

# Operational Activity Decomposition Tree (OV-5a)

---

## **Introduction**

The purpose of this document is to describe the activities of providers, users, and operators of the Information Enterprise (IE) required to meet the operational requirements for the IE described in the Operational Context. Performance of these activities enable an IE that achieves the operational outcomes associated with each of the five core characteristics identified in the Operational Context. These activities and their definitions are based on separate, but related, activity hierarchies taken from the GIG 2.0 ORA v1.5 and DoD IEA v1.2. Activities contained in these two existing documents were aligned, normalized, and then combined to form the activity hierarchy described here.

The OV-5a diagrams in this document show activities only down to the third level of decomposition; the complete OV-5a for the DoD IEA does in fact contain activities to the fifth, and in some cases sixth and seventh, levels of decomposition. The complete OV-5a will be available on a web site in the form of an interactive extract from the Rational System Architect tool used in building this hierarchy. The complete hierarchy is also available in the activity definitions tab of the DoD IEA AV-2 (Integrated Dictionary), which is organized in accordance with the tree structure of the complete OV-5a and so contains definitions for all the activities in the complete OV-5a. The intent here is to provide readers of this document with enough information to understand the scope and context of the activities required to manage, develop, secure, operate, and use the IE. The diagrams in this document are also intended to serve as a tool for navigating the complete (and much more complex) activity decomposition to locate the “leaf-level” activities which they must incorporate into their architectures and with which they must align and/or conform to meet compliance requirements. Users can narrow and improve their searches through the complete activity decomposition by first locating in the diagrams here the areas where those leaf-level activities of interest are likely to reside.

There are several activities within this activity model that may overlap with activities described in enterprise architectures associated with the warfighter, business, and intelligence mission areas. For example, activity A5.2 Provide IA Workforce has counterparts within the Business Enterprise Architecture (BEA). These overlaps will continue to exist until an effective architecture federation method and tool is available to allow the elimination of such redundancies. There is an on-going pilot project co-sponsored by the office of the Deputy Chief Management Officer (DCMO) and the office of the DoD CIO to determine how best to align the BEA and DoD IEA; the intent of this pilot is to determine if existing methods and tools will provide a means to achieve the type of architecture federation required to address this issue.

# Final

## DoD IEA v2.0: OV-5a Operational Activity Decomposition Tree

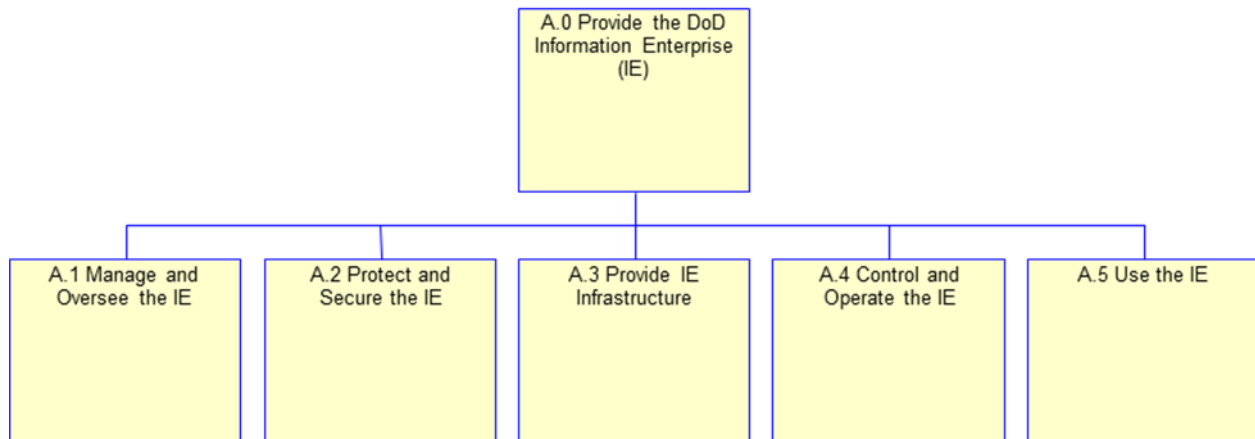
### 36 DoD IEA OV-5a Description

37 As shown in **Figure 1**, there are five main activities performed to ensure a viable information  
38 enterprise for DoD in meeting warfighter, business, and defense intelligence operational  
39 requirements. These activities are:

- 40 • **Manage and Oversee the IE** – This activity governs the development and implementation  
41 of the IE. It establishes and uses those structures and processes required to provide effective,  
42 high-level management and oversight of the components of the IE and its operations. The  
43 activity develops and enforces the required vision, strategy, and guidance to direct the IE so  
44 it meets requirements and applicable law, regulation, and policy (LRP), while at the same  
45 time delivering the capabilities necessary to fully enable net-centric warfighting, business,  
46 and defense intelligence operations for successful mission accomplishment.
- 47 • **Protect and Secure the IE** – This activity develops and implements processes and  
48 mechanisms required to guard critical data, capabilities, the IT infrastructure, and data  
49 exchanges within the IE, while providing authentication and non-repudiation of information  
50 and transactions to enable assurance and trust. It provides the ability to control user access to  
51 data and services, determine vulnerabilities, and prevent the exploitation of these  
52 vulnerabilities by both external and internal threats. The activity enables the monitoring of  
53 IE operations, recognition and assessment of security-related incidents, and selection and  
54 execution of appropriate responses.
- 55 • **Provide IE Infrastructure** – This activity supplies the enterprise-level communications and  
56 computing capabilities required to enable net-centric operations and the Enterprise-wide  
57 services required by all users. It provides basic IT elements/components which are  
58 foundational to the DoD IE and which enable it to fully support assured information sharing  
59 across the Enterprise and with mission partners.
- 60 • **Control and Operate the IE** – This activity implements capabilities required to provide  
61 integrated NetOps in order to enable information access by any user across network and  
62 security domains. It includes processes and mechanisms for Enterprise Management,  
63 Content Management (which includes Records Management), and Network Defense. The  
64 activity enables NetOps to monitor the status and health and direct the actions of DoD IE  
65 resources in support of successful accomplishment of joint warfighting, business, and  
66 defense intelligence missions.

# Final

## DoD IEA v2.0: OV-5a Operational Activity Decomposition Tree



67

68

Figure 1 Key IEA Operational Activities

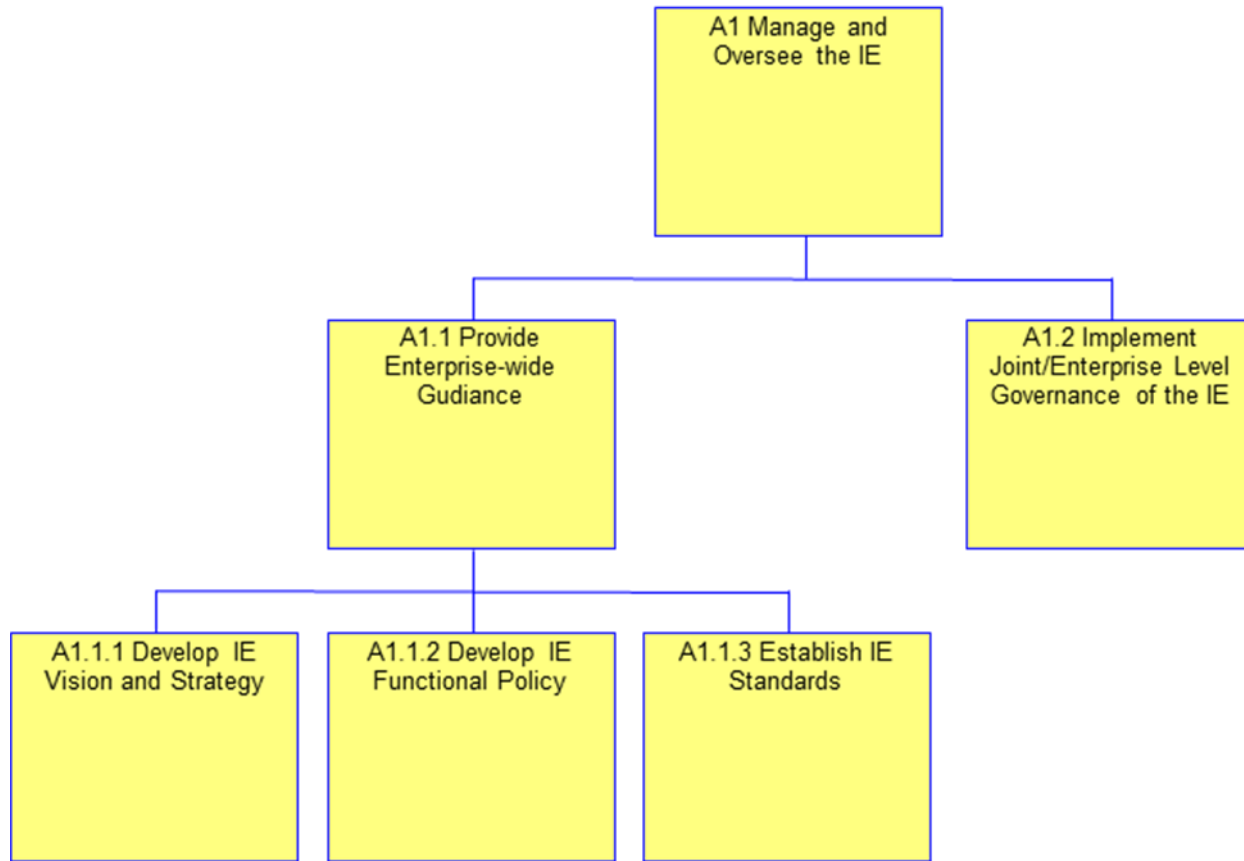
- 69
- **Use the IE** – This activity enables an authorized user to access the IE and use its
  - 70 functionality to easily discover information, services, and applications, regardless of location,
  - 71 and to assess and critique information, services, and applications based on specific needs in
  - 72 order to improve IE capabilities and service. In support of operations, the activity also
  - 73 enables the user to collaborate and share information (which includes data and knowledge)
  - 74 with others.

75 **Figures 2 through 6** show activity decompositions to the third level for each of these key

76 activities. In these separate diagrams, an asterisk (\*) has been placed in any activity box for

77 which additional activity decomposition diagrams exist in the complete OV-5a.

**Final**  
**DoD IEA v2.0: OV-5a Operational Activity Decomposition Tree**

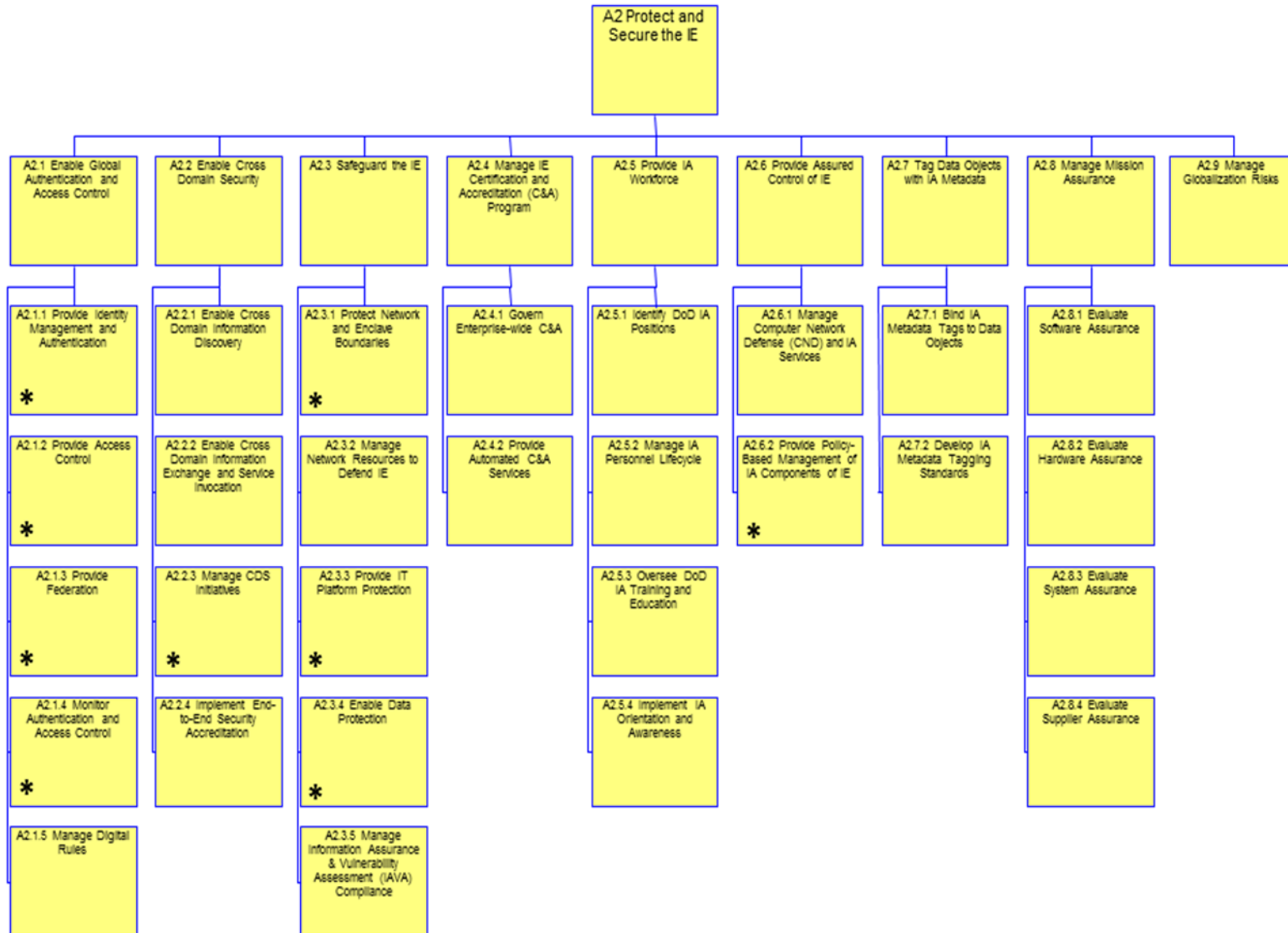


78

79

Figure 2 - Activity Decomposition for Manage and Oversee IE

# Final DoD IEA v2.0: OV-5a Operational Activity Decomposition Tree

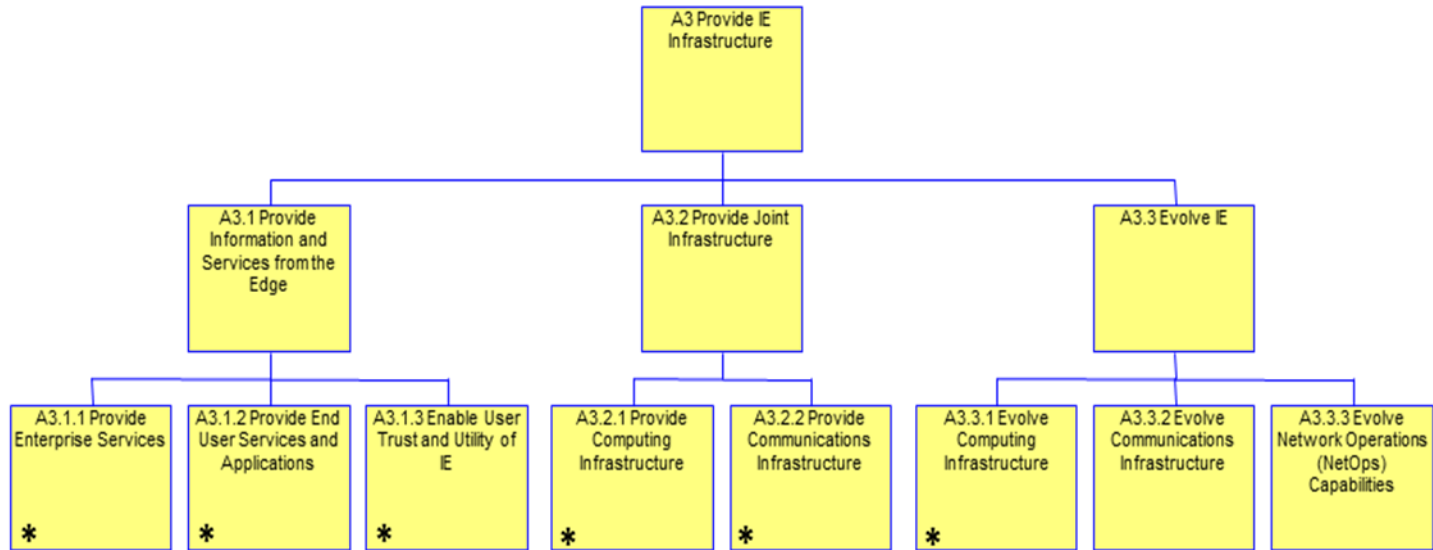


80

81

Figure 3 - Activity Decomposition for Protect and Secure the IE

# Final DoD IEA v2.0: OV-5a Operational Activity Decomposition Tree

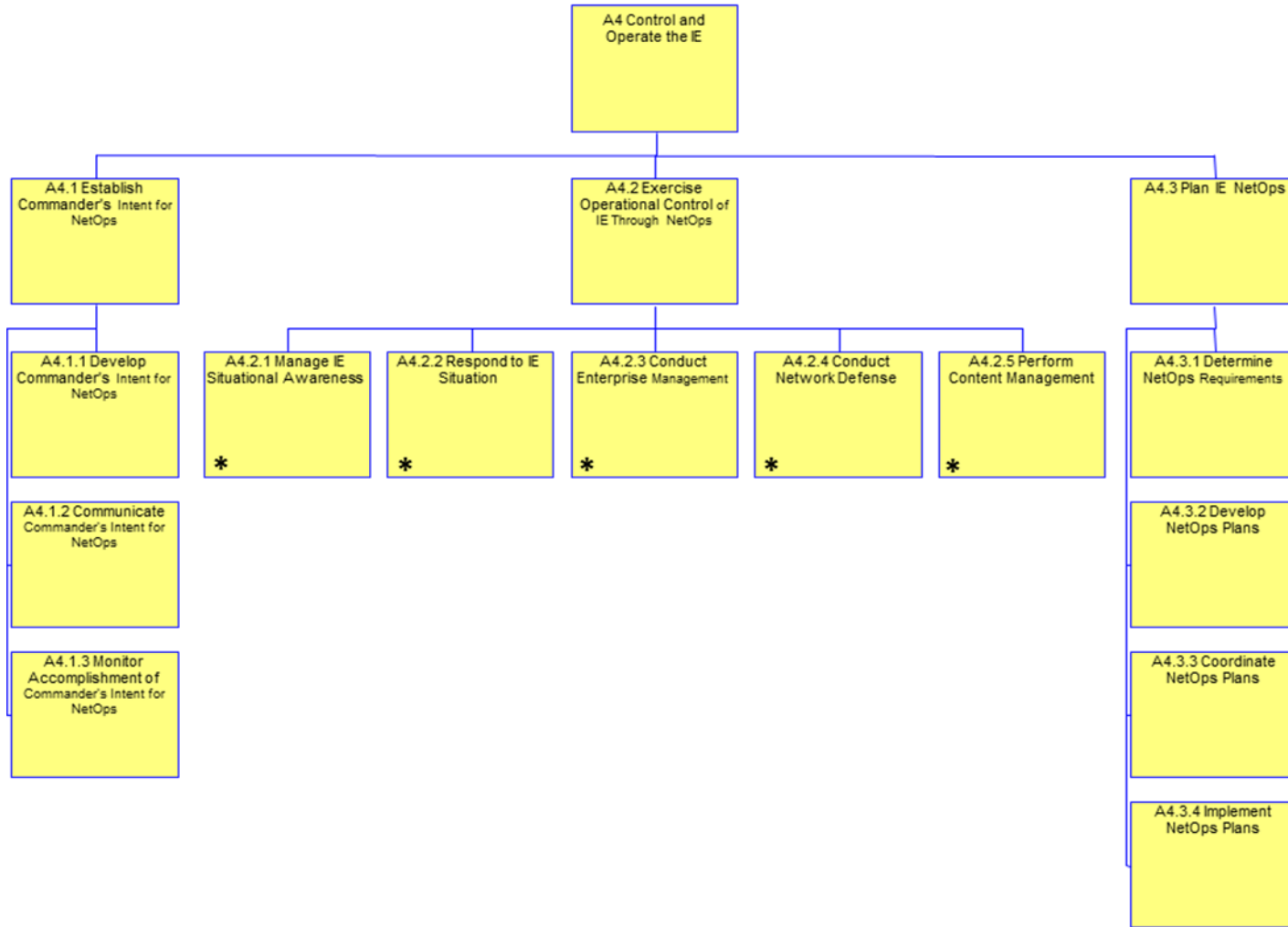


82

83

Figure 4 - Activity Decomposition for Provide IE Infrastructure

# Final DoD IEA v2.0: OV-5a Operational Activity Decomposition Tree



84

85

Figure 5 - Activity Decomposition for Control and Operate the IE

**Final**  
**DoD IEA v2.0: OV-5a Operational Activity Decomposition Tree**

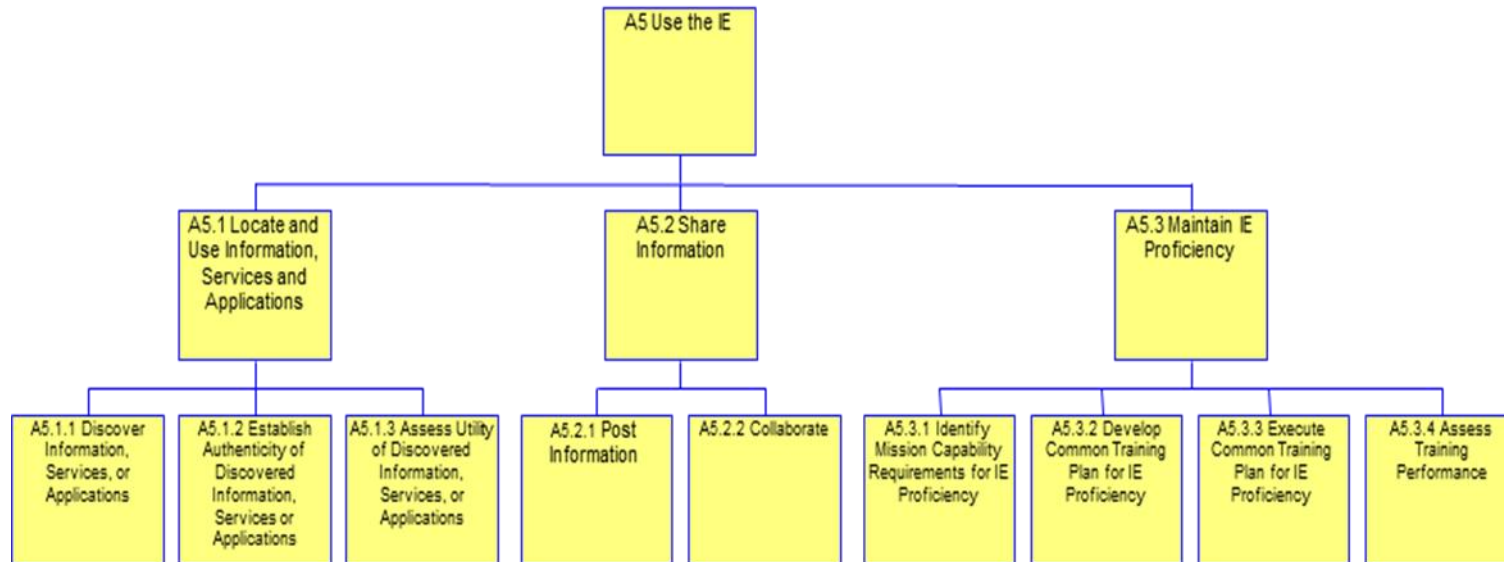


Figure 6 - Activity Decomposition for Use the IE

86

87

88

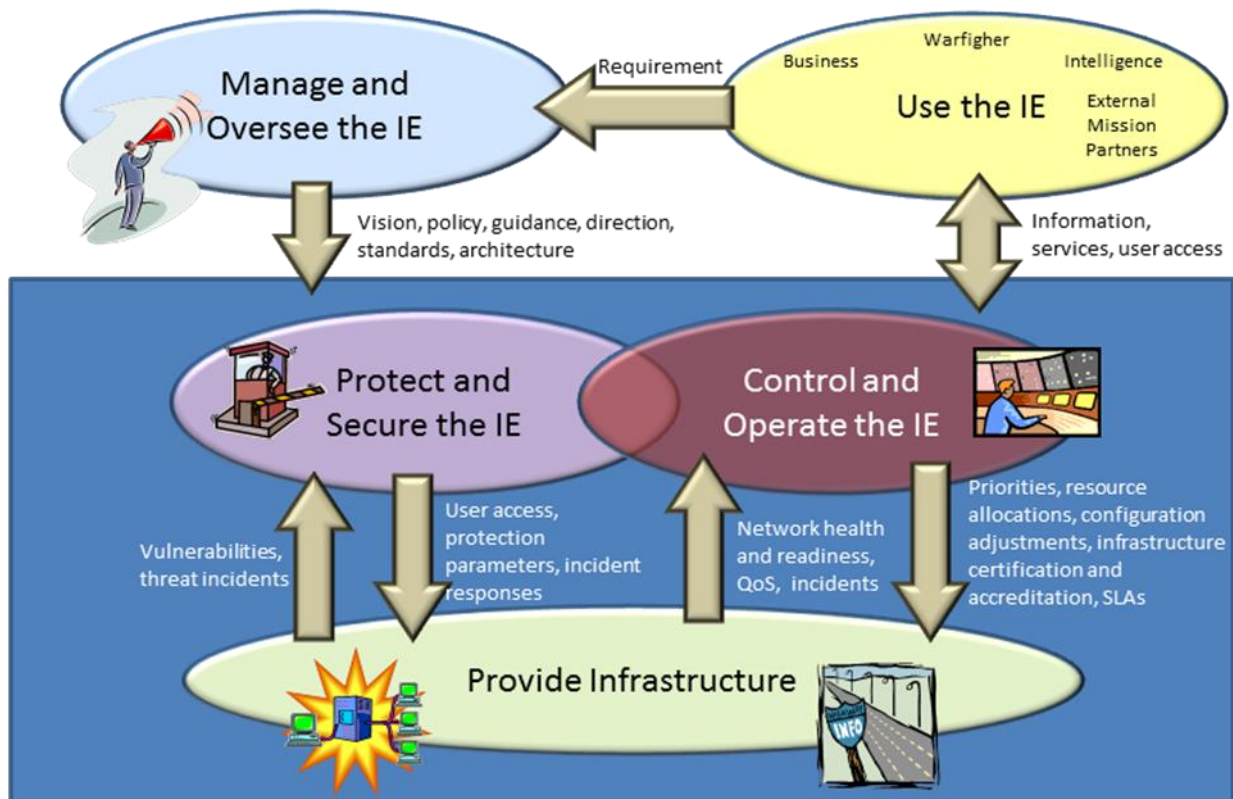
89



# Final DoD IEA v2.0: OV-5a Operational Activity Decomposition Tree

## 90 Relationship of Key Activities

91 **Figure 7** shows how the key activities interoperate with one another to provide an effective IE.  
 92 The Use the IE activity enables internal DoD elements and organizations performing  
 93 warfighting, business, and intelligence operations and external mission partners to provide the  
 94 Manage and Oversee activity with their requirements for the IE. It also provides these users with  
 95 access to and use of the IE to obtain the information and services needed to complete their  
 96 missions.



97

98

Figure 7 - Functional Relationship of Operational Activities in IEA

99 The Manage and Oversee activity turns user requirements into a vision of the IE to which to  
 100 govern. This vision is architected to provide the necessary description of these requirements,  
 101 how they relate, and the resources needed to meet to them. The resulting architecture data is  
 102 analyzed and the results of this analysis used in developing and enforcing policies, guidance,  
 103 direction, and standards to manage the protection, control, and implementation of the resources  
 104 needed to deliver the vision.

105 The Protect and Secure activity takes policy, guidance, and direction from the Manage and  
 106 Oversee activity and works to ensure the IE is secure from both internal and external threats. It  
 107 provides the mechanisms and processes to authenticate users and provide them with authorized  
 108 access to and use of the infrastructure in accordance with the privileges they have been granted,

## Final DoD IEA v2.0: OV-5a Operational Activity Decomposition Tree

109 while at the same time preventing unauthorized users from gaining the ability to improperly  
110 exploit the IE. The Protect and Secure activity sets security parameters for infrastructure  
111 resources to minimize their vulnerability to both exploitation and attack and to prevent their  
112 unauthorized use. It enables monitoring of the IE for vulnerabilities and attempts to improperly  
113 gain access to or attack the IE and provision of the proper security incident responses. It is in  
114 this area where the Protect and Secure and Control and Operate activities overlap, since both  
115 enable monitoring of the IE (for different reasons) and provide appropriate responses to detected  
116 incidents.

117 The Control and Operate activity takes policy, guidance, and direction from the Manage and  
118 Oversee activity and works to ensure delivery of the IE vision through efficient and effective  
119 operation of the IE to meet rapidly and continually changing user needs. The Control and  
120 Operate activity is responsible for certifying and accrediting the infrastructure in accordance with  
121 LRP so the infrastructure fully meets both user needs and those security restrictions established  
122 by Protect and Secure the IE. The Control and Operate activity monitors the health and  
123 readiness of IE resources and the Quality of Service (QoS) they are providing to users in  
124 accordance with negotiated Service Level Agreements (SLAs), and then adjusts infrastructure  
125 operation as necessary to deliver the best possible service. As information and service needs  
126 change in line with shifts in warfighting, business, and defense intelligence operations, this  
127 activity dynamically and proactively adjusts resource allocations and configuration of the  
128 infrastructure to ensure continual and optimal IE operations.

129 The Provide Infrastructure activity supplies internal elements and components performing  
130 warfighting, business, and defense intelligence operations and external mission partners with the  
131 means to access and use information and services needed to successfully complete their  
132 missions, in accordance with the access granted them by the Protect and Secure activity. The  
133 Provide Infrastructure activity enables and underpins the IE, providing basic communications  
134 and computing capabilities necessary for net-centric operation of the IE and those Enterprise-  
135 wide services needed by all users. It provides the Protect and Secure activity with information  
136 on infrastructure configuration for use in assessing vulnerabilities and threat incidents. In turn, it  
137 adopts security parameters set by the Protect and Secure activity to protect infrastructure assets  
138 from exploitation and attack. The Provide Infrastructure activity is directed by the Control and  
139 Operate activity to ensure effective customer service and information and service delivery. It  
140 provides information on infrastructure health and readiness, QoS, and operational incidents, and  
141 dynamically adjusts the configuration and operation of infrastructure resources to meet rapidly  
142 changing priorities and user needs.

### 143 **Value of Operational Activities**

144 These operational activity descriptions provide a detailed definition of all the actions required to  
145 put in place, secure, manage, operate, and use the IE to effectively enable net-centric operations

## Final DoD IEA v2.0: OV-5a Operational Activity Decomposition Tree

146 and meet operational requirements. One overarching value of these activity descriptions lies in  
147 the support they provide stakeholders and users involved in planning for effective IE  
148 implementation, management, and operation. IE Planners (e.g., the DoD and Component CIOs,  
149 IE portfolio and investment managers) can compare current actions being taken to achieve the IE  
150 against these required activities to determine gaps in existing performance. IE Planners can use  
151 these identified performance gaps to measure progress in achieving the desired IE end state by  
152 analyzing the projected results of those activities which are being performed adequately and  
153 comparing them to expected results from being able to perform all activities. In addition,  
154 activities will be aligned with the IE Required Capabilities to show which activities are necessary  
155 to achieve each of these capabilities. By determining where gaps exist in activity performance,  
156 planners should then be able to determine which IE Capabilities can and cannot be delivered to  
157 meet user needs. Using the results of these analyses, IE Planners can prioritize activity  
158 performance gaps and determine how best to assign limited resources to ensure the right  
159 activities can be executed to meet priority needs.

160 A second overarching value of the operational activities lies in the description of security  
161 requirements for the IE provided by the sub-activities under Protect and Secure the IE. These  
162 activity descriptions provide all DoD IEA stakeholders/users with an understanding of the full  
163 set of actions that must be taken to secure information and services in the IE. The IE governance  
164 process must assess and develop policy to enforce compliance with these activities. Both IE  
165 providers and consumers must execute these activities to ensure the IE and its information  
166 remains secure in accordance with that policy and guidance. Execution of security activities  
167 must be monitored and enforced by NetOps to keep the IE secure.

168 For other stakeholders/users of the DoD IEA, specific areas in the activity decomposition have  
169 particular meaning and use:

- 170 • For those governing the IE, predominately the DoD and Component CIOs and their staffs,  
171 activity descriptions found under Manage and Oversee the IE describe specific actions that  
172 required governance processes must incorporate and that governance structures and  
173 organizations must execute in implementing those processes.
- 174 • For providers of IE infrastructure resources, to include solution architects, service developers  
175 and providers, and program managers, activities subordinate to Provide IE Infrastructure  
176 describe actions that must be taken to deliver the proper capabilities with which the solution  
177 aligns. Solution architectures should describe activities aligning with the appropriate DoD  
178 IEA activities or incorporate the appropriate DoD IEA activities to ensure solutions meet  
179 these requirements. Compliance with these activities must be enforced across DoD.
- 180 • For users of IE infrastructure resources, sub-activities under the Use the IE activity describe  
181 the actions that must be taken by consumers to effectively operate with and obtain optimal  
182 value from the IE.