Secure Software Development Lifecycle as illustrated by OWASP

OWASP CLASP:

Security Development Lifecycle (SDL) developed by Microsoft to answer the issues faced by the during various development projects and hence, mostly caters to the need of their development methodology only. The lifecycle of Microsoft SDL includes Training, Requirements, Design, Implementation, Verification, Release, Response. While OWASP has a similar line-up with requirements and analysis, Design, Implementation, Testing and Verification, Maintenance in the life cycle model. CLASP (Comprehensive Lightweight Application Security Process) is an Activity driven, role-based set of process components whose core contains formalized best practices for building security into your existing or new start software development lifecycles in a structured, repeatable, and measurable way. CLASP is the outgrowth of years of extensive field work in which system resources of many development lifecycles were methodically decomposed in order to create a comprehensive set of security requirements. These resulting requirements form the basis of CLASP's best practices which allow organizations to systematically address vulnerabilities that, if exploited, can result in the failure of basic security services.
e.g. confidentiality, authentication, and access control.

	Microsoft SDL	OWASP CLASP
Nature of activities	Constructive	Constructive
Applicability	Only SDLC	Any software development process
Nature	Heavy	Light Weight
Code Integrity	No	Yes
Suitability	Large Organizations	Small and Large Organizations
Assessments	SDL can only identify risk assessment. Cannot able to identify vulnerability assessment.	CLASP can identify vulnerability assessment.
Separate Privacy requirement evaluation	Yes	No
Application testing and assessment	Extensively	Through threat modelling, Code level review, security tests, but no verification of security attributes of resources.