



“Securing Your Business’ Information”

**Registered office: 19791 Edgewood Lane ♦ Huntington Beach ♦ CA ♦ 92646-3815
T: +1 714 965 99 42 ♦ E: RGW@Zygma.biz**

Zygma LLC has independently assessed Evantix’s eBusiness Risk, Audit and Compliance Manager offerings for IS 27001 conformity support. The principal findings of this assessment are summarized by Richard G. Wilsher, CEO and Certified ISMS Auditor for Zygma LLC, as follows:

- i) “Evantix’s Risk Management Framework directly addresses all parts of the IS 27001 requirements for processes and controls and can therefore give a good indication of the maturity of the respondent’s information security management posture;*
- ii) Evantix’s Risk Management Framework provides 1st Party organizations with support for their own achievement of conformity to IS 27001 requirements in all areas, principally:*
 - a. in establishing, implementing, operating and documenting the information security processes and controls, in those areas where the respondent’s service provision is a factor in the organization’s overall security posture; and*
 - b. in the operation of controls in the areas of establishing policy, internal organization of information security, operational processes and addressing and managing risks associated with services delivered by surveyed entities.*

This degree of coverage can translate into valuable and meaningful support to Evantix’s clients, dove-tailing with their in-house risk-, audit- and compliance-management strategies and in turn supporting Evantix’s clients’ own information security management systems. Use of Evantix’s Risk Management Framework can provide for a consistent and repeatable approach to 3rd Party risk management in an IS 27001 context, giving both management and auditors a clear view of how 3rd Party risk is managed and mitigated.

Further details of Zygma’s assessment are available by following [this link](#).

Zygma has found Evantix's Risk Management Framework to have a high degree of correlation between its specific 'ISO/IEC 27001 Conformity' questions and functional aspects with the requirements of ISO/IEC 27001:2005 (IS 27001) which could provide substantial support to organizations wishing to integrate Evantix's service offerings into their own overall information security management system.

Although the specific conformity questions cover 96% of the complete requirements of IS 27001 it is important to understand the following caveats.

The assessment determined coverage or support for any IS 27001 clauses on the basis of whether an Evantix's Control Framework (ECF) question addresses a subject area which is covered by that clause. No comparative weighting has been applied to individual clauses. In practical terms, the degree of effort required to fulfil the requirements of the IS 27001 clauses will not be unitary across all clauses (and indeed, an agreed or widely-acceptable weighting would be extremely difficult to state precisely).

The assessment was a 'desk review' of Evantix's offering and has not sought to take into account the quality of responses which a respondent may submit. The value of any respondent's replies will require that the questionnaire has been faithfully completed, that their replies are accurate and contextually relevant and that the respondent is knowledgeable about their own system(s) and the framework within which the questions are set.

Although it is noted that there are questions directly related to the requirements of IS 27001 these do not address all of the clauses of that standard, nor do they elicit any more than a simple 'Yes' or 'No' from the responder, and hence do not delve into any greater detail, as do other questions in the ECF.

In the absence of any auditing, responses are based entirely upon the respondents, replies and therefore dependent solely upon their un-validated disclosures. Notwithstanding the veracity and accuracy of respondent's replies to the questions set by Evantix, and although the ECF overall has comprehensive coverage of the subjects addressed and required by IS 27001, favorable responses to the ECF's questions do not necessarily mean that a respondent's conformity to IS 27001 is a given nor that such conformity could be easily accomplished, since a variety of other, likely unknown and un-assessed, factors may come into play.

Such factors may be, inter alia, the lack of knowledge as to the depth of implementation of information security management measures on the respondent's part, the maturity of their ISMS (if indeed they have one), and the falsehood of assuming that each of the IS 27001 requirements has equal weighting or significance in comparison to its counterparts.

Whilst it is reasonable to expect that auditing the respondent is likely to strengthen confidence in the results obtained through the ECF, Zygma has not been asked to assess the nature or competence of the auditing processes applied by Evantix and its business partners and hence offers no opinion on that subject. Where the audit is undertaken by a certified IS 27001 auditor it would be reasonable to expect that greater understanding of and confidence in the respondent's conformity would become evident.

Conformity to IS 27001 cannot be assumed to be a non sequitur based simply on the fact that a set of responses to the IS 27001 ECF have a high level of favorable responses.

For 1st Parties using the ECF to assess 3rd Parties, the questions in the ECF and specific processes and controls exercised through the use of Evantix's offerings will support the 1st Party's conformity to IS 27001 across a nominal 46% of the standard's clauses. This figure is subject to the preceding

caveat concerning comparative weighting of IS 27001 clauses. 'Support' means that Evantix's offerings will not be a complete resolution for conformity to any IS 27001 requirements, since it is for the 1st Party to manage and take primary responsibility for their conformity, not for another party to exercise it for them.

1st Parties may choose to use Evantix's IS 27001 questionnaire framework internally for application to its own business units (i.e. as pseudo-3rd Parties). Only a formal IS 27001 assessments could render a determination as to the extent of that 1st Party's conformity to IS 27001.

The extent to which the 1st Party is reliant upon Evantix's offerings to operate its business will clearly affect the extent to which their individual IS 27001-conformity is underpinned by the support offered by Evantix's services: A large business with a small number of respondents managed using Evantix's offering will obviously have a much smaller proportion of its overall information security management reliant upon Evantix than would a small business acting as an integrator of services provided my multifarious respondents, all of which were managed using Evantix's offering. Thus, even though Zygm's findings reflect the general support offered by Evantix's offerings, individual clients will benefit to the extent determined by their particular profile and usage of Evantix's offerings, and no blanket conclusions can be drawn.

Zygm's opinions as set forth in this report relate only to the material it has reviewed first-hand, information described by Evantix's representatives and to Evantix's e-Business Risk and Compliance offering. Nothing in this report expresses any opinion regarding the actual state of information security management within Evantix itself, nor in any of its clients, partners, respondents or other form of affiliate, nor to the correctness of function within the offering including its suitability for use by any party, nor as to the competence of any audit framework or actual audits or auditors in any way related to the Evantix offering.

The review was performed over the period 2008-07-14 to 2008-10-14 and was based on the following Evantix documents at the publication dates stated.

Doc. Title	Doc. Version / date released or provided
Patent Application for A METHOD AND SYSTEM FOR ASSESSING, MANAGING, AND MONITORING INFORMATION TECHNOLOGY RISK	2008-08-06
Evantix Survey Framework Draft	V30b, 2008-08-12
QA process for Evantix control model	2008-08-15
Risk & Compliance Manager Solution PPT presentation	v49
Relationship Survey	v23
Evantix RCP FRD – 3 rd Party Qualification	V1.0
Evantix Business Operations Contact Center Service Delivery, & Client Support	2008-10-01