

At Augmented Grade the product need not do anything additional.

DEV.2 - Design >> Storage

DEV.2.M177: Protect the disk image

This mitigation is required to counter the modification of the disk image.

This mitigation is required to counter the unauthorised reading of data from a disk image.

This mitigation is required to counter an attacker gaining access to a backup.

At Foundation Grade the product is required to use access controls to protect access to the disk image.

At Augmented Grade the product need not do anything additional.

DEV.2.M213: A Red VM must not be able to access stored Black data

This mitigation is required to counter a delayed attack through Black data stored on the Red network.

At Foundation Grade the product is required to have access controls to prevent a Red VM accessing stored Black data.

At Augmented Grade the product is required to ensure Red & Black storage is separated.

This means either (1) having the separation under the control of the virtualisation software and assured as part of the assessment, (2) using storage hardware assured at Augmented Grade for such separation, or (3) using separate connections to separate storage devices for Red and Black.

B. Verification Mitigations

VER.M173: Test the robustness of drivers.

This mitigation is required to counter the exploitation of a driver for virtual hardware

This mitigation is required to counter the exploitation of a paravirtualised driver for virtual hardware

At Foundation Grade the evaluator will confirm that the developer has run robustness tests on all drivers, and that they have passed.

For example, Microsoft provides 'Driver Verifier', as well as testing tools in the Windows Driver Kit (WDK), which could be used to test the robustness of a driver.
Clearly, drivers that fail such tests should not be used.

At Augmented Grade the evaluator will undertake fuzzing of the driver API.

VER.1 - Verify >> Host software

VER.1.M272: Test access controls on memory

This mitigation is required to counter an attack from the Black VM to the Red VM.

This mitigation is required to counter the unauthorised modification of data in memory.

This mitigation is required to counter the unauthorised reading of data from memory.

At Foundation Grade the evaluator will stress-test memory access.

At Foundation grade, all that is expected is that a memory test utility is run in one VM and shown to have no significant effect on another VM.

At Augmented Grade the evaluator will undertake fuzzing of the memory access APIs.

VER.1.M347: Verify update mechanism

This mitigation is required to counter installing compromised software using the update process

At Foundation Grade the evaluator will validate the developer's assertions regarding the suitability and security of their update process.

The update process must provide a mechanism by which updates can be authenticated before they are applied.
The process and any configuration required must be documented within the Security Procedures.

At Augmented Grade the evaluator need not do anything additional.

C. Deployment Mitigations

DEP.M172: Limit the use of paravirtualised drivers.

This mitigation is required to counter the exploitation of a paravirtualised driver for virtual hardware

At Foundation Grade the deployment is required to remove all unused paravirtualised drivers.

At Augmented Grade the deployment is required to only use a paravirtualised driver if the pure virtual driver is not sufficient.

DEP.M221: Protect the system from unauthorised physical access

This mitigation is required to counter an attacker stealing or damaging the system.

At Foundation Grade the deployment is required to restrict physical access to authorised staff.

This should be based on the approach in IS1 (reference [c]).

At Augmented Grade the deployment need not do anything additional.

DEP.M274: Mitigate the risk of running one virtualisation product on another if both are operating at multiple security domains

This mitigation is required to counter the exploitation of an internal cascade.

At Foundation Grade the deployment is required to use different Foundation grade virtualisation products to reduce the risk of a cascade exploit.

Using different products at least means that an attacker must find an exploit in each one, though this may not dramatically increase the difficulty.

At Augmented Grade the deployment is required to avoid layering one virtualisation product within another.

At Augmented grade, the level of protection provided by layering virtualisation products is no longer considered adequate. If it must be done, at most one virtualisation product is considered to contribute to security, with the others being used for administrative or technical convenience. The virtualisation product closest to the hardware layer must be treated as the only virtualisation layer enforcing security, as if all the virtual machines were running on it.

DEP.M349: Mitigate the risk of using several virtualisation products on connected networks to avoid a network cascade

This mitigation is required to counter the exploitation of a networked cascade.

At Foundation Grade the deployment is required to use different Foundation grade virtualisation products to reduce the risk of a cascade exploit.

Using different products at least means that an attacker must find an exploit in each one, though this may not dramatically increase the difficulty.

At Augmented Grade the deployment is required to avoid deploying a virtualisation product if it would cause a network cascade.

At Augmented grade, the 'high' side of one virtualisation product must not be connected to the 'low' side of another virtualisation product. See GPG12 (reference [a]) for further details.

DEP.M354: Do not rely on hardware independence between VMs

This mitigation is required to counter the exploitation of the loss of hardware independence.

At Augmented Grade the deployment is required to check it does not have an availability requirement for two or more pieces of hardware to be physically independent.

If it does have such a requirement, the deployment will need to be designed to maintain it, or else virtualisation should not be used.

For example, a system might be specified as requiring two physically separate machines, because the impact level of a failure of availability would be high. Subsequently virtualising those two machines as two virtual machines on the same piece of physical hardware would undermine that requirement.

Clearly, it is acceptable to maintain such physical independence using physically independent virtualisation products; this mitigation is concerned with the loss of such physical independence.

DEP.1 - Deploy >> Client Network

DEP.1.M262: Protect the virtualised management interfaces

This mitigation is required to counter an attacker accessing the management interface of a VM.

At Foundation Grade the deployment is required to logically separate the VM's management interface.

This Security Characteristic is required because the management interface of the VM will usually have to use the same client network as the virtual machine, so it needs good separation. Typically, this would involve running the management interface over an appropriate grade of VPN.
It is not required if the management interface of the VM is able to directly connect to its own network, though this is likely to be unusual.
Note that this refers to the management interface of (services running on) the VM, not how the virtualisation software manages the VM.

At Augmented Grade the deployment need not do anything additional.

DEP.1.M263: A VM must not be connected to networks in different security domains

This mitigation is required to counter the exploitation of a VM linked to networks in more than one security domain.

At Foundation Grade the deployment is required to not connect a VM to networks in different security domains.

At Augmented Grade the deployment need not do anything additional.

DEP.1.M269: Positively identify the VM

This mitigation is required to counter one VM masquerading as another VM.

At Foundation Grade the deployment is required to enable mutual authentication on all remote inputs.

This could be via an authenticated link over TLS, or SSH, or any other technology that allows both the server and the user accessing it to be authenticated. It is not required for connections that are only used for output (so it is not necessary to convert all web servers to TLS, for example), although it might be a good idea given the possibility of the output being spoofed.

At Augmented Grade the deployment need not do anything additional.

This can be achieved by configuring the Guest OS appropriately, or by features provided by the virtualisation software.

DEP.2 - Deploy >> Management

DEP.2.M193: Control the creation and restoration of VMs, including from snapshots.

This mitigation is required to counter an attacker rolling a VM back to a vulnerable snapshot.

This mitigation is required to counter tricking the system into creating or restoring a VM under the control of the attacker.

At Foundation Grade the deployment is required to restrict the creation and restoration of VMs to virtualisation administrators.

At Augmented Grade the deployment need not do anything additional.

DEP.2.M222: Apply controls to VM migration

This mitigation is required to counter an attacker migrating a VM to a machine under their control.

At Foundation Grade the deployment is required to ensure that migration can only be done by virtualisation administrators.

At Augmented Grade the deployment is required to ensure that migration can only be done to authorised machines.

DEP.2.M223: Control access to the management interface

This mitigation is required to counter a Black-side virtualisation administrator accessing the Red-side.

At Foundation Grade the deployment is required to use role-based security on the management console.

At Augmented Grade the deployment is required to ensure all virtualisation administrators are cleared for the Red side.

DEP.2.M238: Protect physical access to the management network

This mitigation is required to counter an attack through the management network.

At Foundation Grade the deployment is required to limit physical access to the management network.

This can be achieved by denying unauthorised physical access to the management network (thus preventing an unauthorised person connecting a computer to it), or by using some system of machine authentication (such as a TPM) to restrict network access to pre-authorised machines only.

At Augmented Grade the deployment is required to allow only authorised machines on the management network.

This refers to using some system of secure machine authentication to restrict network access to pre-authorised machines only, not something easily spoofed (such as MAC addresses).

DEP.2.M239: Separate the management network

This mitigation is required to counter an attack through the management network.

At Foundation Grade the deployment is required to treat the management network as a segregated Red network, or as a separate network altogether.

Note that a special VM for managing the host is considered part of the host software and as such must only be connected to the management network, not the regular red client network. Similarly, an ordinary VM must not be connected to the management network.

At Augmented Grade the deployment need not do anything additional.

DEP.2.M271: Only virtualisation administrators can deploy or migrate VMs

This mitigation is required to counter the modification of VMs during VM deployment or migration.

At Foundation Grade the deployment is required to restrict VM deployment and migration to virtualisation administrators.

Only virtualisation administrators may deploy or migrate VMs. For automated deployment or migration, this is met by restricting the configuration to virtualisation administrators.

This is a restriction on who can actually perform deployment or migration, not on who can use a VM after it has been deployed.

At Augmented Grade the deployment need not do anything additional.

DEP.3 - Deploy >> Inter-VM Comms

DEP.3.M251: A VM must not connect to a VM in another security domain

This mitigation is required to counter the exploitation of a link from one VM to a VM in another security domain.

At Foundation Grade the deployment is required to forbid connections between VMs in different security domains.

The definition of 'connections' is deliberately left undefined. It does not just mean networks, but any way of passing data from one VM to another.

At Augmented Grade the deployment need not do anything additional.

DEP.4 - Deploy >> Storage

DEP.4.M208: Apply quotas to files created by the Guest OS

This mitigation is required to counter the filling up of storage by writing files from the Guest OS.

At Foundation Grade the deployment is required to employ quotas on all file-systems holding virtual disk files.

At Augmented Grade the deployment is required to use thick-provisioned virtual disks on at least the Red side to prevent space exhaustion.

They can be used on the Black side as well as a precaution.

DEP.4.M209: Throttle local log files

This mitigation is required to counter an attacker making log files grow excessively.

At Foundation Grade the deployment is required to allocate and maintain adequate space for local log files to grow.

'Maintain' implies that the log files are monitored, and action taken if they threaten to outgrow the space available. It is clearly acceptable to achieve this by restricting the ability of log files to grow beyond a particular size (for example, by aging off old entries), but this approach is not required at Foundation grade.

At Augmented Grade the deployment is required to prevent local log files from growing beyond a maximum size.

This could include aging off old entries, provided precautions are taken against attackers generating enough log entries to conceal their activities.

DEP.4.M248: Restrict access to removable media

This mitigation is required to counter the exploitation of media access to work around VM restrictions.

At Foundation Grade the deployment is required to record the protective marking of removable media, and instruct users on correct handling.

The typical problem is that of a user writing to the removable media from one VM and then reading from another VM in a different security domain, without following the correct procedure (such as virus-scanning) for such a cross-domain transfer.

At Augmented Grade the deployment is required to avoid the use of removable media except when operationally required.

DEP.5 - Deploy >> VM

DEP.5.M212: Only a suitably authorised user can change the power state of a VM

This mitigation is required to counter an attacker triggering a VM shutdown.

At Foundation Grade the deployment is required to restrict changes in a VM's power state to specifically authorised users.

A 'specifically authorised user' isn't further defined, and is up to the deployment. It could range from a virtualisation administrator to all users, depending on how the system is deployed. For example, the user of client virtualisation on a laptop needs the ability to shut down their VMs, whereas it may be appropriate to limit the ability to shut down a major server running in a VM to a subset of the staff permitted to administer it.

At Augmented Grade the deployment need not do anything additional.

DEP.5.M234: Follow good administration practices

This mitigation is required to counter the exploitation of a bug in the Guest OS or an application

This mitigation is required to counter an attacker using existing Guest OS privileges.

At Foundation Grade the deployment is required to administer the virtual machine as if it was a physical one.

For example, system and software updates, auditing, anti-virus, application of good security practices, and user account administration must all be handled with the same processes and rigour as if the virtual machine was a separate physical machine.

At Augmented Grade the deployment is required to apply the CESG GAP, or equivalent, to the Guest OS.

DEP.5.M249: Confirm the entropy available to the network encryption is sufficient.

This mitigation is required to counter the exploitation of any loss of entropy in the Guest OS leading to insecure network encryption.

At Foundation Grade the deployment is required to use an external entropy source, or use the NIST tests on the raw entropy data to confirm that the entropy being produced within the VM is sufficient.

In this context, 'external' means that the entropy was generated from some reliable source of entropy outside the VM (and possibly outside the platform altogether). This includes solutions where the network encryption is terminated outside the VM (for example, using a TLS concentrator).
The issue is that the usual sources of entropy on a physical machine (such as disk timings) may not provide the same amount of entropy once virtualised, and the loss of entropy will weaken encryption that relies on it.
If a choice of network encryption has already been validated for use in a virtual machine, there is no need to re-test it.
See reference [d] for the NIST tests.

At Augmented Grade the deployment need not do anything additional.

DEP.5.M268: Disallow auto-mounting in the Guest OS

This mitigation is required to counter the exploitation of the auto-mounting of a device in the Guest OS.

At Foundation Grade the deployment is required to prevent removable storage devices from being automatically mounted.

This also includes devices other than drives that have a storage capability: they must not be automounted, to prevent any attack based on writing to the device from one VM and auto-mounting it from another.

Note that this refers to auto-mounting in the Guest OS, not the initial mounting of storage devices by the host software when the VM is turned on.

At Augmented Grade the deployment need not do anything additional.

DEP.6 - Deploy >> Host software

DEP.6.M38: Use automated configuration tool

This mitigation is required to counter exploitation of an accidental misconfiguration

At Foundation Grade the deployment is required to be configured using automated tools if provided.

At Augmented Grade the deployment is required to periodically check product configuration to ensure that it conforms to CPA requirements using a vendor provided tool if available.

DEP.6.M39: Audit log review

This mitigation is required to counter exploitation of a software logic error

This mitigation is required to counter exploitation of a software implementation error

At Foundation Grade the deployment is required to regularly review audit logs for unexpected entries.

At Augmented Grade the deployment need not do anything additional.

DEP.6.M131: Operating system verifies signatures

This mitigation is required to counter installation of a malicious privileged local service

At Foundation Grade the deployment is required to enable signature verification for applications, services and drivers in the host operating system, where supported and where the product makes use of it.

At Augmented Grade the deployment need not do anything additional.

DEP.6.M159: Update product

This mitigation is required to counter exploitation of a software logic error

This mitigation is required to counter exploitation of a software implementation error

At Foundation Grade the deployment is required to update to the latest version where possible.

At Augmented Grade the deployment need not do anything additional.

DEP.6.M175: Access controls on auditing and logs

This mitigation is required to counter the disabling of auditing

This mitigation is required to counter the unauthorised modification of logs

At Foundation Grade the deployment is required to restrict access to auditing controls and log files to virtualisation administrators.

At Augmented Grade the deployment is required to check daily that all logging and auditing of the virtualisation product is still enabled.

This check can be automated, as long as errors are brought to the notice of an administrator.

DEP.6.M176: Follow auditing guidance

This mitigation is required to counter an attacker exploiting inadequate auditing

At Foundation Grade the deployment is required to implement the guidance in GPG13.

See reference [e].

At Augmented Grade the deployment is required to implement the guidance in GPG13, being aware that GPG13 may impose stricter requirements than would be the case for Foundation grade.

DEP.6.M187: Minimise the host services attack surface

This mitigation is required to counter the exploitation of a host service.

At Foundation Grade the deployment is required to turn off all services available on the host that are not used for virtualisation or supporting features.

This also means that, in the case of hosted virtualisation, the host should not be used for other purposes while it is hosting virtual machines in two or more security domains.

At Augmented Grade the deployment need not do anything additional.

DEP.6.M189: Data on a device must only be accessible to one VM at a time

This mitigation is required to counter linking security domains through a shared device.

At Foundation Grade the deployment is required to configure shared devices so that only VMs in the same security domain can access each data item.

VMs in the same security domain are allowed to share data items, but there must be no sharing between security domains. Generally, this should be interpreted as meaning that no unassured device that can store data may be used by VMs in different security domains. Devices are only permitted to store data from multiple security domains if they have been approved to do so (for example, access is controlled by the virtualisation product itself). Specifically, LUN-masking in an unassured SAN is not sufficient by itself.

At Augmented Grade the deployment need not do anything additional.

DEP.6.M210: Restrict the ability to change the power state of the host from a VM

This mitigation is required to counter an attacker changing the power state of the host.

At Foundation Grade the deployment is required to restrict changes to the power state of the host from within a VM to authorised users.

Changes to the power state include shutting down or suspending the host. 'Authorised users' is not further defined, and is up to the deployment.

At Augmented Grade the deployment need not do anything additional.

DEP.6.M211: Confirm update source before download

This mitigation is required to counter a denial-of-service attack using a large, fake update.

At Foundation Grade the deployment is required to identify server(s) providing updates in a secure way.

For example, identify the update server using TLS with signed certificates, and checking the signatures.

At Augmented Grade the deployment need not do anything additional.

DEP.6.M235: Minimise host services that are visible to different security domains

This mitigation is required to counter the exploitation of a host service.

At Foundation Grade the deployment is required to create separate instances of services provided to different security domains.

In other words, no service should cross-connect different security domains. This includes, for example, a malware-scanning service that can introspect into VMs: if this can introspect into VMs in different security domains, an attacker may be able to compromise the malware scanner to access the other security domain.

At Augmented Grade the deployment need not do anything additional.

DEP.6.M250: The host software must not pass data between networks in different security domains

This mitigation is required to counter data being passed between networks in different security domains.

At Foundation Grade the deployment is required to prevent the host from passing data between networks in different security domains.

It is acceptable for information about network traffic to be logged on the management network, provided the traffic itself is not routed directly to the management network.

At Augmented Grade the deployment need not do anything additional.

DEP.6.M255: All network configuration changes must be done by a red-side virtualisation administrator

This mitigation is required to counter an attacker changing which network a VM is connected to.

At Foundation Grade the deployment is required to use role permissions to limit network configuration changes to Red-side virtualisation administrators only.

At Augmented Grade the deployment is required to only allow Red-side virtualisation administrators access to management functions.

In other words, all managers of the virtualisation product must be fully cleared for the data being processed on it; it is not acceptable at Augmented Grade to give insufficiently cleared staff access to some management functions, relying on role permissions to prevent them having access to any other functions.

DEP.6.M257: Configure resource limits

This mitigation is required to counter a VM refusing to release a resource.

This mitigation is required to counter the overloading of system resources.

This mitigation is required to counter an attack from the Black VM to the Red VM.

At Foundation Grade the deployment is required to ensure the host software and all essential VMs have guaranteed resources.

This will prevent either the host software or essential VMs from being denied necessary resources. Note that host software will include any 'special VMs' needed for the proper functioning of the product.

At Augmented Grade the deployment is required to ensure all non-essential VMs also have limits on the resources they can use.

DEP.6.M264: Protect any out-of-band management technology

This mitigation is required to counter a compromise of the out-of-band management technology through a remote attack.

At Foundation Grade the deployment is required to passphrase-protect access to any out-of-band management technology.

Out-of-band management is also known as Lights-out management.

CESG passphrase advice can be found in reference [f].

At Augmented Grade the deployment is required to use signed certificates to control access to any remote management technology, and check the signatures.

DEP.6.M340: Address Space Layout Randomisation

This mitigation is required to counter exploitation of a software implementation error

At Foundation Grade the deployment is required to enable ASLR in the host Operating System where available.

At Augmented Grade the deployment need not do anything additional.

DEP.6.M348: Administrator authorised updates

This mitigation is required to counter installing compromised software using the update process

At Foundation Grade the deployment is required to confirm the source of updates before they are applied to the system.

The administrator is required to have authorised the updates before use. If an automatic process is used, the administrator must also configure the product to authenticate updates.
The administrator is required to use the update process described within the Security Procedures.

At Augmented Grade the deployment need not do anything additional.

IV. GLOSSARY

32. The following definitions are used in this document:

Term	Meaning
AMD-V	AMD's processor virtualisation extensions
ASLR	Address Space Layout Randomisation
Bare-metal virtualisation	The virtualisation software runs directly on the hardware (i.e. the 'bare metal').
Black, Black-side	The less sensitive security domain, which is typically assumed to be the source of an attack.
Cascade	A cascade occurs when two (or more) virtualisation products are used together to link a wider range of security domains. This can be internal (running one virtualisation product inside another) or across a network (linking the Red VM in one product to the Black VM in another). See reference [a] for further details.
CPA	Commercial Product Assurance.
DEP	Data Execution Prevention (as well as indicating a Deployment mitigation)
DMA	Direct Memory Access
EPT	Extended Page Tables, Intel's technology for virtualising memory access.
GAP	Government Assurance Pack
Host	The physical machine used for the virtualisation, comprising the hardware and the host software.
Hosted virtualisation	The virtualisation software runs on top of (i.e. is hosted by) an operating system, usually a general-purpose one.
Hypervisor	The part of a software product that directly controls the virtual machines; the Virtual Machine Manager.
LUN	Logical Unit Number
Paravirtualised driver	A driver that is virtualisation-aware and works with the host software to offer improved performance, but with the risk of widening the attack surface of the host software.
Red, Red-side	The more sensitive security domain, which is typically assumed to be the target of an attack.
RVI	Rapid Virtualisation Indexing, AMD's technology for virtualising memory access.
Security Characteristic	A standard which describes necessary mitigations which must be present in a completed product, its evaluation or usage, particular to a type of security product.
Security Domain	One or more virtual machines that share a common threat model.
SMI	System Management Interrupt, used on x86 processors to enter SMM (see below).
SMM	System Management Mode, a special highly-privileged mode on x86 processors, originally intended for the control of critical hardware (such as the CPU fan).
TNC	Trusted Network Connect

Term	Meaning
VM	Virtual Machine.
VMM	Virtual Machine Manager
VPN	Virtual Private Network
VT-x	Intel’s processor virtualisation extensions