OWASP Codes of Conduct Project
Supporting OWASP's Mission

- Colin Watson
colin.watson(at)owasp.org

- Whose Conduct?
- Why?
- What Conduct?
- Comparisons
- Statements of Compliance
Not any of these

- OWASP code values, core purpose, code of ethics and principles
  - Brand usage
  - By-laws
  - General disclaimer
- Projects
  - Projects handbook
- Local chapters
  - Chapters handbook
  - Speaker agreement
  - Finance
- Conferences
  - Speaker agreement
  - Training instructor agreement
  - Global Conferences Committee policies
Influence targets

• Not these
  • Contributors including chapter leaders and project leaders
  • Individual members
  • Employees
  • Committee members
  • Board members
  • Supporters

• But yes, these
  • Government bodies
  • Standards groups
  • Education institutions
  • Trade organizations
  • Certifying bodies
  • ...
With what purpose?

- To define a set of minimal requirements specifying what OWASP believes are the most effective ways these types of organization can support OWASP's mission
- OWASP's mission
  - “To make application security visible, so that people and organizations can make informed decisions about application security risks”
Codes of conduct

- Set of minimal standards
- Normative standards
- Not difficult to achieve
History

- Summit 2011 working sessions
  - For Government Bodies, Standards Groups & Education Institutions
    - Outreach to Educational Institutions
    - Minimal AppSec Program for Universities, Governments & Standards Bodies
      - All participants but especially Jeff Williams, Dave Wichers and Dinis Cruz
  - For Certification Bodies
    - Certification
      - All participants but especially Jason Taylor and Jason Li
- Subsequently
  - For Trade Groups
    - Colin Watson
  - For Commercial Organizations
    - Jeff Williams and Colin Watson
Format

Introduction
As understanding of application security becomes a critical part of an individual’s skill set, organizations are eagerly seeking guidance in identifying knowledgeable individuals in application security. We believe that Certifying Bodies can play a role to empower organizations to identify security-minded individuals. While OWASP will never endorse or support any particular certification, we offer this code of conduct to help guide Certifying Bodies to better serve organizations that are ready to embrace an application security certification.

Code of Conduct
1. The Certifying Body MUST NOT misrepresent the Certifying Body’s certification as endorsed or supported by OWASP.
   While OWASP recognizes the need of organizations to identify individuals with an understanding of application security, OWASP will not endorse any certifying body or their certification. One of the bedrock principles of OWASP is to maintain a vendor-neutral position and any endorsement of a certifying body or their certification is in direct contradiction of this core value. We respect your desire to fill a void in the application security space and expect that you will in turn respect our core values and brand name.

2. The Certifying Body MUST include a visible disclaimer if the Certifying Body’s certification is “based on OWASP materials”.
   OWASP will not allow our brand name to be used in the certification title. However, we welcome a Certifying Body to leverage tools, documents, guidelines, and standards that are freely available from OWASP. We recognize that in such cases, a Certifying Body may wish to inform their audience that their certification is “based on OWASP materials”. We are honored by your desire to leverage OWASP materials, but we ask that you honor the OWASP name and clearly disclaim that your use of OWASP materials does not represent an endorsement or association with OWASP.

Recommendations
1. The Certifying Body SHOULD collect and publish feedback from certification applicants, recipients, and organizations recognizing the certification.
   Certifications represent the Certifying Body’s assertion that the recipient meets some minimal criteria, as defined by the Certifying Body. Organizations depend on that assertion when recognizing a Certifying Body’s certification. We believe that organizations need feedback to effectively determine the value of a certification. We do not suggest what feedback should be solicited, nor the exact form or method for this publication, only that it represents your desire to honestly communicate the value and esteem of your certification.

2. The Certifying Body SHOULD utilize questions, answers, evaluation material and processes that are open and freely available to the general public.
   Organizations around the world are depending on certifying bodies to help identify individuals that understand application security. Supplying open questions and answers allows organizations
Output: 

The OWASP Application Security Code of Conduct for Certifying Bodies

Format (continued)

C. The Certifying Body SHOULD be an OWASP Supporter.

The main benefit of becoming an OWASP Supporter is to demonstrate your belief that application security is important and that you are working to help improve the state of application security in the world.

D. The Certifying Body SHOULD leverage OWASP by attending our events, using our materials, and asking our experts for help.

OWASP has a lot to offer certifying bodies. We have freely available tools, documents, guidelines, and standards. We have worldwide events that are open to everyone and all the presentations are recorded and downloadable for use in classrooms. We even have packaged curricula, elearning, and educational materials that are available for potential applicants to use and modify free of charge. Certifying bodies are strongly encouraged to reach out to our experts with their questions, ideas, and even participate in projects.

References

1. PROJECT, OWASP

2. Membership, OWASP
   [https://www.owasp.org/index.php/Membership](https://www.owasp.org/index.php/Membership)

OWASP Application Security Codes of Conduct

In order to achieve our mission, OWASP needs to take advantage of every opportunity to affect software development everywhere. At the OWASP Summit 2011 in Portugal, the idea was created to try to influence educational institutions, government bodies, standards groups, trade organizations and groups active in the application security space. We set out to define a set of minimal requirements for these organizations specifying what we believe to be the most effective way to support our mission.

We call these requirements a "Code of Conduct" to imply that there are no requirements, they represent a minimum baseline, and that they are not difficult to achieve.

Certifying Bodies wishing to announce their compliance with this Code of Conduct should read the associated information on statements of compliance:


Special thanks to Jason Taylor and Jason II for creating this document, and to all the participants in the work session on Certification at the OWASP Summit 2011 in Portugal for their ideas and contributions to this effort.

The latest version of this document, and the other Codes of Conduct, can be found at:


About OWASP

The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

[https://www.owasp.org](https://www.owasp.org)
The OWASP “Green Book”

- The OWASP Application Security Code of Conduct for Government Bodies
Code of Conduct

1. The Government Body MUST establish and enforce a standard that requires application security for organizations and applications under their jurisdiction.

2. The Government Body MUST build application security into software acquisition guidelines.

3. The Government Body MUST provide OWASP a “notice and comment” period when releasing laws and regulations that are relevant to application security.

4. The Government Body MUST define or adopt a definition of application security.

5. The Government Body MUST create and promote public service messages focused on application security.
The OWASP “Blue Book”

- The OWASP Application Security Code of Conduct for Educational Institutions
Code of Conduct

1. The Educational Institution MUST include application security content somewhere in the standard computer science curriculum.

2. The Educational Institution MUST offer at least one course dedicated to application security annually.

3. The Educational Institution MUST ensure that an OWASP Chapter is available to their students and support it.
The OWASP “Yellow Book”

- The OWASP Application Security Code of Conduct for Standards Groups
Code of Conduct

1. The Standards Group MUST include an “Application Security” section in each software related technical standard.

2. The Standards Group MUST provide OWASP a “notice and comment” period when releasing standards that include an application security aspect.

3. The Standards Group MUST define or adopt a definition of Application Security.
The OWASP “Purple Book”

- The OWASP Application Security Code of Conduct for Trade Organizations
Code of Conduct

1. The Trade Organization MUST include an “Application Security” section in their own membership requirements.

2. The Trade Organization MUST provide OWASP a “notice and comment” period when releasing requirements that include an application security aspect.
The OWASP “Red Book”

- The OWASP Application Security Code of Conduct for Certifying Bodies
Code of Conduct

1. The Certifying Body MUST NOT misrepresent the Certifying Body’s certification as endorsed or supported by OWASP.

2. The Certifying Body MUST include a visible disclaimer if the Certifying Body’s certification is “based on OWASP materials”.


### Similar requirements

<table>
<thead>
<tr>
<th>Government Bodies</th>
<th>Educational Institutions</th>
<th>Standards Groups</th>
<th>Trade Organizations</th>
<th>Certifying Bodies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The Government Body MUST establish and enforce a standard that requires application security for organizations and applications under their jurisdiction.</td>
<td>1. The Educational Institution MUST include application security content somewhere in the standard computer science curriculum.</td>
<td>1. The Standards Group MUST include an “Application Security” section in each software related technical standard.</td>
<td>1. The Trade Organization MUST include an “Application Security” section in their own membership requirements.</td>
<td>-</td>
</tr>
<tr>
<td>3. The Government Body MUST provide OWASP a “notice and comment” period when releasing laws and regulations that are relevant to application security.</td>
<td>-</td>
<td>2. The Standards Group MUST provide OWASP a “notice and comment” period when releasing standards that include an application security aspect.</td>
<td>2. The Trade Organization MUST provide OWASP a “notice and comment” period when releasing requirements that include an application security aspect.</td>
<td>-</td>
</tr>
<tr>
<td>4. The Government Body MUST define or adopt a definition of application security.</td>
<td>-</td>
<td>3. The Standards Group MUST define or adopt a definition of Application Security.</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>(2 more unrelated)</td>
<td>(2 more unrelated)</td>
<td>-</td>
<td>-</td>
<td>(2 more unrelated)</td>
</tr>
</tbody>
</table>
## Additional recommendations

<table>
<thead>
<tr>
<th>Government Bodies</th>
<th>Educational Institutions</th>
<th>Standards Groups</th>
<th>Trade Organizations</th>
<th>Certifying Bodies</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Collect and publish feedback from certification applicants, recipients, and organizations recognizing the certification</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Utilize questions, answers, evaluation material and processes that are open and freely available to the general public</td>
</tr>
<tr>
<td>Be an OWASP Supporter</td>
<td>Be an OWASP Supporter</td>
<td>Be an OWASP Supporter</td>
<td>Be an OWASP Supporter</td>
<td>Be an OWASP Supporter</td>
</tr>
<tr>
<td>Assign a liaison to OWASP</td>
<td>Assign a liaison to OWASP</td>
<td>Assign a liaison to OWASP</td>
<td>Assign a liaison to OWASP</td>
<td>-</td>
</tr>
<tr>
<td>Encourage educational institutions to focus on application security</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Leverage OWASP by attending our events, using our materials, and asking our experts for help</td>
<td>Leverage OWASP by attending our events, using our materials, and asking our experts for help</td>
<td>Leverage OWASP by attending our events, using our materials, and asking our experts for help</td>
<td>Leverage OWASP by attending our events, using our materials, and asking our experts for help</td>
<td>Leverage OWASP by attending our events, using our materials, and asking our experts for help</td>
</tr>
<tr>
<td>-</td>
<td>Encourage interested students to participate in OWASP</td>
<td>-</td>
<td>Encourage interested members to participate in OWASP</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>Involve a security expert early in their standard definition process</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Statements of compliance?

• “Organizations SHOULD clearly communicate that they are in full or partial compliance with this Code of Conduct”

• Dangers
  • "XXX complies with OWASP's codes 100%"
  • "XXX is OWASP code compliant"
  • "All XXX's training is undertaken under the terms of the OWASP Code of Conduct on YYYY"
A proposal from Jason Li

OWASP Code of Conduct

Education Institution

1. COMS 245: Intro to WebApp Security
   http://example.edu/course.php?id=245

2. OWASP Never Land Chapter
   http://owasp.org/...

A. N/A (Link to OWASP Membership)

B. Contact Info for Jason

C. Link to Calendar of Edu’s Attended Events (none exists)

D. Link to Organization’s OWASP Participation Page

Non-compliant categories

Grading metric
- e.g. 66%, “Good”, ???

OWASP does not endorse any organizations. Compliance with the OWASP Code of Conduct for Educational Institutions is based on self-reported information from the organization. For more information, visit:
http://sl.owasp.org/CodesOfConduct
Next steps

• First five
  • Finalize v1.1
  • Project assessment
  • Release
  • Promote

• Others
Project web pages

**OWASP Green Book**
The OWASP Application Security Code of Conduct for Government Bodies
Download the current release
v1.11 draft:
- English version PDF
- English version MS Word
Translations
None are currently available.

**OWASP Blue Book**
The OWASP Application Security Code of Conduct for Educational Institutions
Download the current release
v1.11 draft:
- English version PDF
- English version MS Word
Translations
None are currently available.

**OWASP Yellow Book**
The OWASP Application Security Code of Conduct for Standards Groups
Download the current release
v1.11 draft:
- English version PDF
- English version MS Word
Translations
None are currently available.

**OWASP Purple Book**
The OWASP Application Security Code of Conduct for Trade Organizations
Download the current release
v1.11 draft:
- English version PDF
- English version MS Word
Translations
None are currently available.

**OWASP Red Book**
The OWASP Application Security Code of Conduct for Certifying Bodies
Download the current release
v1.11 draft:
- English version PDF
- English version MS Word
Translations
None are currently available.

**What's missing?**
What other types of organization might be able to support OWASP’s mission? What are the most important things they should do?
Join in the OWASP Codes of Conduct Mailing List with your suggestions and feedback.
Make contact

Colin Watson

- colin.watson(at)owasp.org

Codes of Conduct Project


Mailing List

- https://lists.owasp.org/mailman/listinfo/owasp-codes-of-conduct