Email Governance: Are Companies in Financial Industries More Mature?

Gerhard F. Knolmayer, Lukas E. Helfenstein, Gabriela Loosli
University of Bern
{gerhard.knolmayer, lukas.helfenstein, gabriela.loosli}@iwi.unibe.ch

Georg W. Disterer
University of Applied Sciences and Arts Hannover
georg.disterer@fh-hannover.de

Abstract

Emails have drastically changed the way companies and employees communicate. Some Emails are business-relevant and have to be kept for documentation, external and internal audits, and for legal evidence. Many companies defined rules for handling Emails to comply with external and internal requirements.

In this paper we describe indicators for good Email practices and develop a maturity model by weighting these indicators. We sent questionnaires concerning Email policies to the largest German and Swiss companies. The resulting data set was used to analyze whether there are significant differences in the maturity of Email governance between companies belonging to the financial industries and other companies. For many indicators we found that companies belonging to the financial industries look more mature from a descriptive point of view; some differences are also statistically significant. After computing aggregate maturity scores we found a highly significant difference between the two groups of companies.

1. Introduction

In the last 15 years, Email technology has gained broad acceptance and massively changed communication means and style in both business and private life. Emails have become a mass communication phenomenon: It is estimated that in 2010 an average of almost 300 billion Emails were sent per working day [54]. In a survey, two thirds of the respondents estimated that more than 25% of the Emails have business-relevant content; one third assumed even 50% [51]. It has been estimated that from a governance perspective 70% of all Emails have to be archived [38]. Like other types of documents that are relevant for recording business activities, business-relevant Emails must fulfill external and internal audit requirements. However, no standards or unambiguous recommendations how companies should deal with Emails have evolved.

Managing Emails is a subtask of records management [4][13][31][53]. Many companies are quite skeptical about the maturity of their records management; for instance, in 2006 only 26% of internationally operating Swiss companies and only 12% of primarily locally oriented Swiss companies assigned themselves to the two most mature levels on a six-level maturity-scale [42]. Emails have been characterized as the worst managed form of records [44].

In recent years, shady or unethical behavior by some companies has led to increased interest in Corporate Governance and, as an important aspect of it, also in IT Governance [8][11][26][55][56][59]. Several spectacular cases have been described in which companies were blamed behaving unethically, e.g., in relationships with their customers or their personnel. There have been media reports about Emails expressing internal viewpoints diametrically opposed to recommendations given to customers by finance consultants. Emails have been used in litigations concerning environmental catastrophes, fiscal fraud, or as evidence of bullying in workplace conflicts [2][12][16]. In legal procedures companies have been requested to provide authorities with information on the content of Emails at very short notice.

The remainder of this paper is organized as follows. Section 2 reviews previous literature on Email policies and archiving, and summarizes some only partially solved issues. In Section 3 we discuss maturity models and develop an Email maturity model based on quantitatively measurable indicators. We argue that Companies in the Financial Industries (CFI) (i.e. banks and insurance companies) are highly regulated and have to be notably careful in communication with their customers. The importance of Email governance in the
financial industries is emphasized, e.g., in [33][36][61]. We therefore formulate the hypothesis that CFI have elaborated more mature Email policies than Companies belonging to Other Industries (COI). Section 4 describes an empirical analysis of this hypothesis, based on a questionnaire sent to large German and Swiss companies. Section 5 provides descriptive and confirmatory results for industry-specific differences in single maturity indicators and in an aggregate maturity score. The final Section, 6, summarizes the results and indicates further research opportunities.

2. Previous research on Email governance

Thus far Email governance is primarily discussed from a practitioner’s perspective, providing recommendations and guidelines [18][19][22][23][35][41]; many of them are influenced by consultancy or tool offerings. From the viewpoint of records management, Emails are documents that may qualify as records if they are business-relevant; the specific problems resulting from the fact that Emails are a ubiquitous mass phenomenon are not focused in this type of literature [1][45][47][48]. The risks of Email communication have thus far not found much interest in the scientific community.

Most business transactions do not postulate a specific form of agreement. Therefore also non-traditional media can carry legally valid, business-relevant content which should be managed based on its business, legal, compliance, operational, or historical value, disregarding the casualness of its creation or its storage medium (cf. [19]). Because qualifying Emails are business records, the laws and regulations that apply to other business records are also relevant for them.

Due to the impact of Emails in daily work, many companies aim to influence Email communication by means of “Email policies” to reduce the associated business risks. The importance of defining policies and rules and of adhering to them is stressed, e.g., in [5][18][19][22][35][41]. It is recommended to keep policies short [47] and to educate the users about the rationale behind the policies [1].

Several laws and other regulations prescribe that at least Emails with certain types of content must be archived, kept for some time, and made accessible at short notice; lists of such regulations are given, e.g., in [1][4][9][33][53]. One possible procedure could be to archive all Emails. However, not all messages generated by a company have to be retained [19]. In addition to the resulting storage volume, privacy regulations may be hard to follow if users send or receive private Emails. A company may prohibit the private use of business Email accounts [4][18]. This rule, however, may be unrealistic and out of time; employees may not be able to prevent the receipt of private Emails. If the users are allowed to declare incoming Emails as private, a time-lag between receiving and archiving Emails must be provided which could be misused for non-compliant behavior.

If only “business records,” defined as information providing evidence of a company’s business-related activities, events, and transactions [19], are archived, responsibilities for archiving decisions have to be defined [4][19][47]. Deciding which Emails are business-relevant and especially classifying these Emails are time consuming tasks. Artificial intelligence-based auto classification categorizes Emails according to rules. Because categorization errors are inevitable, it has been suggested to keep additionally a copy of every Email to close possible gaps or even to install a hybrid system in which employees have to confirm the suggested classification [19].

If classification is done by users, the company should make sure that the coding lists are simple [19]. Another suggestion to make the task easier is to organize mailboxes like mini-file plans (according to a corporate-wide file plan) so that information belonging together is contained in the same dossier which may be related, e.g., to a business process, a customer relationship, or a lawsuit, together with other types of documents [4][47][53].

It has also been suggested not only to capture the record documenting a final decision but also statements that might indicate why the decision was made [47].

Because the content of Emails may constitute a (legal) risk for the company it is recommended to retain only what is required [4][19] and establish and enforce rules for deleting messages not needed any longer.

Companies seem to struggle in establishing and enforcing business rules for creating, handling, archiving, and erasing Emails. Main reasons why these tasks are difficult to fulfill are [28]:

- Emails are often formulated in an informal language that resembles that of a telephone call more than of a business letter. An unguarded formulation may be wrongly interpreted and provide a negative impression if taken out of context. In lawsuits these weaknesses are interesting prospects for opponent parties, even if they only make a case time consuming and expensive [19].
- Regulations are not very specific in determining requirements for good business practice, especially in areas with rapid technological change. Thus, there are no explicit and clear statements on which Email policies are considered to be compliant with respect to certain regulations.
Maturity models aim to support companies in analyzing their actual performance, in developing policies and measures for improvement, and in controlling the implementation of policies and measures. Providing companies with checklists or questionnaires gives them the chance for self-assessments (as-is situation) in order to compare their scores with those of other companies [3].

With respect to Email governance no established policies and measures to assure compliance exist. Therefore it is difficult for companies to analyze and to assess their own procedures. Tampe [51] suggested the subsequent Maturity Model for Email Management:

1. Aware: There is a awareness that problems and risks exist but the company has taken little action. They use spam- and virus-filters. Storage is done unorganized through local files/folder.

2. Reactive: Awareness and action occur in response to issues. Action is either system- or department-specific. Companies use Hierarchical Storage Management to migrate data and introduce low-level regulation for usage of private Emails.

3. Proactive: The organization places much greater importance on Emails. Companies start to centralize action. Central archiving and basis search capabilities are provided. Partially existence of company-wide rules.

4. Managed: Email is managed as an enterprise asset, well-developed processes for capturing, classification, verification and storage exists. Organizations provide detailed rules and internal control systems.

5. Optimized: Email Management is a strategic initiative. Focus is on continuous improvement of rules and verification. Connections to compliance cockpits.

As in most other maturity models, the maturity levels are only defined verbally, and the indicators used to distinguish the levels are not clearly defined. Even at the lowest maturity level, [51] assumes that companies are aware and use some tools for Email management. Moreover, how would a company be classified which collects data about Email management in a compliance cockpit (cf. Level 5) but without existence of company-wide rules (cf. Level 3) and with local folders (cf. Level 1)? Thus, when applying maturity models the assignment of a firm to a certain maturity level may be ambiguous.

Another maturity model for Email management [42] distinguishes 6 maturity levels, differentiatated as levels 0 to 5. It is argued that level 3, characterized by standardized procedures but missing control, has to be reached for compliance and that aspiring maturity level 5 may be uneconomical if the company is not exposed to very high risks.

In this paper we propose a maturity model which uses 29 well-defined and measurable indicators. The
definition of these indicators is based on literature analysis, expert speeches, and interviews. We arrange these indicators in five groups, as shown in Table 1. The indicators in Group 3 are operationalized on 5-point Likert scales, all other indicators by Yes/No responses.

In the following we give reasons why we have chosen these indicators (cf. Table 1). Many companies define policies for using their IT systems (cf. Indicator Groups 1 and 2). Often guidelines for using Email systems are part of these broader IT policies. We assume that a company which is defining detailed Email policies is more mature with respect to Email governance than a company without a policy or only a cursory one.

However, the existence of policies is only one side of the coin, and awareness and observance of these policies are additional maturity indicators (Group 3). Automated procedures may be implemented to guarantee the observance of rules. We consider the existence of such procedures as further indicators of mature Email governance (Group 4).

In widely discussed cases, companies were unable to present Emails to legal authorities within an appropriate period (cf., e.g., [12]). We assume that these cases have caught the attention of compliance managers, and regard the existence of archiving and extinction procedures as a very important indicator of mature Email governance (Group 5).

Assigning a weight to each indicator is a prerequisite for defining an operational maturity model. Operationalization has also been suggested for the COBIT maturity model [46] and in [21] this property is regarded as essential for a “Governance and Compliance Maturity Model”. The weights were chosen before sending the questionnaire. Their sum is 99; thus, the aggregate maturity score (ams) is bounded by 0 and 99. As in other maturity models, we distinguish five levels and assign the ams to maturity levels (Table 2). Based on ams we can assign each company in a traceable way to one of the five maturity levels.

Empirically determining the indicator weights in a survey was considered as too complex. Thus, the weighting reflects subjective decisions which were based on statements in the literature and on discussions with experts. Within one indicator class we selected identical or similar weights to avoid the potential impression of manipulation. Compared to other maturity models, which are also based on subjectively defined features, the procedure suggested is more comprehensible.

Dependencies between the indicators and their weights exist. For instance, one could argue that the 5 points given to indicator 1.1 (Table 1) expresses undervalued importance. However, a firm without Email policies will also receive no points from indicators 1.2, 1.3, and from indicator groups 2 and 3. Thus, the weight given to the existence of detailed Email policies is implicitly much higher. At first glance the 43 points associated with archiving and extinction may appear high; however, this excludes that a company with inadequate archiving procedures is assigned to maturity levels 4 or 5.

One may presume that companies belonging to highly regulated industries generally follow more compliance-oriented business procedures than others. Among the most highly regulated industries are the life sciences and financial industries. Regulations in life sciences industries are more product and process oriented than communication oriented. In the financial industries the information exchange with customers is considered as more sensitive than in other industries. It seems worth to investigate whether the regulations in the financial industries lead to a more compliance-oriented business practice also in areas for which requirements and good practices are (thus far) not precisely formulated. In particular, one could assume that the rules defined and the procedures implemented with respect to handling Emails are more mature in the financial industries than in other industries [60]. Therefore, we formulate the following hypothesis:

Companies belonging to financial industries have a more mature attitude towards Email governance than companies belonging to other industries.

4. Design of the empirical study

The empirical study used a questionnaire entitled “Governance of Email Communication,” which is based on issues discussed in [28]. It was pre-tested in interviews with IS executives, and sent to the 827 largest companies located in Germany and in Switzerland (Table 3). Data was obtained from the list of Top German Companies published by Die Welt and the list of Top Swiss Companies published by the Handelszeitung. Some obvious corrections had to be made, mainly for changes occurring since their publication. Size was measured by consolidated revenues for companies focusing on production, commerce, and services, by balance sheet totals for banks, and by premium incomes for insurance companies. As the number of large companies in Switzerland is smaller than in Germany, fewer companies were selected in Switzerland, to reduce effects of company size. The response rate was 11.4 % (cf. Table 3). The numbers of usable responses differ because of unanswered questions and “Don’t know” responses; low numbers of responses exist in particular to questions about archiving procedures (cf. Indicators 5.2-5.6) because many companies did not systematically archive Emails.
Table 1. Indicators for Good Email Governance

<table>
<thead>
<tr>
<th>#</th>
<th>(Group of) Indicators</th>
<th>COI [%]</th>
<th>CFI [%]</th>
<th>p-values for differences</th>
<th>Weights</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Policies for Email Handling</td>
<td></td>
<td></td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>1.1</td>
<td>Has your company formulated policies that control users’ handling of Emails?</td>
<td>90</td>
<td>100</td>
<td>0.095</td>
<td>5</td>
</tr>
<tr>
<td>1.2</td>
<td>Have (at least parts) of these policies been communicated to your employees in writing?</td>
<td>95</td>
<td>96</td>
<td>0.655</td>
<td>3</td>
</tr>
<tr>
<td>1.3</td>
<td>Did the employees confirm the notice of these policies in writing?</td>
<td>50</td>
<td>44</td>
<td>0.396</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Content of the Email Policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>The Email policy specifically prohibits harassing, abusive, intimidating, or other offensive Emails</td>
<td>82</td>
<td>88</td>
<td>0.330</td>
<td>2</td>
</tr>
<tr>
<td>2.2</td>
<td>The Email policy specifically states obligations to respect confidentiality, privacy, and data protection</td>
<td>92</td>
<td>96</td>
<td>0.409</td>
<td>2</td>
</tr>
<tr>
<td>2.3</td>
<td>The Email policy specifically states that Emails should be treated as official business documents although sometimes containing informal and causal wording</td>
<td>47</td>
<td>63</td>
<td>0.158</td>
<td>2</td>
</tr>
<tr>
<td>2.4</td>
<td>The Email policy specifically states that management may access and disclose employees’ Emails unless they are marked as private</td>
<td>51</td>
<td>67</td>
<td>0.147</td>
<td>2</td>
</tr>
<tr>
<td>2.5</td>
<td>The Email policy specifically states that confidentiality of Emails is low unless they are encrypted</td>
<td>70</td>
<td>88</td>
<td>0.066</td>
<td>2</td>
</tr>
<tr>
<td>2.6</td>
<td>The Email policy requests encryption of sensitive Emails</td>
<td>67</td>
<td>68</td>
<td>0.558</td>
<td>2</td>
</tr>
<tr>
<td>2.7</td>
<td>The Email policy only permits utilization of encryption methods that are officially released for company use</td>
<td>44</td>
<td>63</td>
<td>0.099</td>
<td>2</td>
</tr>
<tr>
<td>2.8</td>
<td>The Email policy specifically addresses the risk of receiving special attachment formats that contain malicious code more often than others</td>
<td>75</td>
<td>75</td>
<td>0.602</td>
<td>2</td>
</tr>
<tr>
<td>2.9</td>
<td>The Email policy prohibits forwarding business Emails to private Email accounts</td>
<td>47</td>
<td>92</td>
<td>0.000***</td>
<td>2</td>
</tr>
<tr>
<td>2.10</td>
<td>The Email policy prohibits sending business Emails from private Email accounts</td>
<td>29</td>
<td>68</td>
<td>0.001***</td>
<td>2</td>
</tr>
<tr>
<td>2.11</td>
<td>The Email policy mentions “Good Practices” for Email communication (e.g., using reasonable subject lines, avoiding unnecessarily long distribution lists)</td>
<td>65</td>
<td>67</td>
<td>0.548</td>
<td>2</td>
</tr>
<tr>
<td>2.12</td>
<td>The Email policy requests to automatically send absence notices or forwarding Emails to a substitute</td>
<td>52</td>
<td>83</td>
<td>0.006**</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Relevance of Email Policies in Day-to-Day Work</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>How do you assess the present awareness of employees about the Email policies on a 5-point scale?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2</td>
<td>How do you assess the present observance of the Email policies by employees on this scale?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Automated Procedures Supporting Email Governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>Procedures to prevent forwarding Emails to apparently private Email accounts</td>
<td>23</td>
<td>35</td>
<td>0.206</td>
<td>2</td>
</tr>
<tr>
<td>4.2</td>
<td>Procedures to encrypt (all or specified) outgoing Emails</td>
<td>13</td>
<td>15</td>
<td>0.484</td>
<td>2</td>
</tr>
<tr>
<td>4.3</td>
<td>Procedures to prevent end-to-end encryption (e.g. PGP) of outgoing Emails</td>
<td>4</td>
<td>25</td>
<td>0.010**</td>
<td>2</td>
</tr>
<tr>
<td>4.4</td>
<td>Procedures to delete locally stored Email archives (e.g. PST-files of MS Outlook)</td>
<td>2</td>
<td>15</td>
<td>0.038*</td>
<td>2</td>
</tr>
<tr>
<td>4.5</td>
<td>Procedures to limit mailbox quotas</td>
<td>82</td>
<td>92</td>
<td>0.202</td>
<td>2</td>
</tr>
<tr>
<td>4.6</td>
<td>Procedures to relocate Emails to alternative storage media after a certain retention period</td>
<td>54</td>
<td>59</td>
<td>0.497</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>Email Archiving and Extinction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1</td>
<td>Has your company defined general policies that address archiving of Emails?</td>
<td>56</td>
<td>71</td>
<td>0.149</td>
<td>13</td>
</tr>
<tr>
<td>5.2</td>
<td>If not: Are such policies defined for dedicated departments or levels of hierarchy?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.3</td>
<td>Have (at least parts of) these policies been communicated as written “Archiving Policy” to all employees?</td>
<td>74</td>
<td>82</td>
<td>0.371</td>
<td>6</td>
</tr>
<tr>
<td>5.4</td>
<td>Are attachments of Emails dealt like the bodies of the Emails in archiving procedures?</td>
<td>91</td>
<td>88</td>
<td>0.533</td>
<td>6</td>
</tr>
<tr>
<td>5.5</td>
<td>Are Emails marked or detected as private excluded from archiving procedures?</td>
<td>30</td>
<td>40</td>
<td>0.365</td>
<td>6</td>
</tr>
<tr>
<td>5.6</td>
<td>Is the integrity of the Email archive checked (e.g., whether it is unaltered and recoverable)?</td>
<td>36</td>
<td>40</td>
<td>0.531</td>
<td>6</td>
</tr>
<tr>
<td>5.7</td>
<td>Has your company defined rules for extinction of archived Emails (after certain retention periods)?</td>
<td>33</td>
<td>41</td>
<td>0.403</td>
<td>6</td>
</tr>
</tbody>
</table>

Legend: *** significant at 99.9%; ** significant at 99%; * significant at 95%.
Table 2. An operationalized maturity model for Email governance

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Minimum Score</th>
<th>Maximum Score</th>
<th>Description of Maturity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>19</td>
<td>Unprofessional</td>
</tr>
<tr>
<td>2</td>
<td>20</td>
<td>39</td>
<td>Aware but only limited organizational implementation</td>
</tr>
<tr>
<td>3</td>
<td>40</td>
<td>59</td>
<td>Either detailed Email policies or (some) archiving procedures implemented</td>
</tr>
<tr>
<td>4</td>
<td>60</td>
<td>79</td>
<td>Detailed Email policies defined and archiving procedures partially implemented</td>
</tr>
<tr>
<td>5</td>
<td>80</td>
<td>99</td>
<td>Detailed Email policies defined; handling and archiving Emails has reached a high professionalism</td>
</tr>
</tbody>
</table>

Table 3. Data about the survey

<table>
<thead>
<tr>
<th></th>
<th>Germany</th>
<th>Switzerland</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of questionnaires sent</td>
<td>540</td>
<td>287</td>
</tr>
<tr>
<td>Number of questionnaires sent to companies belonging to financial industries</td>
<td>70</td>
<td>87</td>
</tr>
<tr>
<td>Number of analyzable questionnaires received</td>
<td>46</td>
<td>48</td>
</tr>
<tr>
<td>Number of analyzable questionnaires received from companies belonging to financial industries</td>
<td>12</td>
<td>14</td>
</tr>
<tr>
<td>Number of analyzable questionnaires received from companies belonging to other industries</td>
<td>34</td>
<td>34</td>
</tr>
</tbody>
</table>

The questionnaires were addressed to the Chairmen of the Supervisory Boards who have topmost responsibility for compliance. We assumed that it would be easier to win the attention and support of these persons by a paper-based questionnaire than, e.g., by a Web-based survey. A reminder was sent two months later. The questionnaire could be answered anonymously. The type of industry in which the company is primarily active was one of the first questions, and this question was answered by all companies but one.

5. Results of the empirical study

5.1. Descriptive results

Based on our hypothesis we assumed that there might be differences between CFI and COI in some values of the indicators shown in Table 1. Columns 3 and 4 of Table 1 show the percentages of companies affirming the respective indicators. When considering all 29 maturity indicators, CFI were found to have lower values than COI for only 3 of them (1.3, 3.2, and 5.3).

In 2001, more than 81% of large US companies had formulated policies governing their employees’ use of Email [19]. Our study determined the corresponding value as 92% for large German and Swiss companies. All responding CFI and almost all responding COI had formulated Email policies. The percentage of companies communicating written Email policies is slightly higher than those found for Singapore in 2005 [44]. Email policies of CFI are more detailed than those of COI (Indicator Group 2).

Figure 1 shows the distribution of answers for the two groups of companies in the five classes defined for the indicators in group 3 and also gives the percentages for each class; Figure 2 indicates the corresponding averages. In all figures the bars in the lighter shade of gray refer to COI and the darker ones to CFI. The percentages of highly and very highly aware resp. observant users (cf. Figures 1 and 2) are lower than the 85% resp. 74% found for Singapore in 2005 [44].

Automated procedures to support advanced governance rules are applied rarely (Group 4). The issue of access to end-to-end encrypted Emails is considered only by a few companies. The need to enforce retention and disposal policies for locally stored Email messages is emphasized, e.g., in [37], but such policies are implemented rarely [29].

Figure 1. Awareness and observance of Email policies
The percentage of companies with policies for archiving Emails is with 59% higher than the 43% reported in [24] and the 46% indicated in [51]. In [58] 33% of the respondents claimed to archive all Emails and 54% to archive selected Emails. Another study found that 68% of the respondents were not satisfied with their companies’ Email archiving rules [43].

5.2. Confirmatory results

In a first step we used nonparametric test methods to determine whether the differences of the indicator values for CFI and COI are statistically significant. We applied one-sided significance tests because of the hypothesis formulated in Section 3. The one-sided Mann-Whitney U-Test was used for the ordinal scaled indicator values in Group 3, and the Exact Fisher Test for the nominal scaled indicator values (Yes/No responses in Groups 1, 2, 4, and 5). Table 1 shows for each indicator the p-value obtained for the difference between COI and CFI. We consider a difference as significant if the p-value is smaller than 0.05. All differences in which the COI value was higher than the CFI value are not statistically significant. In 5 cases the higher indicator values of CFI were identified as a significant difference. We add some comments on these differences.

We detected very highly significant differences (0.001 level) in the Email policies of CFI and COI with respect to using private Email accounts for fulfilling business tasks (Indicators 2.9 and 2.10). One of the problems of Email governance mentioned in Section 2 is caused by employees using their private Email account(s) offered (typically free), e.g., by Google, Microsoft, and Yahoo, for business-relevant communication. The use of private Email accounts may be in the interests of the company if the employees do not have remote access to their business Email accounts to provide rapid answers in time-critical communication. However, there are high risks associated with such a procedure, e.g., with respect to security of the Email content and completeness of documentation if Emails sent from the private account are not copied to the business account. According to [40], 63% of the employees frequently or sometimes send Emails and company data to their private Email accounts. Osterman Research found that more than 16% of the employees regularly communicated about business issues by using private Email accounts [24]. It seems that many companies outside the financial industries have not recognized the risks caused by using private Email accounts in business activities.

In CFI, timely fulfillment of an order must be guaranteed even when the addressee of the Email is absent. Therefore, it is not surprising that CFI pay highly significantly (0.01 level) more attention to substitution arrangements and Email forwarding than COI do (Indicator 2.12). The same holds for preventing end-to-end encryption, which circumvents access to the archived Emails (Indicator 4.3). The difference is significant but in both groups of firms this issue is often neglected. Also retention and disposal policies for locally stored Email messages are rarely implemented; although at a low level, CFI are again significantly more active than COI with respect to this issue (Indicator 4.4; 0.05 level).

In a second step we weighted the affirmative answers of the respondents obtained for the Indicator Groups 1, 2, 4, and 5 with the weights defined in Table 1. The indicator scores in group 3 were added, e.g., with a score of 5 for a very high assessment, of 3 for a middle assessment, and of 1 for a very low assessment. Thus, we obtained an aggregate maturity score for each company, which we used to assign the company to one of the maturity levels defined in Table 2. Figure 3 shows the results. 46% of the CFI but only 22% of the COI are assigned to the highest maturity levels 4 and 5. The average aggregate maturity score for CFI is 3.31 and 2.75 for COI. We also performed sensitivity analyses with different weighting vectors and obtained similar differences for “reasonable” weights.
The one-sided Mann-Whitney U-Test is appropriate for testing the significance of the difference. It shows that the difference between the maturity of Email management between the two groups of companies is highly significant (0.01 level). This supports our hypothesis that the maturity of Email governance is higher in companies belonging to the financial industries than in other companies.

6. Conclusion and Outlook

This paper considered the Governance of Email communication, which is, of course, only a small element of IT Governance, and an even smaller aspect of Corporate Governance. However, today many compliance officers and CIOs are struggling to implement robust policies for creating, handling, archiving, and erasing Emails. The literature provides arguments why such policies are possibly more important for companies belonging to the financial industries (CFI) and why these companies should have reached a more mature status of defining, implementing, and controlling policies and procedures than companies in other industries (COI).

Based on our survey on Email policies of large German and Swiss companies, we obtained for 25 of 29 characteristics data indicating higher maturity for CFI than for COI. However, testing these differences for significance with nonparametric test procedures revealed that only 5 of them were significant at the 0.05 level. In contrast, the aggregate view, based on aggregate maturity scores computed from the 29 single indicators, showed at the 0.01 level a significantly higher maturity of companies in the financial industries than in other companies. It could be helpful if companies in the financial industries would share their knowledge and experiences in this area with their customers.

Besides the support for our hypothesis, a main contribution of the paper is the development of an operational maturity model which supports companies in analyzing and assessing their current Email governance and in improving it. The list of indicators can also be used as checklist for a self-assessment and for comparisons with peer companies. Companies may derive improvement measures from the model. Further research could evaluate and refine the maturity model by broader empirical evidence.

This research focused on large German and Swiss firms. There is broad consensus that the common practice of Email governance in small and medium-sized companies is less professional than in large companies. Using other communication channels than Email for business purposes may cause additional risks; for instance, our respondents confessed that governance of Instant Messages [17][39] and business-relevant Chats is at a clearly lower maturity level than Email governance [15]. Handling business-relevant SMS, which will typically be mixed with private messages, in a compliant way seems to be an unsolved issue. In any case, a more intense exchange of experiences and viewpoints between companies should be valuable in this area which suffers from lack of clarity.

7. References


[54] H. Tschabitscher, How Many Emails Are Sent Every Day?
http://email.about.com/od/emailtrivia/f/emails_per_day.htm
http://searchfinancialsecurity.techtarget.com/tip/Email-security-and-compliance-best-practices