Paper 025-2011

Global Risk Management: How SAS® Enterprise GRC Manages Nonfinancial Risk in a Distributed Enterprise

Victor (Guowei) Jiang, Hao Qiu, SAS Institute Inc., Beijing, China

ABSTRACT

SAS Enterprise GRC (governance, risk management, and compliance) is a SAS solution to help customers automate the management of nonfinancial risks (for example, strategic risks, operational risks, reputational risks, and so on), compliance, and internal audit processes. This paper depicts the scenario of a global bank with several branches in different countries (U.S., China, Saudi Arabia, and Japan): HQ sets up a multilingual environment; clerks in local offices input loss data in different languages; language-specific e-mail messages are sent in the approval process; the loss data are collected and assembled in HQ and finally generated into different language reports.

INTRODUCTION

WHAT'S GRC?

GRC is an integrated, holistic approach to organization-wide governance, risk, and compliance, ensuring that an organization acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology, and people, thereby improving efficiency and effectiveness. This definition is translated into a frame of reference as below.

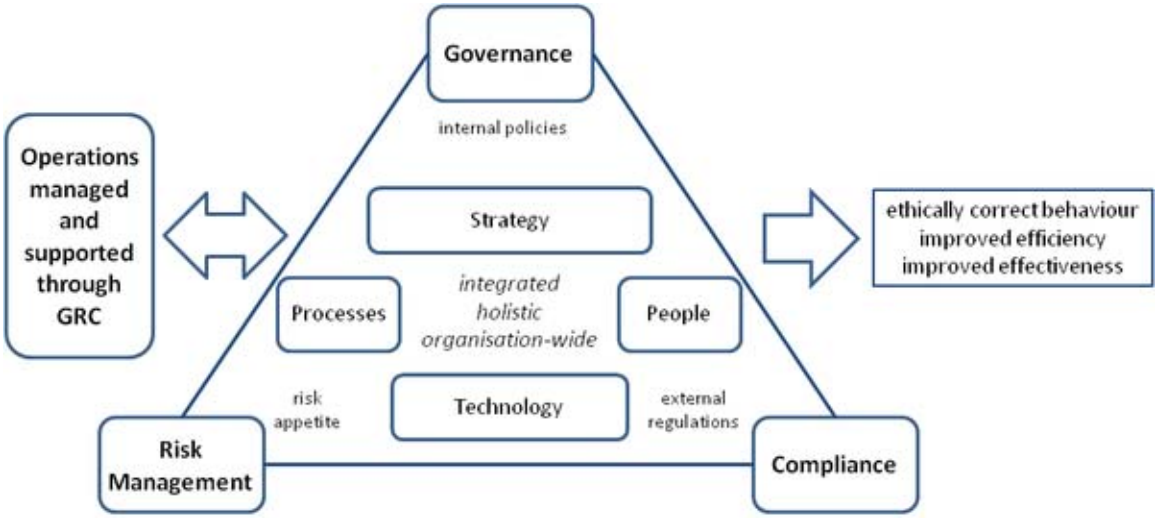


Figure 1. Frame of Reference for GRC Research

Nonfinancial risk such as operational risk is an important aspect of GRC management.

WHAT IS GRC SOLUTION?

GRC solution is a type of application used to automate the management of governance, risk management, and compliance data. There are many challenges for a GRC solution used in a distributed enterprise, including the following:

- Clerks in different countries hope to see the product with their own languages.
- Clerks in Saudi Arabia hope to see layout of the product rendering from right to left.
- Clerks in different countries can use date, time, number, and currency formats with local conventions.
- Clerks in a branch are permitted only to manipulate data within their own region.

- Internal control rules in different countries are also different. Clerks should be able to customize workflows to fit various rules.
- Different branches have different business structures.

WHAT IS SAS ENTERPRISE GRC?

SAS Enterprise GRC is a user-friendly, Web-based GRC solution by SAS that automates the management of governance, risk, and compliance data across the enterprise within a single integrated platform.

SAS Enterprise GRC facilitates the entry, collection, transfer, storage, tracking, and reporting of operational losses, gains, recoveries, and key risk indicators (KRIs) that are drawn from multiple locations across an organization.

It can also be used to do the following:

- Conduct audits
- Manage policies
- Conduct risk and control assessments
- Test controls
- Investigate incidents
- Create and track issues and develop action plans
- Scenario analysis

Figure 2. Screenshot of SAS Enterprise GRC

SAS Enterprise GRC is powerful and able to support multiple-language deployment and implementation for a distributed enterprise very well. Let us see it from the following scenario.

A SCENARIO OF A GLOBAL BANK

iFinance, a global bank, owns branches in four countries, including the U.S., China, Saudi Arabia, Japan, and headquarters in the U.S. iFinance uses SAS Enterprise GRC to manage loss incidents, including the process of creation, investigation, validation, and reporting.

iFinance has various business lines as Ffigure 3 shows.

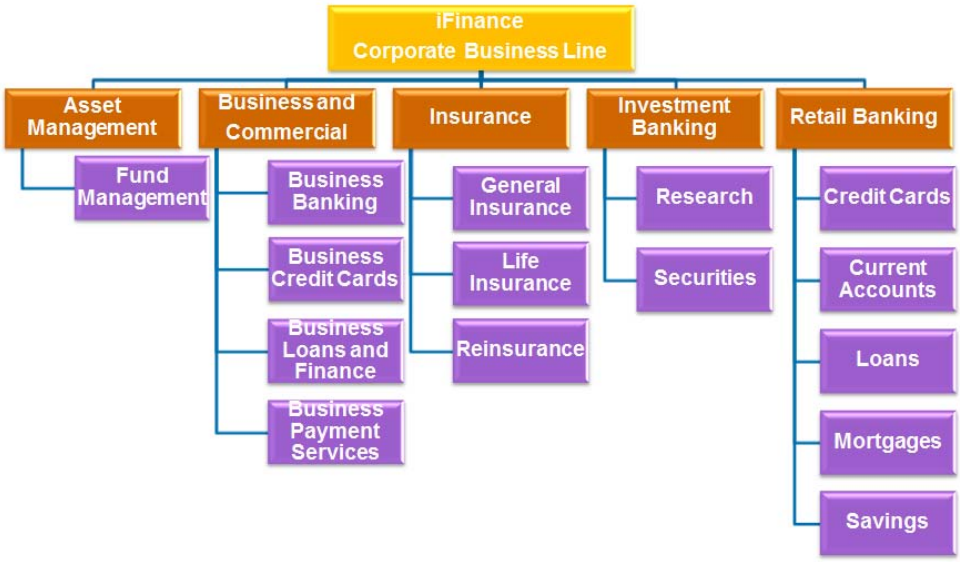


Figure 3. iFinance Corporate Business Line

In 2010, a rogue trader in the U.S branch uses insider information to make trades on securities. iFinance is fined $200,000 by Securities and Exchange Commission accordingly. Similar incidents also occur in the China, Japan, and Saudi Arabia branches. They are fined 200,000 Chinese Yuan, 200,000 Japanese yen, and 200,000 riyal respectively.

Branch	Loss Amount
U.S.	200,000 Dollars
China	200,000 Chinese Yuan
Japan	200,000 Japanese Yen
Saudi Arabia	200,000 Riyal

Let us see how iFinance makes use of SAS Enterprise GRC to manage those incidents.

INCIDENT MANAGEMENT PROCESS

This is a chart to show the management process of how incidents are tracked and reported.

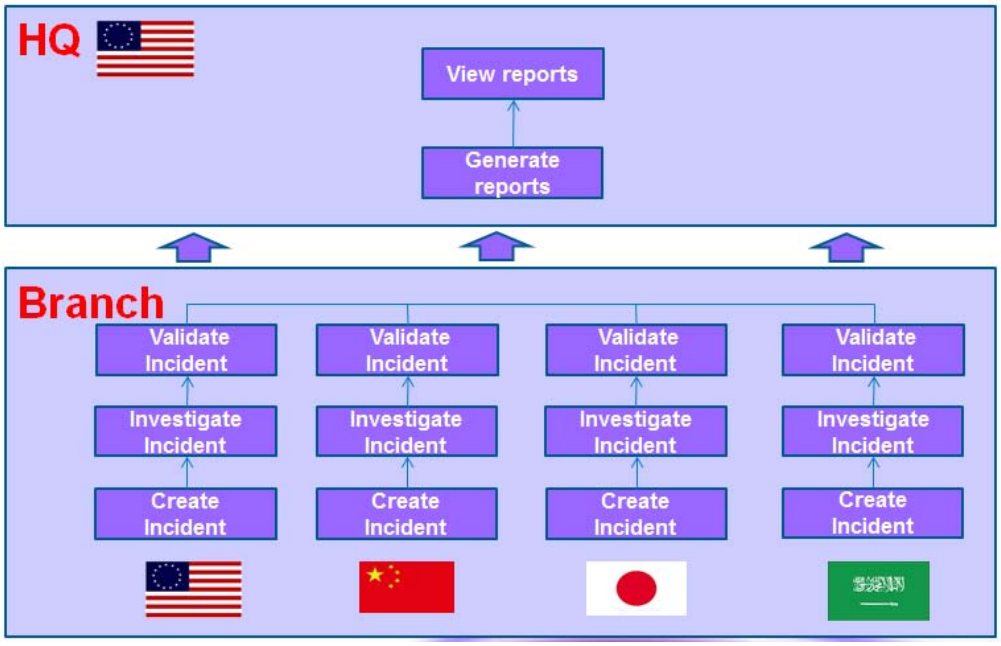


Figure 4. Incident Management Process

The incident management process is completed using the following five-phase steps in SAS Enterprise GRC:

1. Setup Environment

The administrator in headquarters is responsible for setting up a multilingual environment and preparing all data, such as all types of workflows and thresholds in SAS Enterprise GRC.

2. Create Incident

Incident creators in each branch discover an event has occurred and create an incident.

3. Investigate Incident

Incident investigators in each branch accept the incident, investigate the incident, and provide details about the following items:

- financial and nonfinancial effects
- recoveries
- allocations
- causes
- failed controls

One or more investigators can be involved in this stage to capture the required data. After all information has been gathered by all parties, the incident is sent for validation.

4. Validate Incident

Incident validators in each branch review and validate the incident. One or more validators can be involved in this stage. The validation process repeats until the responses have been verified at all workflow stages. After all required validators have approved the incident details, the incident is fully validated.

5. View Report

The reports are generated and viewed by managers. Please note that clerks in the U.S., China, Japan, and Saudi Arabia will create, investigate, and validate incidents respectively. Let us look at each step in detail.

1) SETUP ENVIRONMENT

First of all, the administrator in headquarters sets up the environment and prepares all the data, including users to log in, exchanges rates, and workflow. After all the data is ready, they can be viewed in Web pages.

1. Users

Here is the Web page to view users. Users with different roles are listed.

Users

	User ID	E-mail Address	Title
1	Deanna	deanna@orionstar.com	Deanna - Administration
2	Gloria	glory@orionstar.com	Gloria - Allocation and Recovery Approval,Cause Ma
3	Lisi	lisi@orionstar.com	Lisi - Incident Investigation
4	Mike	mike@orionstar.com	Mike - Central Risk Management
5	Robert	robert@orionstar.com	Robert - Incident Management Validation
6	Victor	victor@orionstar.com	Victor - Incident Creation

Figure 5. View Users

2. Exchange rates

As the base currency is the euro, exchange rates are provided to convert from US dollar to euro, from Chinese Yuan to euro, from Japanese yen to euro and from riyal to euro. Their usage will be introduced later.

Exchange Rates

	Effective From	Exchange Rate	To Currency	From Currency
1	April 1, 2011 12:00:00 AM EDT	1.361600	USD	EUR
2	April 1, 2011 12:00:00 AM EDT	9.043100	CNY	EUR
3	April 1, 2011 12:00:00 AM EDT	5.106200	SAR	EUR
4	April 1, 2011 12:00:00 AM EDT	112.875800	JPY	EUR
5	March 1, 2011 12:00:00 AM EST	1.361600	USD	EUR
6	March 1, 2011 12:00:00 AM EST	9.043100	CNY	EUR
7	March 1, 2011 12:00:00 AM EST	112.875800	JPY	EUR
8	March 1, 2011 12:00:00 AM EST	5.106200	SAR	EUR

Figure 6. View Exchange Rates

3. Workflows

Workflow determines business processes. Business processes in different countries are different. Their usage will also be introduced later.

Save Cancel

Operational Point (US)

Risk Event Type: (None Selected)
Management Organization: iFinance > Investment Banking > Securities
Geography: Americas > North America > United States
Product: (None Selected)
Process Type: (None Selected)

Validation Stages (1) Add Management Validation Stage... | Add Risk Validation Stage...

Stage	Name	Validation Stage ID	Source System	Applies to	Stage Type	Minimum Threshold	Maximum Threshold	Validators	Order Delete
1	Validation Stage for Securities Department	10060	Monitor	Near Misses, Gains, Losses	Management Validation			Robert - Incident Management Validation	X

Figure 7. View Workflows

2) CREATE INCIDENT

After the environment is ready, incident creators in each branch will enter loss incident in this Web page.

Incident creators specify the detail information of the incident, including a short description of the event, discovery date, and estimated amount, in SAS Enterprise GRC.

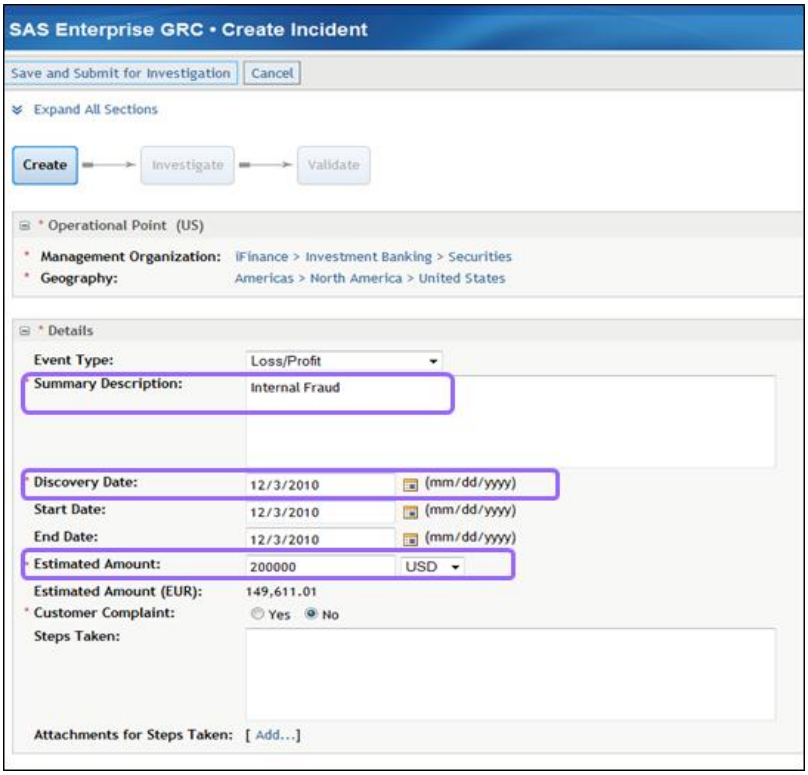


Figure 8. Create Incident

1. Graphical user interface

When the American clerks login, they can view the English Web page①. The Chinese②, Japanese③, and Arabic④ clerks can also view Web pages with their native languages. For the Arabic Web page, please note that what has changed is more than the language. Layout of the whole webpage renders from right to left in accordance with their convention.

Furthermore, clerks can also input data⑤ in their native languages.

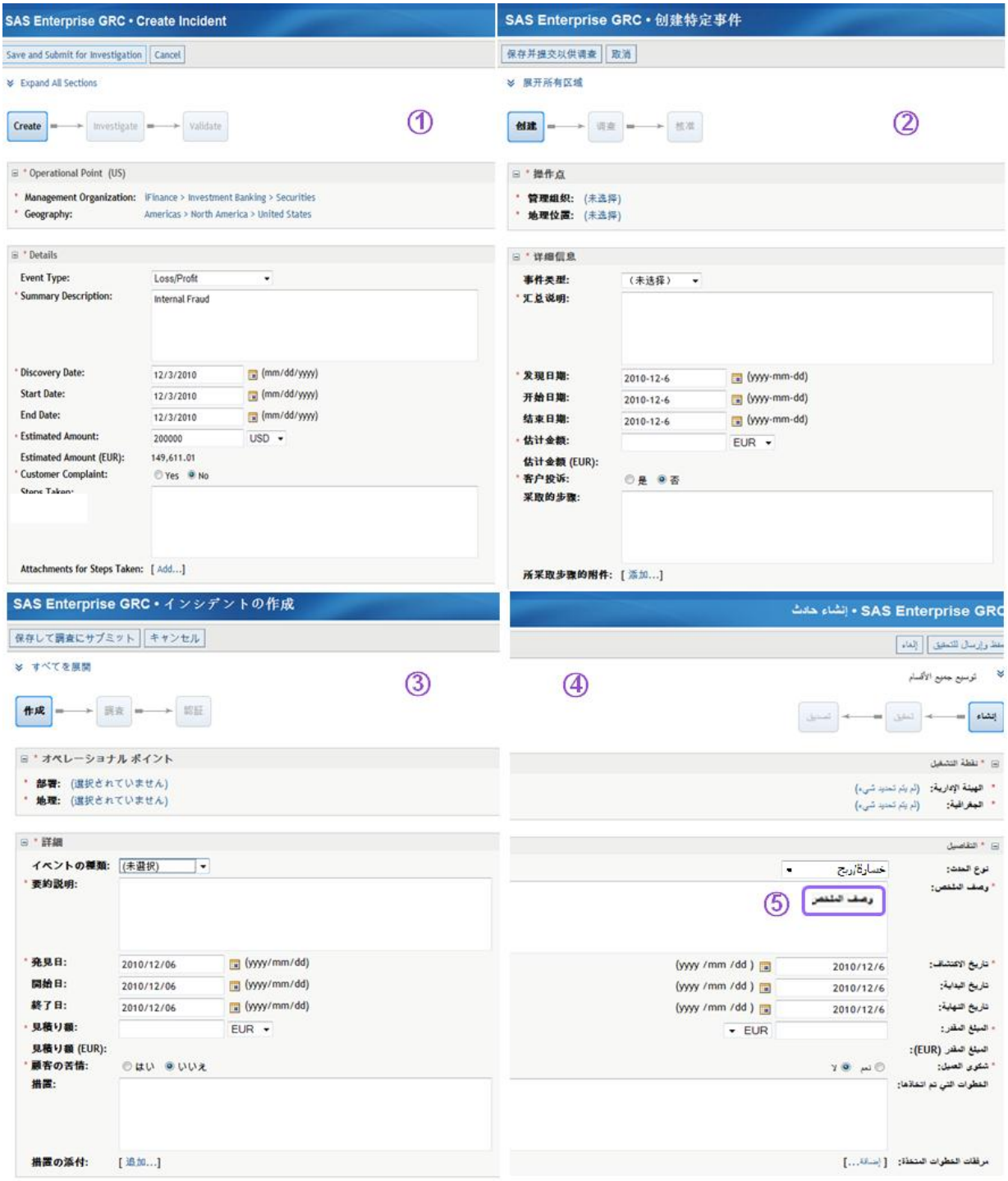


Figure 9. Four Various Languages

2. Currency conversion

The estimated amount of loss incident can be specified in the local currency. It need be converted into the base currency for reporting purposes. Exchange-rate data used for this conversion have been prepared in advance by the administrator.

When a clerk in the U.S. branch enters a monetary value in dollars, the value is automatically converted to the corresponding amount in the base currency (euro). When a clerk in the China branch enters a monetary value in CNY, Chinese yuan, it is converted automatically.

Actually, losses can be entered in any currency. However, for reporting purposes, the amount must be reported in the base currency. The euro is the base currency in this example. The base currency is specified and configured when setting up the system.

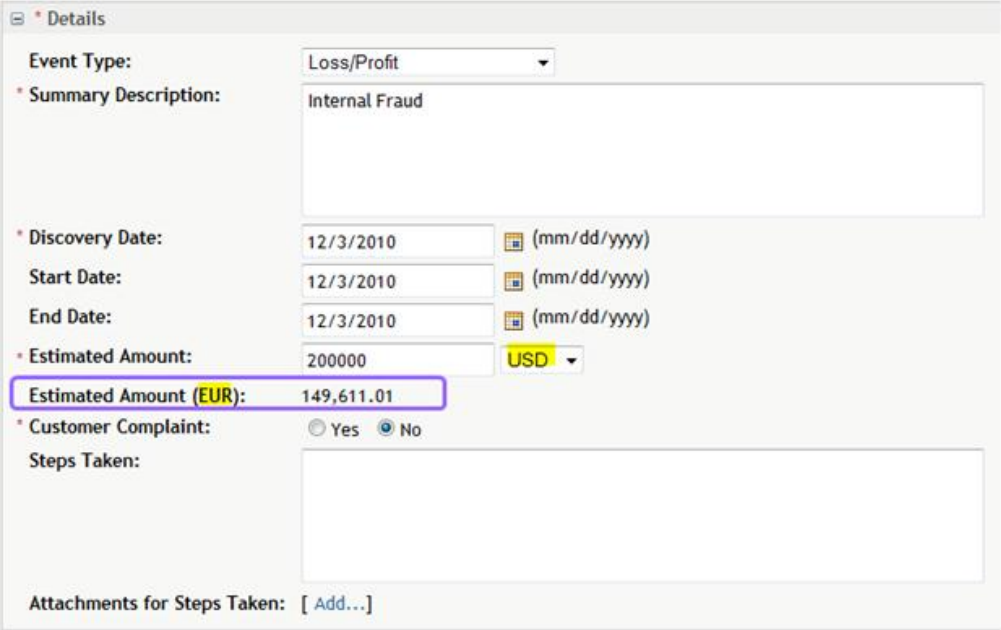


Figure 10. Convert from U.S. Dollar to Euro

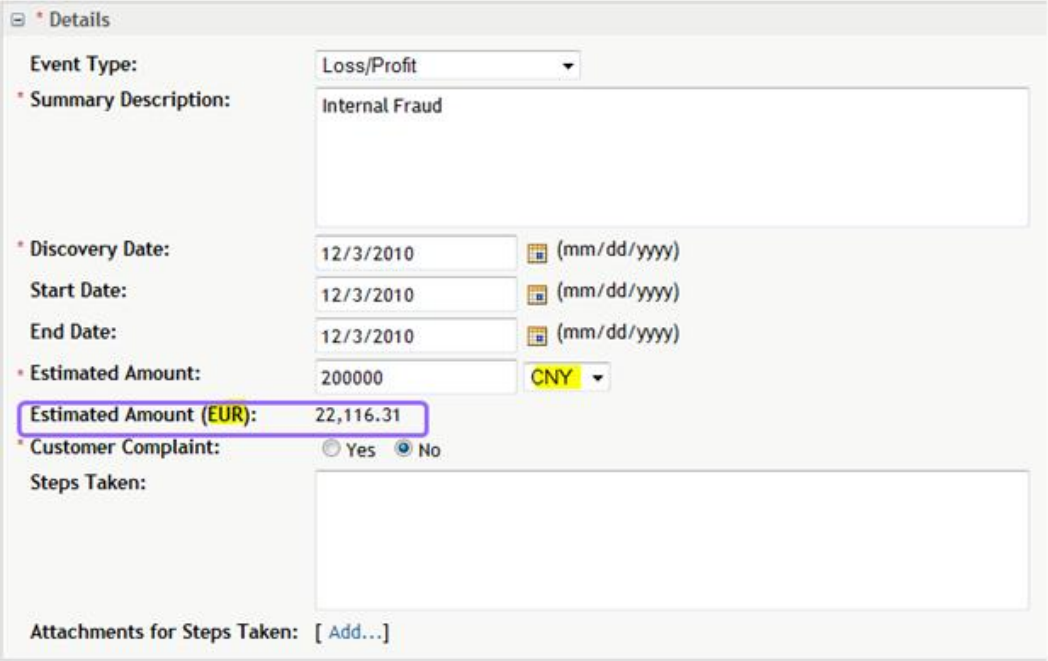


Figure 11. Convert from Chinese Yuan to Euro

3. Security mechanism

As we know, in a distributed company, the loss data in one branch are confidential even for other branches. This is to say, clerks in the headquarters and branches can manipulate loss data only within their permission. Access control in geography dimension can be leveraged to implement this.

This screenshot shows that clerks in the headquarters are permitted to view and manipulate the four incidents from all branches. However, American clerks are permitted only to manipulate data in U.S. branch and Chinese clerks are permitted to manipulate data only in the China branch. That is logical and necessary.

Actually, SAS Enterprise GRC offers three types of security to meet the complicated and flexible requirements in the real world: authentication, identification, and authorization.

Figure 12. Access Control - Headquarters

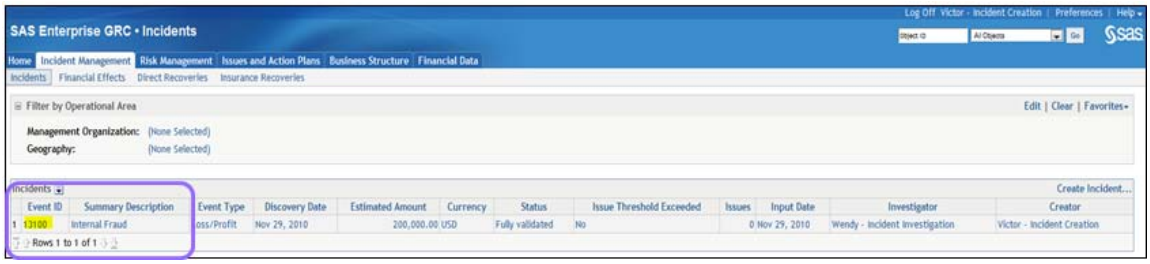


Figure 13. Access Control – U.S. Branch

Figure 14. Access Control – China Branch

3) INVESTIGATE INCIDENT

After incident creation, an alert notification e-mail is automatically sent to an incident investigator to alert that an incident is ready for investigation.

1. Alert notification e-mail

Clerks in the U.S. can receive English alert notification e-mail. Likewise, clerks in China can receive Chinese alert notification e-mail.

Furthermore, the e-mail content is based on a template and is also customizable for different countries. So the clerk can configure not only the language of the e-mail but also the content for various countries.

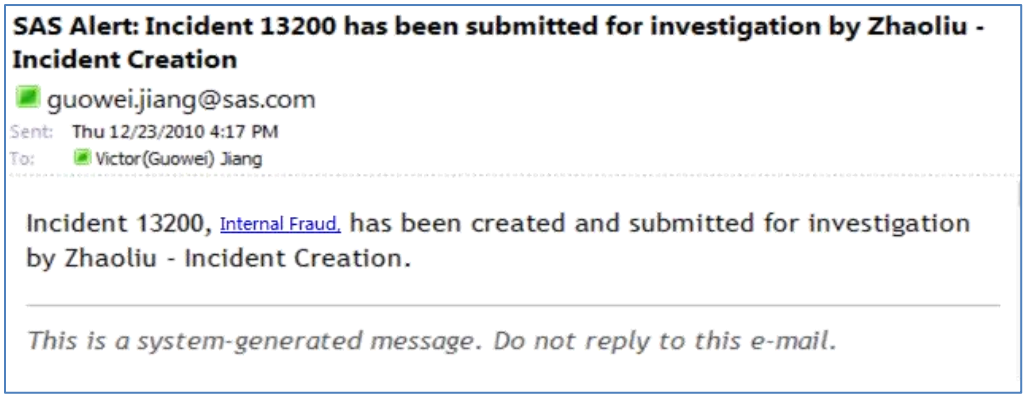


Figure 15. English Alert Notification Mail

Figure 16. Chinese Alert Notification Mail

2. Business line

The incident investigator investigates the whole event and inputs information such as a detailed event description, actual loss amount, and root cause.

The incident investigator will enter the business line where the incident happens in this Web page. In the left graph, a U.S. incident investigator selects the geographic area, and then the relevant five business lines in the U.S. branch are shown. Similarly, in the right graph, the two business lines in the China branch are shown for a Chinese incident investigator. It is reasonable to show business lines within the branch rather than showing all.

Figure 17. Different Business Lines in U.S. and China

3. Date and number format

The graph above is an English Web page. Below is an Arabic one. They show different date formats. The date format in the U.S. is month/day/year, while it is year/month/day in Saudi Arabia. Similarly, the number format is different as well.

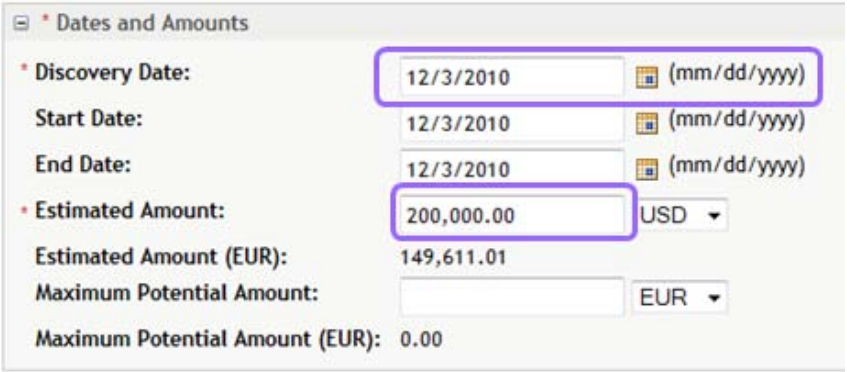


Figure 18. Date and Number Format in U.S.

Figure 19. Date and Number Format in Saudi Arabia

4) VALIDATE INCIDENT

After investigation, an alert notification will be sent to an incident validator. Moreover, the notification will also appear in the task list in the home page. This is the Web page to validate incident.

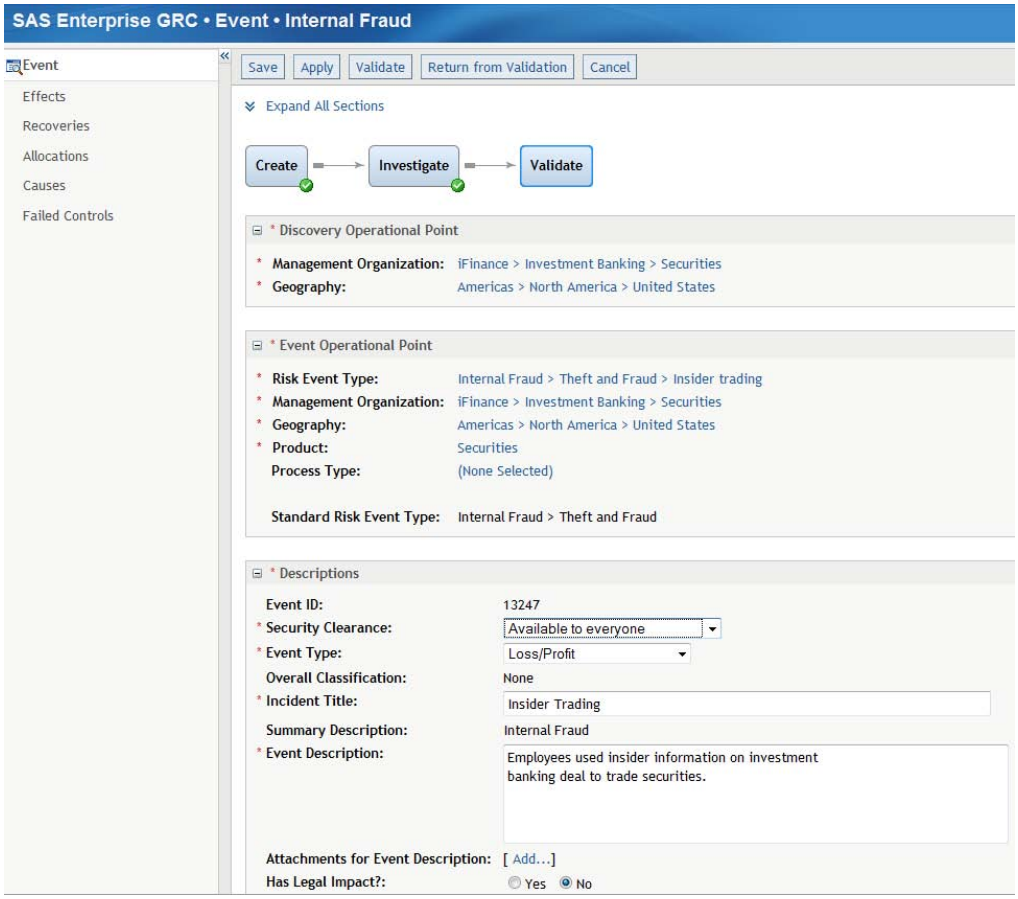


Figure 20. Validate Incident

The result of the investigation will be validated. If the result is not approved, it can be returned for re-investigation.

Validation is based on internal control rules. Different branches might have different internal control rules. The rules define who should validate it and define the number of validation stages.

For example, in the China branch, an incident is validated by local clerks if the loss amount is less than 10,000. Otherwise, it is validated by HQ. In the U.S. branch, an incident is validated only by local clerks no matter what the amount is.

The difference of internal control rules is implemented via customizable workflow in SAS Enterprise GRC.

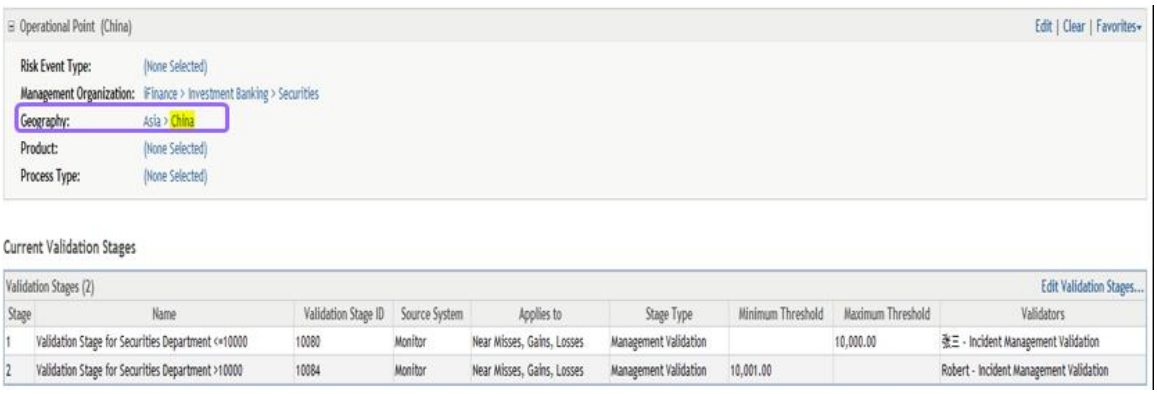


Figure 21. Workflow in China

Operational Point (US) — Edit | Clear | Favorites

Risk Event Type:	(None Selected)
Management Organization:	iFinance > Investment Banking > Securities
Geography:	Americas > North America > United States
Product:	(None Selected)
Process Type:	(None Selected)

Current Validation Stages

Validation Stages (1) — Edit Validation Stages...

Stage	Name	Validation Stage ID	Source System	Applies to	Stage Type	Minimum Threshold	Maximum Threshold	Validators
1	Validation Stage for Securities Department	10060	Monitor	Near Misses, Gains, Losses	Management Validation			Robert - Incident Management Validation

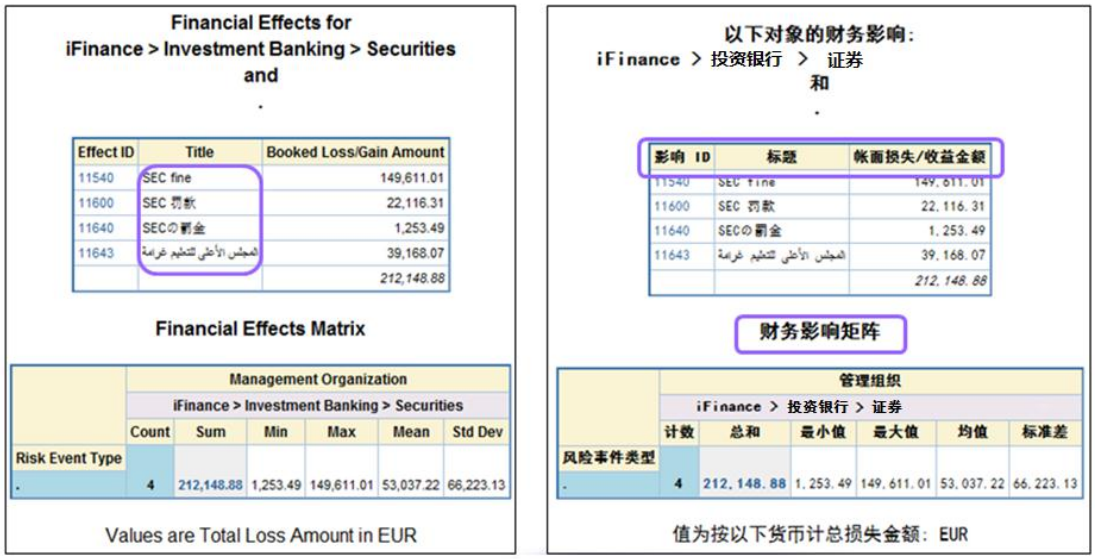
Figure 22. Workflow in the U.S.

5) VIEW REPORT

Clerks in the U.S, China, Japan, and Saudi Arabia have finished their workflows. The reports, including data in all branches, can be generated at this time.

In the left graph, various languages are displayed in one report. That is useful when different branches use different languages to enter data.

In the right graph, the title and column title are Chinese whereas they are English in the left graph. That means the language of the title and column title can also be changed and would be useful if the headquarters is located in another country and managers want to view report in their native language.



Financial Effects for
iFinance > Investment Banking > Securities
and
.

Effect ID	Title	Booked Loss/Gain Amount
11540	SEC fine	149,611.01
11600	SEC 罚款	22,116.31
11640	SECの罰金	1,253.49
11643	المجلس الأعلى للتنظيم غرامة	39,168.07
		212,148.88

Financial Effects Matrix

	Management Organization					
	iFinance > Investment Banking > Securities					
	Count	Sum	Min	Max	Mean	Std Dev
Risk Event Type						
.	4	212,148.88	1,253.49	149,611.01	53,037.22	66,223.13

Values are Total Loss Amount in EUR

以下对象的财务影响:
iFinance > 投资银行 > 证券
和
.

影响 ID	标题	帐面损失/收益金额
11540	SEC fine	149,611.01
11600	SEC 罚款	22,116.31
11640	SECの罰金	1,253.49
11643	المجلس الأعلى للتنظيم غرامة	39,168.07
		212,148.88

财务影响矩阵

	管理组织					
	iFinance > 投资银行 > 证券					
	计数	总和	最小值	最大值	均值	标准差
风险事件类型						
.	4	212,148.88	1,253.49	149,611.01	53,037.22	66,223.13

值为按以下货币计总损失金额: EUR

Figure 23. Multilingual Support in Report

The amount is reported in the base currency (the euro). As mentioned above, exchange rates are used to convert from four currencies to the euro. Then the loss amounts from four branches are collected and aggregated.

Branch	Loss Amount	Loss Amount (Euro)
U.S.	200,000 Dollars	149,611.01
China	200,000 Chinese Yuan	22,116.31
Japan	200,000 Japanese Yen	1,253.49
Saudi Arabia	200,000 Riyal	39,168.07
Total		212,148.88

Managers in headquarters are able to view the report, including data from all over the Enterprise. Moreover, managers in each branch are also able to view the report, including data in their own branch. The report at the top left corner is for the U.S branch. Only data within the U.S. branch appear. The reports for China, Japan, and Saudi Arabia branches are also listed.

Figure 24. Reports for Different Branches

Above is the scenario to process the incident. It shows the power of SAS Enterprise GRC to manage incidents in a distributed enterprise. Moreover, there are many good supports in other processes. For example, questionnaire-based assessment can be performed to collect information about risks within the organization. The questionnaire is made and sent to assessors. Assessors in different countries are able to view questions and choices in their native languages. If clerks use a language without relevant translation prepared, the default language specified by the administrator will be used.

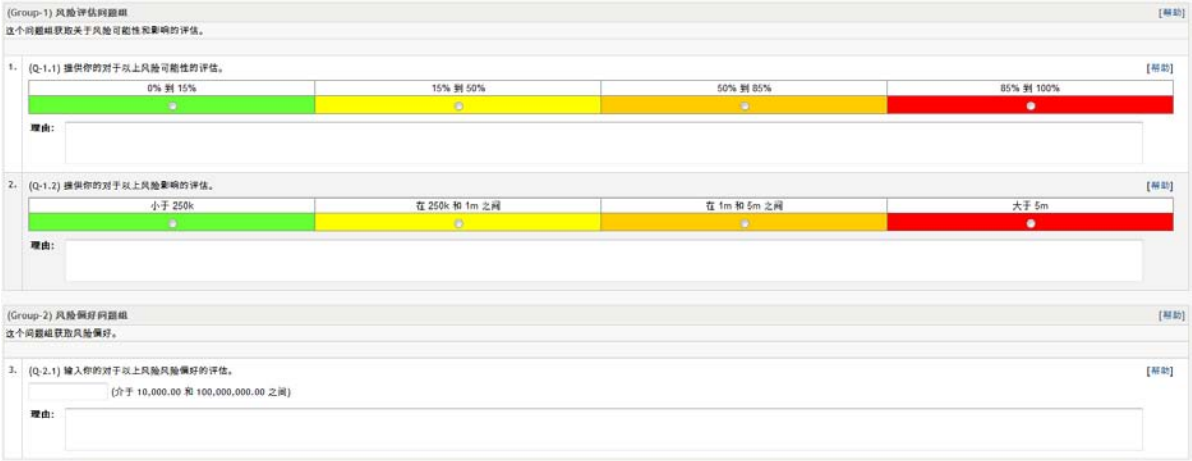


Figure 25. Chinese Questionnaire

Figure 26. English Questionnaire

CONCLUSION

SAS Enterprise GRC supports various languages in the the graphical user interface, user data, alert notification e-mail, and reports.

It supports right-to-left rendering, various date, time, number, and currency formats, suitable security mechanisms, and customizable workflows for a distributed enterprise.

- Multiple languages
  - Graphical user interface and user data
  - Alert notification e-mail
  - Reports
- Right-to-left rendering support
- Date, time, and number formats
- Currency
- Customizable workflow

- Security
- Diversity of business structure

In conclusion, SAS Enterprise GRC is a perfect product to manage nonfinancial risks in a distributed enterprise.

The SAS Legal Department is currently implementing SAS Enterprise GRC to manage compliance processes across a number of roles and departments at SAS. Other SAS departments – including SAS Finance and SAS Ergonomics – are beginning SAS Enterprise GRC implementations to provide standard out-of-the-box workflow, and repeatable, reportable processes for conducting audits and providing employees with ergonomic workstations. SAS Enterprise GRC has been implemented for more than 80 customers, from financial services, energy and utilities, manufacturing, and retail to public sector, and from local to distributed enterprises.

REFERENCES

The following references or sources can be used for additional information and research activities:

- "Governance, risk management, and compliance." Wikipedia. Available at http://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance. Accessed on February 15, 2011.
- SAS Enterprise GRC 4.3: User Guide. Available at http://support.sas.com/documentation/onlinedoc/securedoc/index_egrc.html
- SAS Enterprise GRC 4.3: Administrator's Guide. Available at http://support.sas.com/documentation/onlinedoc/securedoc/index_egrc.html

ACKNOWLEDGMENTS

We would like to thank Jungle Cheng, Carol Rigsbee, Susan Kahler, and Chloe Li for reviewing drafts of this paper and providing valuable suggestions, especially Chloe Li's great help.

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the authors:

Guowei (Victor) Jiang, Software Engineer of Solution Testing Group
Hao Qiu, Manager of Solution Testing Group
SAS Institute Inc.
19/F North Wing, Central Office Tower, Junefield Plaza, No. 10 Xuanwumenwai Dajie Xuanwu District
Beijing, China
100052
Work Phone: +86 10 8319-3814/3805
Fax: +86 10 6310-9130
E-mail: guowei.jiang@sas.com; hao.qiu@sas.com

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration.

Other brand and product names are trademarks of their respective companies.