	1	2	3	4	5	6	7	Existing Format in ONAP		SECCOM Proposed	Reference
	ONAP Logging Guidelines Rev 1 from 2017				Log Spec v1.1	Log Spec v1.2	Log Spec v1.3				
No.	Audit Log (Inbound)	Metric Log (Outbound)	Error Log (internal)	Debug Log					Security Log	Proposed Requirement	
1	BeginTimestamp	BeginTimestamp	Timestamp	Timestamp	BeginTimestamp	LogTimestamp	LogTimestamp	Date-time that processing activities being logged begins. The value should be represented in UTC and formatted per ISO 8601, such as “2015-06-03T13:21:58+00:00”. The time should be shown with the maximum resolution available to the logging component (e.g., milliseconds, microseconds) by including the appropriate number of decimal digits. For example, when millisecond precision is available, the date-time value would be presented as, as “2015-06-03T13:21:58.340+00:00”. (1,2,3,4,5) use %d field - see %d{"yyyy-MM-dd'T'HH:mm:ss.SSSXXX",UTC} (5,6)	Timestamp	The container and container application MUST log the field “date/time” in the security audit logs.	R-97445
2	EndTimestamp	EndTimestamp			EndTimestamp	EntryTimestamp	EntryTimestamp				
3	ElapsedTime	ElapsedTime			ElapsedTime	ElapsedTime	ElapsedTime				
4						InvokeTimestamp	InvokeTimestamp				
5	RequestID	RequestID	RequestID	RequestID		RequestID	TransactionID	Universally unique transaction request ID (UUID) (1,2,3,4) UUID to track the processing of each client request across all the ONAP components involved in its processing (6,7) [LOG-232] Rename requestID to TransactionID - ONAP JIRA	Transaction ID	The container and container application MUST log Transaction ID.	None
6	serviceInstanceID	serviceInstanceID			ServiceInstanceID	ServiceInstanceID	ServiceInstanceID				
7	threadId	threadId	ThreadId		ThreadID	thread	thread				
8	physical/virtual server name	physical/virtual server name			VirtualServerName	VirtualServerName	VirtualServerName				
9	serviceName	serviceName	ServiceName		ServiceName	ServiceName	ServiceName	Externally advertised API invoked by clients of this component (1,2,3) For Audit log records that capture API requests, this field contains the name of the API invoked at the component creating the record (e.g., Layer3ServiceActivateRequest). For Audit log records that capture processing as a result of receipt of a message, this field should contain the name of the module that processes the message. (5) The service inside the partner doing the call - includes API name(6,7)	~~Service / Program Name~~	~~The container and container application MUST log the field “service or program used for access” in the security audit logs.~~	~~R-06413~~
10	PartnerName	PartnerName	PartnerName		PartnerName	PartnerName	PartnerName	This field contains the name of the client application user agent or user invoking the API if known. (1,2,3, 5,) The identification of the entity that made the request being served. For a serving API that is authenticating the request, this should be the authenticated username or equivalent (e.g. an attuid or a mechid) authenticated = userid If an authenticated API, then log the userid Otherwise, if the HTTP header "X-ONAP-PartnerName" was provided, then log that (note: this was a direction that we seemed to be going but never completed) Otherwise, if the HTTP header "X-FromAppId" was provided, then log that Otherwise, if the HTTP header "User-Agent" was provided, then log that Otherwise, log "UNKNOWN" (since the field is currently required, something must be in it) (7)	Service / Program Name	The container and container application MUST log the field “service or program used for access” in the security audit logs. The container and container application MUST log the field “Login ID” in the security audit logs.	R-06413 R-89474
11		TargetEntity	TargetEntity		TargetEntity	TargetEntity	TargetEntity				
12		TargetServiceName	TargetServiceName		TargetServiceName	TargetServiceName	TargetServiceName				
13		TargetVirtualEntity			TargetVirtualEntity						
14						TargetElement	TargetElement				
15	StatusCode	StatusCode			StatusCode	StatusCode	StatusCode	This field indicates the high level status of the request. It must have the value COMPLETE when the request is successful and ERROR when there is a failure. (1,2,5) This field indicates the high level status of the request - one of (COMPLETE, ERROR, INPROGRESS) (6,7)	Status Code	The container and container application MUST log a "status code" in the security audit logs.	R-15325
16	ResponseCode	ResponseCode			ResponseCode	ResponseCode	ResponseCode				
17	Response Description	Response Description			ResponseDescription	ResponseDesc	ResponseDesc				
18	instanceUUID	instanceUUID			InstanceUUID	InstanceID	InstanceID				
19	Category log level	Category log level				level	level	One of the following Enum: “INFO”	“WARN” |”DEBUG”	“ERROR”	“FATAL”. (1,2) %level (6,7)	Log Level	The container and container application MUST use an appropriately configured logging level that can be changed dynamically.	R-28168
20	Severity	Severity			Severity	Severity	Severity	Optional: 0, 1, 2, 3 see Nagios monitoring/alerting for specifics/details (1,2, 5) Logging level by default aligned with the reported log level - one of INFO/TRACE/DEBUG/WARN/ERROR/FATAL (6,7)	Severity	The container and container application MUST log the severity level of a processing event.	None
21					AlertSeverity						
22	Server IP address	Server IP address			ServerIPAddress	ServerIPAddress	ServerIPAddress				
23	Server	Server			Server	ServerFQDN	ServerFQDN				
24					ServerFQDN						
25	ClientIPaddress	ClientIP			ClientIPAddress	ClientIPAddress	ClientIPAddress				
26	class name	class name			ClassName						
27	ProcessKey	ProcessKey			ProcessKey						
28											
29	CustomField1	CustomField1			CustomField1						
30	CustomField2	CustomField2			CustomField2						
31	CustomField3	CustomField3			CustomField3						
32	CustomField4	CustomField4			CustomField4						
33	detailMessage	detailMessage	detailMessage			p_message	p_message	Optional: the rightmost (“last”) field in a log record. When present, its value may be formatted if/as useful to meet specific/individual use case(s). (1,2,3) Standard attribute - defined in logback.xml - Message - used for %msg% (6,7)	Log Message	No specific security requirements, but this field is necessary to log security events.	None
34	Unused	Unused									
35					RemoteHost						
36						p_marker	p_marker	The marker labels INVOKE, ENTRY, EXIT – and later will also include DEBUG, AUDIT, METRICS, ERROR when we go to 1 log file - this field is %marker (6,7) Add the term "Security" to the ENUM (SECCOM)	Log Type Name	The container and container application MUST log the field "Log type" in security audit logs.	None
37									Container Image Name / Tag	The container and container application MUST log the Container Image Name/Tag. The image name/tag is as returned by the docker images command. NOTE: Images are not required to have tags	None
38									Container Image Digest	The container and container application MUST log the container image digest. The digest is a cryptographic digest as returned by the docker images --digests command.	T1036, T1525
39									Container ID	The container and container application MUST log the container ID. The container ID is the same that is returned by the docker ps -q command. NOTE: The container ID is unique for life time of the the container instance. Once the container is killed, this ID goes away.	None
40									Container Name	The container and container application MUST log the container name. This is the unique name of the image (webserver, FW, DCAE01). This is returned by the docker ps command.	None
41									Role / Attribute ID	The container and container application MUST log the Role or Attribute ID of the Principal identity of the entity accessing the requested service or API. Note: The group ID is in reference to a Role or Attribute as part of a RBAC or ABAC scheme.	None
42									Protocol	The container and container application MUST log the field “protocol” in the security audit logs.	R-25547
43			ErrorCategory								
44			ErrorCode								
45			ErrorDescription								
46				DebugInfo							
47				End of Record							
48						InvocationID	InvocationID	UUID correlates log entries relating to a single invocation of a single component In the case of an asynchronous request, the InvocationID should come from the original request (6,7)			
49						ContextName	ContextName	The logging enhancement team could not find any definition for this field and it was agreed to leave out the description for this field. (6,7)			
50						User	User	User - used for %X{user} (6,7)	Principal ID	The VNF MUST log the field “Login ID” in the security audit logs.	R-89474
51						p_logger	p_logger	The name of the class doing the logging (in my case the ApplicationController – close to the targetservicename but at the class granular level - this field is %logger (6,7)			
						p_mdc	p_mdc				