Australian Government
Department of Finance and Deregulation
Australian Government Information Management Office

Whole-of-Government

Common Operating Environment Policy

Document Version Control

Document name	***Project Plan***
Organisation:	Department of Finance and Deregulation
Project:	WofG COE
Document status:	Official Release
Version No:	2.0
File name:	WofG COE Policy v2.0.docx
Date:	13th December 2011

Document Revision History

Version	***Date of Issue***	***Author***	***Reason for Change***
1.0	26/11/2010	Mark Croonen Coralie Volgyesi	Initial Release
1.2	5 April 2011	Leanne Chaplin	Update ISM Reference
2.0	13th December 2011	Leanne Chaplin Paul Ketelaar	2011 Policy Review

DOCUMENT OWNER: Director, Common Operating Environment, Agency Services Division.

Table of Contents

WHOLE OF GOVERNMENT COMMON OPERATING ENVIRONMENT POLICY

Common Operating Environment

Introduction / Background

1. To drive greater efficiency and transparency across Australian Government operations, the government has established a coordinated procurement contracting framework to deliver efficiencies and savings from goods and services in common use by Australian Government Departments and Agencies subject to the Financial Management and Accountability Act (FMA Act 1997).

2. The Whole of Government (WofG) Common Operating Environment (COE) was identified by the Desktop Scoping Study (Recommendation 2) as a critical element in driving future savings in services provisioning and increasing the flexibility and responsiveness of government operations.

3. In October 2009, the Government agreed to the development of a Whole of Government Common Operating Environment Policy. This policy is expected to:

    a. Optimise the number of desktop Standard Operating Environments (SOE) consistent with meeting the Government's business objectives;
    b. Improve agency ability to share services and applications; and
    c. Support the Government's e-Security Policy.

4. On October 16, 2009, the Secretaries' ICT Governance Board (SIGB) approved the ICT Customisation and Bespoke Development Policy. Among other aims, this policy is expected to increase opportunities to standardise government business processes and systems.

5. The WofG COE Policy complements the ICT Customisation and Bespoke Development Policy by standardising and decreasing the number of desktop operating environments to be supported across Government. As of June 2010, there were a more than 186 separate SOE images built with different components, standards and technologies.

Goals

6. **Optimise the number of desktop SOE images**
   To meet the Government's business objectives, defined common standards in hardware and software will reduce the number of SOE images required to support business needs. In turn, this will reduce the cost of SOE development and maintenance.

7. **Support the Government's e-Security Policy**
   The COE will mandate a common desktop security configuration to be used across agencies; this will improve the level of security across agency networks. Industry partners will be provided with a consistent baseline to make application design more consistent across agencies and inherently more secure.

8. **Improve Agency ability to share services and applications**
   By using the agreed common standards, agencies will be able to share services and reduce the need for duplication. Lead agencies will be in a position to implement an application or service, which can then be reused by other government agencies.

9. The COE will enable agencies to respond more quickly to changing technology cycles, facilitating more cost-effective upgrades and supporting a move to more rapid adoption cycles, enhancing agency and government agility

Principles

10. The principles relate to the goals of the policy. They are enduring and should not require modification as technology changes.

11. Both the COE policy and principles are designed to be complementary to other policies. The COE Policy leverages principles defined by the cross agency services architecture[1] and the Government's principles for the Reuse of Software and other ICT Assets.

12. **Common and agreed standards**
    The COE will be based on common standards; where practical these will be based on open standards. Common standards will facilitate component reuse and the sharing of resources.

13. **Meets agency business requirements**
    The COE must be flexible enough to meet the requirements of all the agencies. It must also be capable of supporting multiple unique SOEs if there is a unique business requirement.

[1] http://www.finance.gov.au/Publications/cross-agency-services-architecture-principles/index.html

14. **Secure**
    The COE must be secure on all levels and it must provide confidentiality, integrity and availability. Any procedures defined by the COE must have clear accountability and must be auditable. The COE Policy (subject to the Information Security Manual (ISM) and the Protective Security Policy Framework (PSPF)) is applicable across all classification levels (e.g., unclassified through to Top Secret).

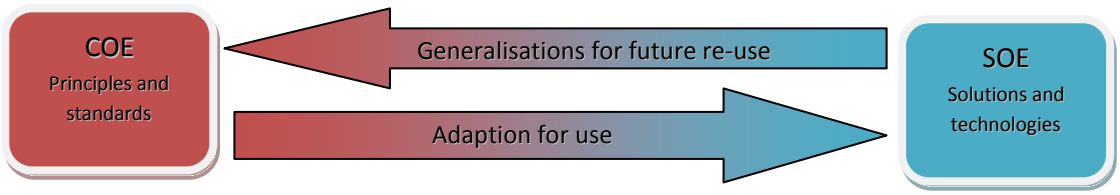
15. **Supportable**
    All components used must be supportable to ensure the COE remains reliable and stable. Support must be readily available and cost efficient. The supporting skill sets must also be readily available.

16. **Complies with legislative requirements**
    The COE will comply with all relevant legislative requirements.

Composition

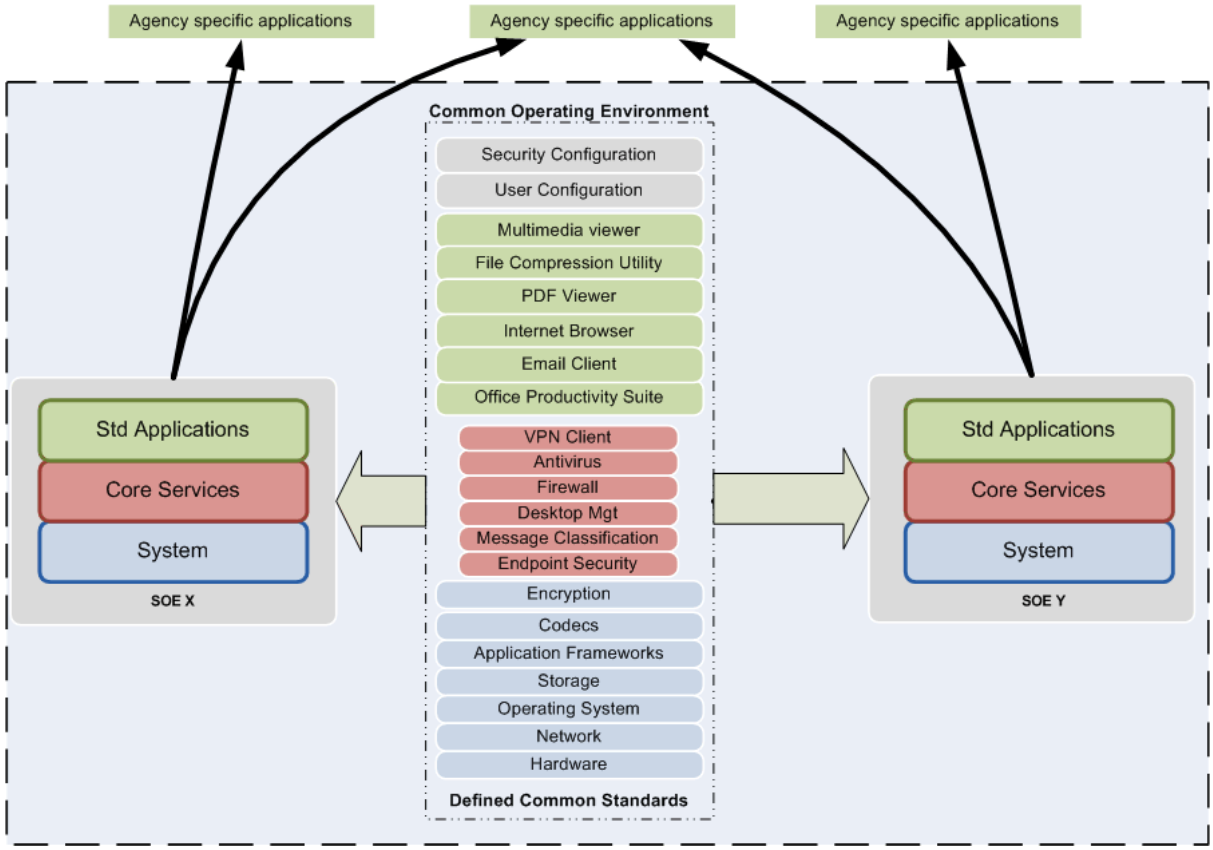
17. The WofG Common Operating Environment is to be based on principles that are supported by the standards. The use of common standards promotes interoperability, provides common functionality and supports a consistent user experience. These standards will be applied to all SOEs regardless of how the desktop environment is delivered. E.g. Desktop, thin-client or desktop virtualisation.

18. The COE can accommodate multiple SOEs. The COE policy defines the principles and standards while the SOE identifies the solutions and technologies.



19. The COE principles and standards are documented as part of the policy. Each SOE will be built in accordance with platform specific build documentation, which will detail how the standards are instantiated for each platform.

20. A SOE is a specific solution based on the COE. It is comprised of an operating system, core services, a standard application set, a defined security configuration and a defined user configuration.



COE Composition

21. The **System** is defined as the layer of the SOE that the end user does not directly interact with, but is used to support the layers above such as the core services and standard applications.
22. **Core services** are services that are exposed to the user to perform a function, but do not manipulate or modify the user's data.
23. **Standard applications** are generic applications which can be used to view, manipulate or save data.
24. Agency specific applications are used to deliver specific business needs. Agencies are responsible for the licensing and maintenance of these applications, as they are not considered part of the COE.

Standards

25. A component which is listed as 'MANDATORY' must be included in the SOE image and built in accordance with the platform specific build documentation.

26. Optional components do not have to be included in the SOE image but, if included, must be built in accordance with the platform specific build documentation.

Category	Component	Standard	Effect
Configuration Data	Security Configuration MANDATORY	a. Workstations should be configured to ensure unneeded software, operating system components and hardware functionality or features are removed or disabled. b. By default, users are not to have accounts which grant them privileged access to the system. Privileged access to systems must be granted in accordance with the ISM c. Where possible, the configuration must be centrally managed and not applied at the local system level d. The configuration must be endorsed by DSD e. Must support logging as defined by the section on page 16 of this policy f. The application of security patches or other security maintenance activities must take precedence over energy saving considerations g. Must support centralised operating system patching	a. Workstations are to be hardened in accordance with the Software Security Chapter in the ISM Controls Manual. b. The Access Control Chapter of the ISM Controls Manual defines privileged access and supports the use of separate accounts where privileged access is required. c. The security configurations will be specified by AGIMO and endorsed by DSD
	User Configuration MANDATORY	a. Must support a consistent user experience regardless of the delivery mechanism b. All configurations should be in line with the best practice as defined in the platform specific guidelines c. Where possible the configuration must be centrally managed and not applied at the local system level d. Unnecessary functionality in the user interface is removed for the purpose of improving system performance. ICT green guidelines need to be taken into consideration in configuration of the user environment	a. The modular build standards mean that the same user experience can be delivered regardless of whether the user is on a desktop or virtual client b. Where practical the user configuration will be defined in the platform specific guidelines to promote a consistent look and feel across agencies c. Agencies should seek to standardise on common user applications to promote a consistent user experience across the agencies d. The user configuration should support settings which reduce power consumption, such as the use of blank screen savers
Standard Applications	Multimedia Viewer	a. Must be capable of supporting at least one of the endorsed codecs	a. Agencies should ensure that the multimedia viewer can support the preferred video, audio and DVD playback

Category	Component	Standard	Effect
		b. Must comply with Application Management as defined by the section on page 15 of this policy c. Must have endorsed security settings applied as defined by the section on page 16 of this policy	codec b. Agencies need to ensure that applications/systems do not have hardcoded dependencies which would prevent the multimedia viewer complying with N-1 application management
	File Compression Utility	a. Must be compatible with the Zip file format version 6.3 of the standard as outlined by PKware b. Compression utilities should be configured to ensure that the zip file format is the default format c. Must comply with Application Management as defined by the section on page 15 of this policy d. Must have endorsed security settings applied as defined by the section on page 16 of this policy	a. Unicode file names and content are supported in the version 6.3 of the PKware standard b. To promote compatibility between agencies where a compression utility is used, it should be configured to use the zip file format as the default
	PDF Viewer	a. Must comply with Application Management as defined by the section on page 15 of this policy b. Must support the Open PDF file format as defined by ISO/IEC 32000-1:2008 c. Must have endorsed security settings applied as defined by the section on page 16 of this policy	a. Agencies need to ensure that applications/systems do not have hardcoded dependencies which would prevent the PDF viewer complying with N-1 application management
	Internet Browser	a. Must be able to be centrally managed and configured b. Must not allow end user to install unauthorised add-ins c. Must comply with Application Management as defined by the section on page 15 of this policy d. Must have endorsed security settings applied as defined by the section on page 16 of this policy	a. Users should not be able to configure their browsers by installing unapproved add-ins or toolbars
	Email Client	a. Must be able to work offline b. Any offline cache data must be stored in accordance	a. A user must be able to read and draft email while disconnected from the corporate network

Category	Component	Standard	Effect
		with the security classification of that data. c. Must support messaging protocols securely and in accordance with the ISM. d. Must support shared calendars and contacts e. Must have endorsed security settings applied as defined by the section on page 16 of this policy f. Must comply with Application Management as defined by the section on page 15 of this policy	b. Offline mail cache must be stored appropriately to ensure it cannot be accessed by unauthorised persons
	Office Productivity Suite	a. Must support the Office Open XML format as defined by ECMA 376 1st Edition and/or ISO/IEC 29500:2008 standards b. Must comply with Application Management as defined by the section on page 15 of this policy c. Must have endorsed security settings applied as defined by the section on page 16 of this policy	a. The intention is to standardise on a file format to facilitate the exchange of information between agencies. This does not preclude the use of other file formats. b. An agency's office suite must have the ability to read and write the endorsed file format. c. Agencies need to ensure that applications/systems do not have hardcoded dependencies which would prevent the Office Productivity Suite complying with N-1 application management
Core Services	VPN Client	a. All requirements for encryption must be in accordance with the Cryptography Chapter in the ISM Controls Manual b. Two factor authentication should be used where possible	a. Two factor authentication should be seen as essential for users connecting from a third party network
	Antivirus MANDATORY	a. Must support automated deployment b. Must not rely only on pattern based detection methods c. Must prevent end users stopping the service d. The Antivirus solution can be resident in a subsystem such as a hypervisor e. Must support centralised administration, signature/engine updates/reporting f. Must NOT ask the users permission to report scanning	a. The client must be able to be installed after the deployment of the base image b. Pattern based detection only provides protection on known viruses and does not counter the threat from zero day attacks c. Where the client is virtualised the Antivirus solution may be installed at the hypervisor level for ease of management

Category	Component	Standard	Effect
		results or install updates g. Must support logging as defined by the section on page 16 of this policy	
	Firewall MANDATORY	a. Must be capable of preventing unauthorised inbound and outbound connections b. Must be supported by central management and configuration c. Must prevent end users stopping the service d. Firewall must be able to change its configuration automatically based on location e. Must support logging as defined by the section on page 16 of this policy f. Firewalls should be able to manage network connections from the application level	a. Refer to the Software Security Chapter in the ISM Controls Manual - Installation of software based firewalls limiting inbound and outbound network connections b. If the firewall solution incorporated into the operating system meets the required standards it should be used. This will reduce complexity and costs and will be updated as part of the operating system c. Network connections should be able to be managed from the application level rather than only filtering on the address and port. For example iexplore.exe should be allowed to communicate out to <address>:80 rather than just allowing any application to communicate out to <address>:80
	Desktop Management	a. Must support automated deployment b. Must support remote desktop connectivity for support staff c. Must support notification of active remote desktop sessions d. Must have the ability to collect asset/configuration information e. Must support logging as defined by the section on page 16 of this policy	a. The client must be able to be installed after the deployment of the base image b. Unless there is a legal reason, users should be notified of when their desktop session is being accessed by a third party
	Message Classification	a. Must support the Australian Email Protective Marking Standard	

Category	Component	Standard	Effect
	End Point Security	a. Must support automated deployment b. Must support central configuration c. Must support the disabling of external ports such as USB, eSata or Firewire to selected user groups d. Must support the disabling of optical drives for both read and write e. Must support the prevention of unauthorised installation of USB devices such as scanners and cameras f. Must support the prevention (and reporting) of the installation of unauthorised USB mass storage devices such as USB thumb drives g. Must be able to record all activity in audit logs which cannot be modified h. Must support logging as defined by the section on page 16 of this policy	a. The client must be able to be installed after the deployment of the base image
The System	Encryption	a. All requirements for encryption must be in accordance with the Cryptography Chapter in the ISM Controls Manual	a. Where desktop/laptop encryption is required the preferred solution must support at a minimum this level of encryption
	Codecs	a. Must support a codec capable of video playback as defined by the MPEG-4 part 2 standard b. Must support a codec capable of audio playback as defined by the MPEG-1 or MPEG-2 Audio Layer 3 standard c. On systems with an optical drive, must support a codec capable of DVD playback	a. When developing new applications or upgrading legacy applications agencies should use the preferred codecs to promote interoperability b. Additional codecs may be installed as required

Category	Component	Standard	Effect
	Application Frameworks	a. Must be in vendor support b. Must comply with Application Management as defined by the section on page 15 of this policy c. New systems should not have hard coded dependencies on a framework	a. Agencies should only support N-1 in their environment. The principle of N-1 is to reduce the complexity and the support requirement for the environment b. Legacy applications which have a need for an older framework outside of N-1 should have the required framework deployed as part of the application and not as part of the SOE c. New systems or applications should only have a requirement for an N-1 framework. As part of the implementation, maintenance of the new system needs to be factored in so the system will continue to work with the future states of N-1 in the environment
	Storage	a. Data on local hard drives and portable media must be stored in accordance with its security classification b. Storage of information on local drives is to be avoided	a. Data should not be stored on the local systems
	Operating System MANDATORY	a. The operating system must be procured in accordance Commonwealth Procurement Guidelines and in accordance with Whole-of-Government ICT policies including the ICT Customisation and Bespoke Development Policy b. Must be capable of supporting the principles outlined in this policy c. Patches for the OS must be able to be deployed remotely without interaction from end users d. Agencies should adhere to effective patching policies that take into account system importance, patch testing and patch severity e. Must have a 64 bit architecture version available f. ICT green guidelines need to be taken into consideration in configuration of the operating system	a. Agencies must first consider an operating system that is a supported COTS product. Any Non COTS solutions must have minimal customisation and there must be an ability to purchase commercial support for the distribution b. Where common operating systems are used, similar build standards, frameworks should be used to allow the sharing of data and packaged applications c. Agencies are encouraged to deploy the 64 bit versions of their preferred operating system d. Operating systems must be able to minimise power consumption by supporting settings such automatic shutdown and sleep mode e. Standard applications are approved as part of the COE and Agencies are responsible for the approval of their

Category	Component	Standard	Effect
		g. Power considerations should not impact the deployment of patches h. Must support logging as defined by the section on page 16 of this policy i. Only applications approved by an appropriate Agency authority are to be deployed j. Deployed applications are to be installed in defined locations only k. Users must not have write permission to directories that software is executed from l. Must have endorsed security settings applied as defined by the section on page 16 of this policy m. Desktop operating systems and installed software must support IPv6	own additional business applications. Applications are to be installed in defined locations, for example, in Program Files, not a users home directory f. Users may not have write permission to software executable directories. This prevents users from executing arbitrary or malicious software and bypassing any White listing capability if implemented g. IPv6 must be supported by the desktop operating system and installed software h.
	Network MANDATORY	a. Must support the WofG Internet Protocol Version 6(IPv6) Strategy	a. Network interfaces must support IPV6
	Hardware	a. All hardware must comply with minimum specifications as outlined by the Desktop Hardware panel b. Hardware must support the Green ICT guidelines	a. All desktops need to be procured in accordance with the WofG Desktop Hardware panel

Application Management

27. To maintain consistency and reduce complexity, all applications used as part the COE (the System, Core Services and Standard Applications) must be the current and supported version (known as N) or its immediate predecessor (known as N-1). N refers to the major version of an application, e.g. version 2.x is N, version 1.0 or 1.1 are N-1. This will ensure all applications are supported and by allowing the N-1 version gives the agency flexibility to plan required upgrades.

28. Support for existing or legacy applications should be structured so dependencies such as codecs and application frameworks are tied to the application and not the SOE. This will support a modular design of the SOE and ensure that the SOE can be maintained in accordance with the N-1 application management principle. To support the modular design agencies should consider the use of virtualisation to decouple legacy applications from the SOE. The form of virtualisation best suited for an agency will be dependent on factors such as the infrastructure and the network bandwidth available.

29. As the agencies converge on the COE standards, it is expected that the need for the virtualisation of legacy applications will be reduced.

30. To ensure the desktop environment remains consistent, application updates should be pushed by a centrally managed distribution mechanism. Applications which are installed on the desktop should not be configured to pull updates from external sources, such as vendor websites. Client based update services such as these should be disabled or not installed. The updating of anti-virus signatures or configuration files is not considered to be an application update.

31. To facilitate application white listing where possible, applications must be installed in the locations as detailed in the specific system build documentation for each platform.

32. Application Whitelisting must be used to help prevent unapproved applications from running.

Software Packaging

33. To support the goal of agencies being able share services, the packaging of software should be managed so an application can be packaged once and reused many times. Agencies should look to use application virtualisation to achieve this. Virtualisation may reduce the number of distribution methods required and make it possible for agencies to share packaged applications.

Security and User Configurations

34. All standard products will have defined security configurations based on DSD's and the vendor's recommendations. Configuration settings will be specified by AGIMO and endorsed by DSD.

35. The security and user configurations for each operating system platform will be detailed in the specific system build documentation for each platform. This will represent the minimum requirements for the environment with agencies able to add configurations to meet their requirements.

36. Agency specific security and end user configurations may be applied on top of the COE configurations; however, they must not decrease or weaken the level of security provided by the base COE configurations.

Logging

37. To ensure legal and security requirements are met in accordance with the ISM and NAA "Administrative Functions Disposal Authority, Technology and Telecommunications" policy, Agencies must have a logging policy which clearly defines:
    a. what events they capture
    b. why the events need to captured
    c. how long the logs will be stored for

38. Log details should include:
    a. date/time of event
    b. user details
    c. workstation details
    d. event message and relevant details

39. Logs should be kept for the following categories:
    a. security configuration
    b. anti-virus, firewall
    c. desktop management
    d. end point security
    e. operating system functions to include:
        - privileged operations and access
        - log on/log off events
        - failed authentication attempts
        - system/application security alerts.

40. To ensure data integrity, Agencies should use a configuration of either remote logging or the transfer of local event logs to a central server. The use of centralised logging does not preclude the logs also remaining resident on their local systems.

Governance

Understanding and Complying with the WofG COE Policy

41. This Policy applies to all FMA Act Agencies. It is also available to Commonwealth Authority and Companies (CAC) Act Agencies and the States and Territories.

42. It is the responsibility of all FMA Act Agencies to ensure they understand and comply with this Policy.

43. Agencies must ensure their environment remains compliant with the policy as published at the time it was developed. Agencies must also remain compliant with future releases of the policy.

44. Compliance with the COE standards will be monitored and conducted by Agencies, with these results to be incorporated into the AGIMO annual benchmark reports.

Related policies and initiatives

45. The COE policy is supported by and complements the following policies and initiatives:

    a. Section 44(1) of the Financial Management and Accountability Act 1997 (FMA Act) requires all Government Departments to use available resources in an efficient, effective and ethical manner.

    b. "Strategies to Mitigate Targeted Cyber Intrusions". This policy addresses the top four priorities identified in this list and several others.

    c. The COE policy addresses the first requirement of the governance requirements as identified in schedule 1 of the ICT Customisation and Bespoke Development policy

    d. Process for Administration of Opt-Outs from Whole-of-Government Arrangements

    e. Australian Government Information Security Manual

    f. Green ICT guidance list, the COE will support the Green ICT guidance list. All SOE images built in accordance with the COE policy must implement the relevant configuration settings as outlined in the Green ICT guidance list

    g. National Security Information Environment Roadmap, the COE policy provides common standards to deliver a secure desktop environment and promotes interoperability between agencies

    h. Strategy for the Implementation of IPv6 in Australian Government Agencies

Actions arising from policy breaches

46. Breaches which are assessed to be against policy rather than security breaches will be referred to the relevant agency for action in accordance with local disciplinary procedures.

47. Breaches that impact security will be addressed as identified below.

48. Unlawful access to, alteration of or unauthorised disclosure of information held by the Commonwealth, by Departmental officials or other persons is subject to the sanction of criminal law. Section 70 of the Crimes Act 1914 covers the protection of official information and Section 79 deals with the protection of official secrets. Breaches may result in imprisonment.

49. For Penalties under the Criminal Code Act 1995, please refer to Operational Guidelines 7.3 Protective Security, Section 18, Misuse of IT&T Resources and Sanctions

50. For actions resulting from the loss or improper use of public property, please refer to Operational Guidelines 9.6 Incidents Involving Commonwealth Officials.

51. Members of staff who become aware of security incidents or violations must report them to their agency's service desk, the IT Security Adviser (ITSA) or the Agency Security Adviser (ASA) in accordance with their agency's procedures.

Opt Out

52. This policy is subject to the process for administration of opt-outs from Whole-of-Government arrangements.

53. Initial opt-out considerations will be factored into the transition plan and are expected to show how alignment to the policy will be achieved as part of the transition plan. Claims for opting out will not be considered during the transition phase.

54. When seeking an opt-out, an agency will need to include a remediation plan to detail how it will return to the WofG COE policy. Opt-outs are limited to a maximum of 3 years, after which the original business case will be reassessed to ensure it is still valid.

55. While it is recognised that agencies may have a need to develop separate SOE images, it is expected that these images will comply with the standards set out for the COE to ensure that agencies can still share data and services in a seamless manner.

Exemptions

56. This Policy is directed at general-purpose systems such as managed desktops and laptops. Embedded computers, process control systems or specialised scientific systems are outside the scope of this policy.

57. Modifications to these exempted systems are to be minimal and they should only deviate from the COE to the extent required to make the device or application functional.

58. Agencies are not required to seek an opt-out for exempted systems as they are automatically excluded from the policy. As part of their annual benchmark reporting, agencies will need to report on the number of excluded systems, the reason for their exclusion and modifications made to the system.

59. All excluded systems are still required to meet security standards as defined in the Information Security Manual (ISM).

60. Agencies may make temporary changes to the configuration baseline if it is required to support a critical agency need. Agencies must inform AGIMO as soon as practical of the changes. AGIMO, in consultation with DSD, will assess the impact of the change and based on the assessment, agencies will be expected to either;

    a. Detail a mitigation strategy for the required change and a timeline for when the agency will be able to conform to the baseline configuration.
    b. Continue with the temporary change until it can be reviewed as part of the normal review cycle, at which point the change will either be accepted into the configuration baseline or the agency will be advised to seek an opt out

Policy Implementation

61. The standards endorsed by this policy come into effect when an agency is ready to deploy a new version of their base SOE. At this time agencies will need to follow their normal application testing regimes and build the SOE in accordance with the standards endorsed by this policy.

62. A new version of the SOE is considered to be an upgrade of the operating system or the deployment of a substantial update such as the release of a service pack.

63. Agencies may choose to integrate aspects of this policy prior to an operating system upgrade and are encouraged to be proactive where ever possible.

Roles and Responsibilities in relation to the COE Policy

64. AGIMO:
    a. All WofG COE Policy instantiation activities. These include:
        - Coordinate, develop and publish the WofG COE Policy
        - Coordinate, develop, build and test the Windows7 SOE (pilot activity)
        - Coordinate, develop and publish the WofG COE Policy Transition Plan
        - Identification of potential WofG software licence options
        - Identification of reporting metrics and inclusion in annual benchmarking activities

    b. Ongoing management and maintenance of the WofG COE Policy, the supporting SOEs and related documentation sets. This includes:
        - Annual reviews of the COE Policy, covering:
            - Coordinating requests for change for the WofG COE Policy
            - Coordinating policy change request reviews
            - Understanding the security implications associated with change requests
            - Testing of proposed baseline configuration changes
            - Recommending changes
            - Updating COE Policy, baseline configuration and documentation as required
            - Publishing updates
        - Identification of SOE standard software with WofG licensing potential
        - Coordination of compliance audits and reporting
        - Endorsement of security configuration and ongoing changes to the security baseline (including security configuration exception/issues resolution)
        - Management and maintenance of the SOE documentation sets and images
        - Provision of policy advice and guidance
        - Availability of baseline configuration and supporting documentation
        - Programming of COE Policy and baseline configuration updates
        - Review of Desktop Hardware panel specifications in conjunction with panel hardware updates

65. WofG COE Working group
    a. Assist and support AGIMO in managing and maintaining the WofG COE Policy. This includes:
        - Definition of COE standards and composition
        - Endorsement of WofG COE Policy and supporting SOE documentation sets
        - Annual review of WofG COE Policy and SOE image requests for change

66. Government Agencies:
    a. Ensuring business specific applications work within the specifications of the COE
    b. Providing feedback to AGIMO on any COE Policy or SOE image related issues (including security configuration settings)
    c. Ensuring policy compliance (including security configurations) is maintained on their networks
    d. Initiating a COE Policy Opt Out request where appropriate
    e. Programming and scheduling of agency upgrades
    f. Inform AGIMO of any emergency changes to the configuration baseline
    g. Provide data as required for the reporting metrics

67. SIGB/CIOC
    a. Endorsement and approval of the COE policy and supporting SOE documentation sets
    b. Review of recommended opt out requests

68. DSD
    a. Review and endorsement of COE security configurations and any proposed changes to the COE security configuration baseline
    b. Assist AGIMO with assessing the security impact of any opt out requests to include
        - Identification of unacceptable risk
        - Identification of acceptable risk mitigation methods

69. Lead Agency
    a. Lead Agencies may be identified to assume some of the AGIMO responsibilities. These may include:
        - Management and maintenance of the SOE documentation sets and images
        - Testing of proposed SOE changes
        - Review and maintenance of SOE images
        - SOE image performance monitoring
        - Testing of SOE images against recommended hardware specifications as defined by the Desktop Hardware procurement panel.

COE Policy Review Cycle

70. The COE standards will be reviewed annually, starting with a call for change requests from agencies in July each year. Requests for changes can be based on business or technology requirements.

71. This will be followed by a two month review period of the requested changes starting in August. The review will be lead by AGIMO and supported by members of the COE working group.

72. The COE standards and the SOE documentation sets will then be revised from October with updates to be released in December.

WofG Common Operating Environment Policy Review	AGIMO	COE WG	Agencies	SIGB/CIOC	DSD	Lead Agency
COE Policy requests for change identified	A/R	C	C		C	C
COE Policy changes reviewed	A/R	R	C/I		C	C
Security implications of changes understood and endorsed	A/R	C	C/I		R	C
Recommended changes tested against baseline configuration	A/R	I	I		C	R
Recommended changes agreed	A/R	R	C/I	I	C	C
Baseline configuration and documentation updated	A/R	I	I		I	R
Changes approved	A/R	C	I	R	I	I
Update COE Policy, baseline configuration and documentation published	A/R	I	I	I	I	I

- **Responsible:** person who performs an activity or does the work.
- **Accountable:** person who is ultimately accountable and has Yes/No/Veto.
- **Consulted:** person that needs to feedback and contribute to the activity.
- **Informed:** person that needs to know of the decision or action.

SOE Implementation Roles

73. Agencies are responsible for all programming and scheduling activities related to their operating system upgrades. AGIMO will provide advice and guidance and access to the SOE images and associated documentation. Testing of business applications is an agency responsibility. Any issues that would require a change to either the COE Policy or SOE image or supporting documentation are to be reported to AGIMO.

WofG Common Operating Environment SOE Implementation	AGIMO	COE WG	Agencies	SIGB/CIOC	DSD	Lead Agency
COE Policy advice and guidance	A/R					
SOE documentation and image availability	A/R	I	I		I	I
Programming of Agency SOE upgrades	C/I		A/R			
Ensuring COE Policy compliance	C/I		A/R			
Testing and management of agency business applications	I		A/R			
Initiation of opt out requests where appropriate	C/I	I	A/R		C/I	
Reporting COE Policy or baseline configuration issues	C/I	I	A/R		C/I	I

- **Responsible:** person who performs an activity or does the work.
- **Accountable:** person who is ultimately accountable and has Yes/No/Veto.
- **Consulted:** person that needs to feedback and contribute to the activity.
- **Informed:** person that needs to know of the decision or action.