

# CONFORMITY ASSESSMENT PUBLICATION

---

## CAB Risk Management Grid





**THIS PUBLICATION IS COPYRIGHT PROTECTED**  
**Copyright © 2016 IEC, Geneva, Switzerland**

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office  
3, rue de Varembe  
CH-1211 Geneva 20  
Switzerland

Tel.: +41 22 919 02 11  
Fax: +41 22 919 03 00  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://www.iec.ch)

**About the IEC**

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

**About IEC publications**

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

**IEC Catalogue - [webstore.iec.ch/catalogue](http://webstore.iec.ch/catalogue)**

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

**IEC publications search - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)**

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

**IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)**

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

**Electropedia - [www.electropedia.org](http://www.electropedia.org)**

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

**IEC Glossary - [std.iec.ch/glossary](http://std.iec.ch/glossary)**

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

**IEC Customer Service Centre - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)**

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: [csc@iec.ch](mailto:csc@iec.ch).



# CONFORMITY ASSESSMENT PUBLICATION

---

## CAB Risk Management Grid

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

## CONTENTS

FOREWORD.....	3
INTRODUCTION.....	4
1 Summary of Risk Topics .....	5
2 Overview of current IEC social media presence (2016-01) .....	12
2.1 Links.....	12
2.2 General comment.....	12
2.3 Information flow .....	13
2.4 Information access .....	13
2.5 Information content .....	14
2.6 Information type .....	14
3 Social Media Risk .....	15

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

---

**CAB Risk Management Grid****FOREWORD**

This document is a living document to be used by the IEC CA Systems and the CAB

The text of this publication is based on the following documents and decisions:

Document(s)	Decision(s)
CAB/721/DL	CAB Decision 22/7
C/1469/R	CB Decision 2007/12
CAB/752/R, CAB/762A/RM	
CAB/782/R, CAB/794A/RM	
CAB/852/INF, CAB/864A/DL	CAB Decision 26/4
CAB/1314/DV, CAB/1341/DL	CAB Decision 36/9
CAB/1384/INF, CAB/1400/DL	CAB Decision 37/15
CAB/1525/INF, CAB/1531A/RM, CAB/1530/DL	CAB Decision 39/22

## INTRODUCTION

The IEC is an international organization defined and governed by its Statutes and Rules of Procedure. The IEC is a membership organisation, whose members are the National Committees of countries. The members exercise authority and control over the IEC through the Council and the Council Board.

The object of the IEC is to promote international co-operation on all questions of standardization and related matters, such as the verification of conformity to standards in the fields of electricity, electronics and related technologies, and thus to promote international understanding. This object, *inter alia*, is achieved by issuing publications, including International Standards, and by offering conformity assessment services.

The two main activities of the IEC are standards development (SD) and conformity assessment (CA).

The IEC CA activities are, currently, third party testing and certification activities. However, IEC does not perform testing or certification itself, but rather provides a framework in which professional Certification Bodies and Testing Laboratories, from around the world, participate. It is those professional Certification Bodies and Testing Laboratories that do the testing and issue the certificates.

The IEC CA activities, by their very nature, create both opportunities and risks for IEC. As an essential, good management practice, the risks need to be identified, assessed and managed.

The IEC Statutes and Rules of Procedure, in its Article 12, indicate that the Council, through the Council Board, delegates to the Conformity Assessment Board (CAB) the overall management of the IEC CA activities.

This document is the current reference of the CAB Risk Management Grid.

## **CAB Risk Management Grid**

### **1 Summary of Risk Topics**

- Governance of IEC Conformity Assessment Systems
- IEC Brand
- Loss of Recognition as a Leader in Global Conformity Assessment Services
- Financial
- Legal
- Intellectual Property
- Operational

Risk	Risk factor	Mitigation measure in place	Residual risk level	Recommendation as indicated in the conclusion
Governance of IEC Conformity Assessment Systems	Limited oversight of CAB	The Basic Rules of all of the CA Systems are in the process of being harmonized	Under control	CAB to monitor the activities of CAB WG 11 and the IEC CA Systems via the reports provided and the input from the market via the national mirror committees
	Inappropriate IEC CA System development and/or amendments of their Basic Rules	Basic Rules and new Programmes are subject to approval of the CAB The IEC CA Systems regularly report to the CAB	Under control	
	Scope extension	IEC CA Systems report at each CAB meeting – The Scope is subject to the Basic Rules which shall be approved by CAB Scope extension criteria is defined in CAB Decision 25/9 Proposal: AB to consider to set a policy of IEC CA Systems reporting to the CAB when they initiate a work for scope extension	Appropriate	
		Feedback from the market via the national mirror committees is an additional control mechanism	Appropriate	
	Inappropriate selection or use of standards (including standards from IEC or other sources)	Proposal: CAB shall approve standards to be used within approved scope of a IEC CA System CAB should also consider requesting IEC CA Systems to notify addition and/or deletion of standards being used in their Schemes	Additional mitigation needed	
	Lack of accountability to Council and to Council Board	CAB reports to Council Board	Appropriate	

Risk	Risk factor	Mitigation measure in place	Residual risk level	Recommendation as indicated in the conclusion
IEC Brand	<p>Inappropriate activity that could tarnish the reputation of the IEC CA Systems and of the IEC itself</p> <p>Example: An IEC CA System has one or more members who systematically disregard the IEC CA System's rules</p>	<p>The IEC CA Systems have detailed operating rules and procedures in place</p> <p>Peer assessment process for regularly assessing and monitoring the competence of certification bodies and testing laboratories based on ISO/IEC Standards as well as the IEC CA Systems' Basic Rules, Rules of Procedure, and Operational Documents</p>	<p>Appropriate</p> <p>Appropriate</p>	
	<p>Use of inappropriate standards by the IEC CA Systems or one of their certification bodies</p>	<p>The IEC CA Systems' Basic Rules have provisions for use of mainly IEC Standards</p> <p>The use of other documents than IEC and ISO Standards needs the approval of CAB</p> <p>Peer assessment is an effective means to assure that Certification Bodies use the appropriate standards. IEC CA System and Scheme's Rules cover contingencies and resulting actions</p>	<p>Under control</p> <p>Appropriate</p> <p>Appropriate</p>	<p>To encourage the National Committees to adopt and implement IEC standards without modifications and to commit themselves to withdraw conflicting national standards</p>
	<p>Inappropriate use of Certificates, Logos and/or Marks</p>	<p>The IEC CA Systems proactively request information on examples of misuse. Each IEC CA System has a Technical Secretariat to receive complaints/feedback from industry and CA Members</p> <p>The IEC CA Systems prepare, at each Management Committee meeting, an agenda item on this matter. The report under this agenda item shall include known incident(s) of misuse of marks owned by the IEC and certificates within the IEC CA Systems, where the IEC's brand or name is adversely impacted.</p>	<p>Under control</p>	<p>CAB, IECEE, IECQ, IECEX and IECRE are further investigating this item</p>

Risk	Risk factor	Mitigation measure in place	Residual risk level	Recommendation as indicated in the conclusion
		<p>NOTE In the case of the IECEX, the Ex Mark Committee, as identified in the IECEX Basic Rules, fulfils this role for the IECEX Mark</p> <p>The annual report from the Chairman of each IEC CA System to the CAB shall include the relevant cases. If there were no cases, the Report shall state this</p> <p>The CAB report to the Council Board after the IEC CA System Chairmen's annual reports have been approved shall include the IEC CA Systems' operations and other relevant cases reported in the IEC CA System Chairmen's annual reports</p> <p>Online certificates database prevents inappropriate use of Certificates, Logos or Certification Marks</p>		
	<p>Development and use of an IEC Mark or Label could have severe liability consequences related to product incidents and/or trademark infringements</p> <p>Proposal: CAB to develop a policy related to the acceptance of Marks developed by the IEC or IEC CA Systems</p>		Additional mitigation needed	CAB should review new Marks being proposed by the IEC or IEC CA Systems

Risk	Risk factor	Mitigation measure in place	Residual risk level	Recommendation as indicated in the conclusion
Loss of Recognition as a Leader in Global Conformity Assessment Services	Other international organizations entering into the Global CA services area	IEC should be seen as the leader in global CA services. IEC also needs increased presence at the NC level that also includes regulatory participation. CAB should determine how to achieve these	Additional mitigation needed	
		IEC needs to reach out early to establish working relations with those organizations potentially considering offering global CA services.	Additional mitigation needed	
Financial	Impact on IEC results Example: Imbalance in the IEC CA System's budget	Accounts of each of the IEC CA Systems are audited by IEC's external auditors and reported to CAB for approval	Under control	Measures shall be taken to reduce dependence on unreliable sources of income
	Shortage of income	Annual accounts and budgets and forecasts are subject to approval by Management Committees of the IEC CA Systems and then finally approved by CAB	Under control	IEC CA Systems to continue to build up reliable reserves according to the guidance set by the General Secretary endorsed by CAB
		Reserves exist that serve (mainly) to avoid financial problems	Appropriate	IEC CA Systems to continue to report to CAB on their finances (including annual forecasts) and their budgets
	New certification activities and scope extensions	Both the management committees (stakeholders) of the IEC CA Systems and CAB approve new activities after checking if there is a viable business plan by the IEC CA System. (refer to CAB Decision 25/9)  There is also feedback from the market via the national mirror committees  CAB has established the criteria for proposed scope extensions	Appropriate	

<b>Risk</b>	<b>Risk factor</b>	<b>Mitigation measure in place</b>	<b>Residual risk level</b>	<b>Recommendation as indicated in the conclusion</b>
Legal	Liability of the IEC under national or international law  Example: An IEC CA System offers a service that cannot control the actions of its operators, e.g. a hypothetical IEC SDoC Register	Insurance arrangements take into account the liabilities which may attach to IEC through the activity of the IEC CA Systems	Appropriate	
		The IEC CA Systems' Basic Rules cover: Exclusion of liability Legal protection Exoneration	Appropriate	
		Lawyers have confirmed that the basic rules are appropriate regarding legal liability	Appropriate	
Intellectual Property	Concerns pertaining to the translation of IEC CA Systems' documents into other languages and their use by other organizations as proprietary documents for use at the local level	Review the current rules for use of IEC documents, IEC CA Systems documents, logos and marks (including labels), and formulate recommendations for harmonization and consistent application	Additional mitigation needed	IEC legal (office) together with IEC CA Systems Secretaries to prepare common guidelines for use by all IEC CA Systems
Operational	Deterioration in performance quality	Review by CAB based on the IEC CA System's reports that also include the operational data, main customer's complaints, membership suspension and cancellations as well	Appropriate	
	Diminishing international acceptance	On-going monitoring of acceptance by keeping statistics; possible use of surveys conducted to measure market acceptance	Appropriate	
	Operational changes that may impact on IEC CA Systems' customers	Review complaints via the existing Boards of Appeal  Industry participates in the IEC CA Systems' Management Committees	Appropriate	

Risk	Risk factor	Mitigation measure in place	Residual risk level	Recommendation as indicated in the conclusion
		If CB proposal is approved by the Council, Nov 2014: Then CAB to endorse the IEC CA Systems' Rules of Procedure notified by the IEC CA Systems		
	Inappropriate ISO/IEC conformity assessment Standards	CAB members and IEC CA System Secretaries are actively involved in CASCO activities	Appropriate	

## 2 Overview of current IEC social media presence (2016-01)

### 2.1 Links

IEC website links to IEC social media corporate pages given at the bottom of all webpages pages:

- Facebook      [www.iec.ch/facebook](http://www.iec.ch/facebook)
- Twitter        [www.iec.ch/twitter](http://www.iec.ch/twitter)
- LinkedIn       [www.iec.ch/linkedin](http://www.iec.ch/linkedin)
- Pinterest      [www.iec.ch/pinterest](http://www.iec.ch/pinterest)
- YouTube       [www.iec.ch/youtube](http://www.iec.ch/youtube)
- Slideshare     [www.slideshare.net/IECStandards](http://www.slideshare.net/IECStandards)

and other IEC social media corporate web pages:

- Google+        [www.iec.ch/google+](http://www.iec.ch/google+)

and an IEC blog is also accessible from the IEC homepage via:

- >News & Views > IEC Blog

or directly to [www.blog.iec.ch](http://www.blog.iec.ch), it runs on WordPress.

IEC current Social Media Overview																					
Information →  Platform ↓	Flow		Access			Content							Type								
	Out only	In & out (share)	IEC controlled	General public	Account needed	IEC approved	IEC general	Articles	Events	Technology	Services	Interviews	Comment/ opinion	News	Text	Images	Video	Mixed media	Aggregated content	Presentations	
Facebook	X		X	X		X	X	X	X	X	X	X	X		X	X	X	X			
fans	X		X	X									X	X	X						
Google+	X		X	X		X	X	X	X	X	X	X			X	X	X	X			
Circles/followers	X		X	X									X	X							
LinkedIn	X		X	X		X	X	X	X	X	X	X	X		X	X	X	X			
group & subgroups	X	X	X	X									X		X						
Twitter	X		X	X		X	X	X	X	X	X	X	X	X	X	X	X	X			
followers	X		X	X									X		X						
Pinterest	X		X	X	X	X	X	X	X	X	X	X	X			X	X				
Youtube (YT)	X		X	X		X	X		X	X	X	X					X				
Vimeo	X		X	X				X	X	X	X						X				
Slideshare	X		X	X		X	X		X	X							X		X		
IEC blog (WordPress)	X		X	X		X	X	X	X		X	X			X	X					

### 2.2 General comment

In the social media environment there are official IEC pages established, within the different platforms, on which officially approved content is placed. The terms “official IEC” and “officially approved” are intended to mean that the IEC communications team is managing the

pages and the content. There are also non-official pages established by individuals or groups, who are often part of the IEC community, and who wish to discuss specific topics or subjects. Examples of these are IEC TC/SC discussion forums.

In general, IEC has control of the official pages and content, and little or no control over the non-official pages and content.

### **2.3 Information flow**

Depending on the social media platform, the flow of information can be unidirectional, outward only, or bidirectional, inward and outward.

Most open leading social media platforms like Facebook, LinkedIn, Google+, Twitter and YouTube are platforms that IEC uses specifically to place approved information (text, images, video, etc) and where platform account holders from the general public or approved public can share the information and/or add comments, “likes” etc. IEC can use those channels for overall brand positioning and specific campaigns designed to promote events, activities or impact of our work. All shared information and re-shared industry news are public so public responses and engagement is monitored and followed up if needed. These platforms are necessarily bidirectional.

The IEC LinkedIn groups (online community strictly for professionals) contain content, which is moderated – the IEC communications team has full control over final posts appearing in this social media channels.

Twitter is often used as a channel to allow real-time comments and opinions from the general public or concerned audience (a chatroom platform). Twitter hashtags often appear quickly for specific occasions – an event or sub-part of an event – and allow participants to exchange comments and opinions on the fly. Those hashtags just as often also quickly disappear after the event but serve as a good aggregation mechanism for audiences wishing to use posts with event #hashtag as notes.

Social media channels can also be used as a feedback and engagement mechanism to collect comments about a published article, for example an e-tech article might propose a Twitter discussion or reactions in Facebook comments.

### **2.4 Information access**

Access to the information on the various platforms is governed by two things. Firstly, for all the official IEC social media platforms in order to post and access analytics it is necessary to have an account associated with at least one individual representing IEC officially, e.g. Facebook, Google+, LinkedIn, Twitter, etc. Secondly, some of the information sources on the platforms that are controlled within the corporate page, such as scheduling of posts, access to page insights or approving new LinkedIn group members require official IEC authorization to be accessed. Sometimes it is possible for members of the general public to see general information without a platform account or IEC access rights, but to go to a deeper level, to share or post information requires both. Access to specific social media channels is also moderated on the level of SproutSocial – (a tool used by IEC for social media posting, social analytics and network building).

It is worth remembering that most of the IEC public facing, shared content is designed for public use and so it is accessible by the general public without the need to log in to the relevant social media channel. For example the IEC Facebook fan page posts are visible to the public without Facebook login, but our fan page stats (insights) are only visible to the IEC communications team.

## 2.5 Information content

The information content that is generally uploaded or posted on the different platforms varies between the groups of platforms based on the primary goal of the platform in our social media strategy and the nature of the tool (technical functionality, shared content type, target audiences).

The obvious example is YouTube which owes its existence to video sharing. It is designed to enrich the image of our brand articulated through the leading core social media channels (Facebook, Twitter, Google+ and LinkedIn). The videos that IEC uploads are of all types including interviews, event promotions, technology and general IEC promotion. Commenting on YouTube is allowed, likes and shares are common but the primary goal of this channel is to display video content and allow easy embedding in other websites.

Facebook, Twitter and Google+ are very similar and cater to the general public, while LinkedIn is focused more on professionals. Content on these four platforms is pretty similar and they offer similar functions for sharing and posting comments, etc. All four have options to group people (Facebook and LinkedIn groups, Google+ circles, Twitter lists), follow their updates, allow them to follow us and add them as authorized members (friends). These platforms are used to promote all manner of information about the IEC and its activities, events, technologies, e-tech articles and so on. They also offer a forum for some technical discussions. IEC controls the uploaded information, but does not control or filter the forum discussion and posted comments. Public engagement through discussions is welcomed but it is monitored ("social listening") through alerts and notifications and it is moderated if needed (not deleted but hidden for future reference or simply directly addressed).

Pinterest is essentially an image/photo sharing system which serves as a/the leading promotional and traffic driving tool (its primary goal is to direct users to the IEC website). Its content is therefore mainly images and photos, but it is also evolving and now also allows text to be associated with the images. On the IEC corporate Pinterest page, only IEC can upload images, but those images can be commented-on by Pinterest account holders. Users can collaborate in groups ("boards" that are collections of visual content).

Slideshare is a social network platform designed specifically for sharing presentations and other documents. It is a public knowledge sharing tool which also helps brand positioning, but it is normally used as a secondary tool – content is posted only if it is available.

The IEC blog (on the WordPress platform) is basically short articles posted by members of the IEC communications team. The content can be on any subject related to IEC activities and work.

## 2.6 Information type

On Facebook, Twitter, Google+ and LinkedIn information can be text, images, video, mixed content, aggregated content and links. The information on YouTube is video. Pinterest was designed for sharing photos and images, and Slideshare for sharing presentations. The IEC Blog is basically for articles, which generally means images and text, but can also be used for aggregated content (collections of social media posts or embedded content from other websites).

### 3 Social Media Risk

The SANS Institute, [www.sans.org](http://www.sans.org), created a white paper titled *Risk Assessment of Social Media* [www.sans.org/reading-room/whitepapers/privacy/risk-assessment-social-media-33940](http://www.sans.org/reading-room/whitepapers/privacy/risk-assessment-social-media-33940) which identifies the two main social media risks as “reputation damage and data leakage”.

A third risk is the lost opportunity of not participating in social media and therefore the risk of not being part of, or shaping, the discussion.

IEC Social Media Participation Risk Management Grid							
Risk			type	P	I	Mitigation	Contingency
Brand damage	False accusations, incorrect information, mis-information, politically incorrect information, rude or abusive information.	Official IEC posting	reputation	1	3	IEC Social Media Policy with content review process. Staff training.	IEC crisis management process – track & monitor, detect, report, investigate, respond, monitor results. Ongoing social listening – alerts and notifications. Remove/correct posting.  Contact the post owner through private channels to ask for correction.  Use IEC social media community pressure to correct the posting.  Use reporting provided by social media tools ('report abuse buttons')
		Private IEC staff posting		1	3	IEC Social Media Guidelines for Staff. Staff training.	
		Posted by non-IEC		2	2	Sites/groups, etc not “managed” by IEC have members from the IEC community that moderate the posted information. False information, if publicly corrected by IEC team, is less critical and quickly corrected.	
Litigation	Legal attack by IP owner for non-referenced/licensed use of IP	Official IEC posting	financial, reputation	1	1	IEC Social Media Policy with content review process. Staff training.	Remove/correct posting.  Formal apology.
		Private IEC staff posting		2	1	IEC Social Media Guidelines for Staff. Staff training.	
Data leakage	Illicit access to IEC databases, proprietary information, trade secrets, etc		strategic	1	2	No direct links between the social media platforms and the IEC IT system. Technical barriers such as firewalls, anti-malware, etc.	Legal action (if aware of the breach and can identify the guilty party)
	Disclosure of sensitive or strategic information	Official IEC posting		1	3	IEC Social Media Policy with content review process. Staff training.	Remove immediately.
		Private IEC staff posting		2	3	IEC Social Media Guidelines for Staff. Staff training.	Staff sanctions.

P = likelihood of the risk occurring (scale of 1 lowest to 3 highest)

I = impact if the risk occurs (scale of 1 least to 3 most)

Mitigation = what can be done to avoid the risk (reduce the “P”)

Contingency = what can be done to minimize the impact when the risk occurs





INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

3, rue de Varembé  
PO Box 131  
CH-1211 Geneva 20  
Switzerland

Tel: + 41 22 919 02 11  
Fax: + 41 22 919 03 00  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://www.iec.ch)