

Session 197

Inspect What You Expect: Building a Global Framework for Business Success

Karen Beaman – Founder/CEO

Pat Crane – Regional Vice President

John Gibbons – Vice President, Research and Strategy

Jeitosa Group International



Agenda for This Session

- Introduction
- Vendor Globalization
- Global Compliance
- Security and Cloud Computing
- Conclusion



Vendor Globalization Strategies



Vendor Globalization Model

Business Impact	L2: Language Translations <i>(employee / manager self-service, HR admin / business partner roles, etc.)</i>	L4: Global Compliance <i>(government-mandated reporting, governance, and compliance, etc.)</i>
	L1: Data Structures <i>(names, addresses, country-specific data elements, etc.)</i>	L3: Business Processes <i>(country-specific rules, audits and approval processes, etc.)</i>
Business Complexity		Source: Jeitosa

Business Impact: the value of globalizing that function to the organization

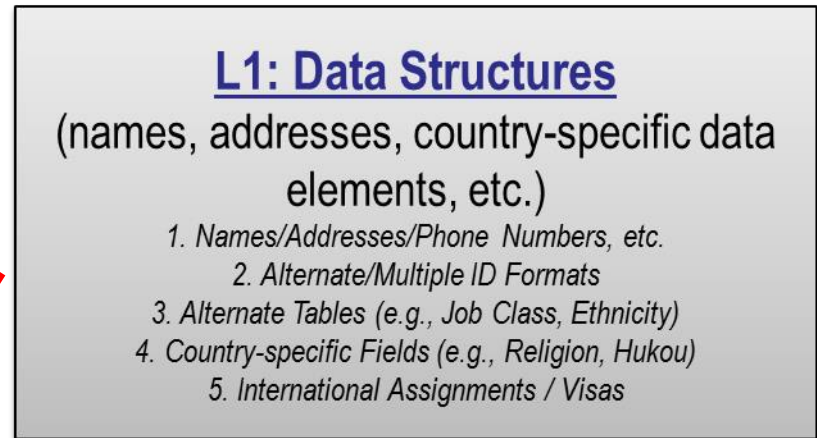
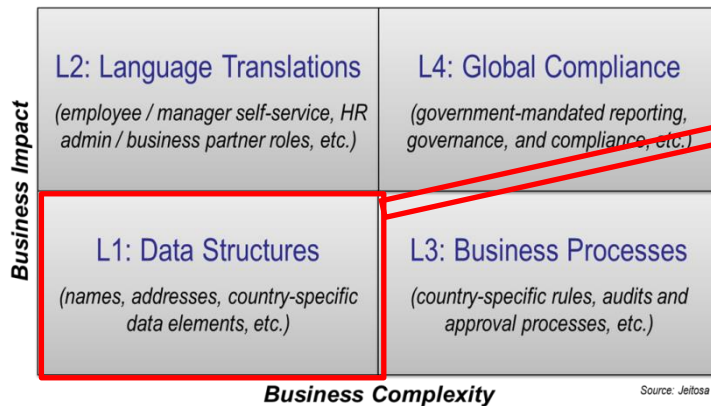
Complexity: the difficulty of globalizing that function by the vendor



Globalization Level 1: Data

First level of vendor globalization: Data

- *Data structures for international names, addresses, telephone numbers, etc.*
- *Country-specific fields like religion in Germany, Hukou in China, etc.*
- *Simplest level of globalization, providing a low level of business value*



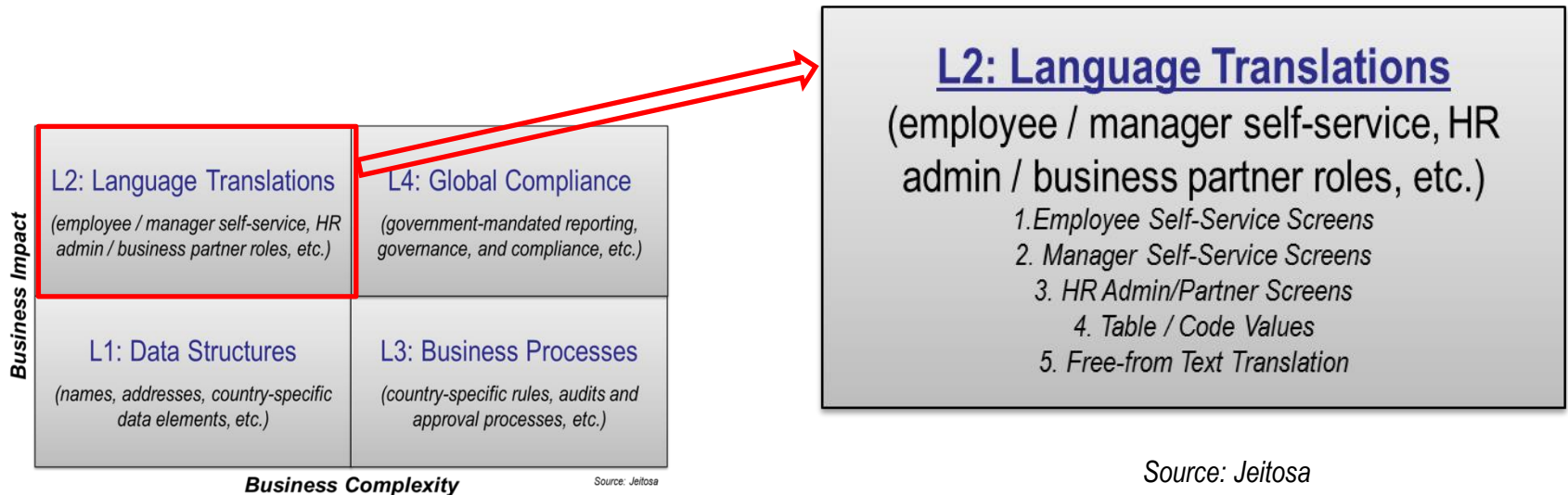
Source: Jeitosa



Globalization Level 2: Language

Second level of vendor globalization: Language

- *Has the vendor translated just the self-service screens or have they also translated those functions used by the HR partner and back-office administrators?*
- *Do they provide for translation of code and table values, as well as free-form text translations?*
- *Clearly there is greater business benefit to the customer if more of the product has been translated.*



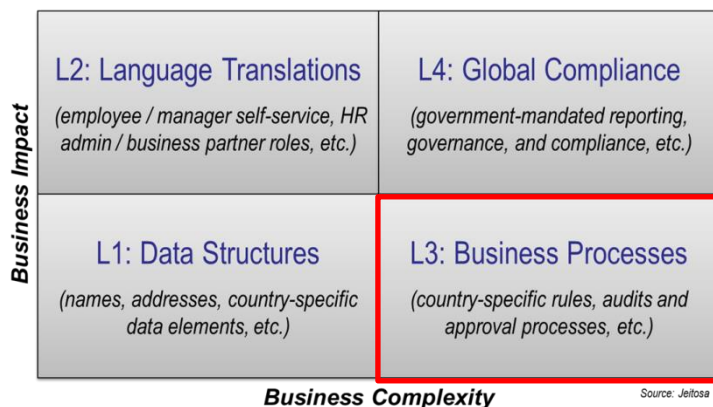
Source: Jeitosa



Globalization Level 3: Business Process

Third level of vendor globalization: Business Processes

- *Does the vendor allow for different business process by country and region? For example, can the product handle the complex employment and severance agreements in some countries, vacation accrual and time off policies, and global benefits and pension programs, such as superannuation in Australia?*
- *With all the different legislation and regulations around the world, this level of globalization is much more complex for the vendor, and certainly represents significant business benefit for the customer.*



Business Complexity

Source: Jeitosa

L3: Business Processes (country-specific rules, audits and approval processes, etc.)

1. Employment Types/Contracts
2. Compensation Plans/Allowances
3. Time-off Accruals/Absence Management
4. Termination/Severance Agreements
5. Global Benefits/Pension Funds

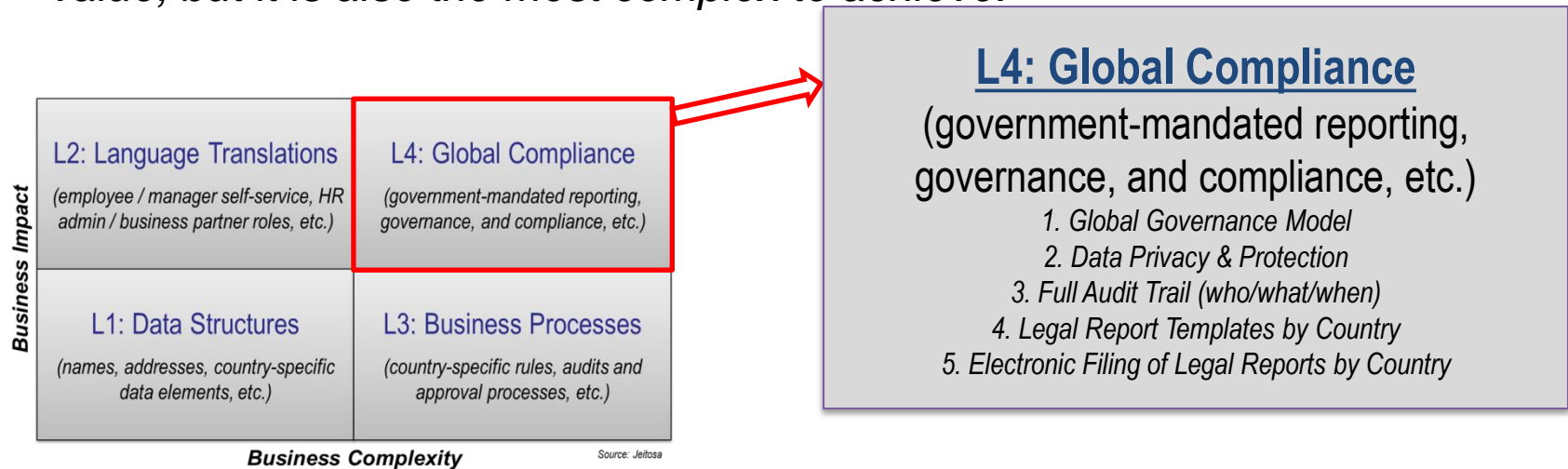
Source: Jeitosa



Globalization Level 4: Compliance

Fourth level of vendor globalization: Global Compliance

- *How well does the vendor support your ability to comply globally with legislation around the world (beyond simple data capture)?*
- *What does the vendor provide for global governance, compliance, and data privacy and protection?*
- *This level of globalization provides the customer with the greatest business value, but it is also the most complex to achieve.*



Source: Jeitosa



Vendor Globalization Report Card

Vendor Globalization Report Card

	Vendor1	Vendor2	Vendor3
L1: Data Structures			
1. Names/Addresses/Phone Numbers, etc.	●	●	●
2. Alternate/Multiple ID Formats	●	●	●
3. Alternate Tables (e.g., Job Class, Ethnicity)	●	●	●
4. Country-specific Fields (e.g., Religion, Hukou)	●	●	●
5. International Assignments / Visas	●	●	●
L2: Language Translations			
1. Employee Self-Service Screens	●	●	●
2. Manager Self-Service Screens	●	●	●
3. HR Admin/Partner Screens	●	●	●
4. Table / Code Values	●	●	●
5. Free-from Text Translation	●	●	●
L3: Business Processes			
1. Employment Types/Contracts	●	●	●
2. Compensation Plans/Allowances	●	●	●
3. Time-off Accruals/Absence Management	●	●	●
4. Termination/Severance Agreements	●	●	●
5. Global Benefits/Pension Funds	●	●	●
L4: Global Compliance			
1. Global Governance Model	●	●	●
2. Data Privacy & Protection	●	●	●
3. Full Audit Trail (who/what/when)	●	●	●
4. Legal Report Templates by Country	●	●	●
5. Electronic Filing of Legal Reports by Country	●	●	●

“Global” vendors tend to be more mature with regard to data structures and language translations; however, there is considerable less maturity when it comes to global business processes and compliance.

Source: Jeitosa



Vendor Globalization Assessment

Vendor Globalization Assessment

	5=Extremely 3=Somewhat 0=Impossible	Availability	Usability	Configurability	Cost Level
L1: Data					
1.1 Personal Contact Information					
1.2 Multiple/alternate ID Formats					
1.3 Alternate tables and codes					
1.4 Country-specific data elements					
1.5 International assignments & visas					
Summary					
L2: Language					
2.1 Employee Self-Service screens					
2.2 Manager Self-Service screens					
2.3 HR Admin / Partner screens					
2.4 Table codes and values					
2.5 Free-form text translation					
Summary					
L3: Business Process					
3.1 Employment types and contracts					
3.2 Compensation plans and processes					
3.3 Time-off and absence management					
3.4 Termination and severance agreements					
3.5 Benefits and pension plans					
Summary					
L4: Compliance					
4.1 Support for global governance					
4.2 Support for data privacy					
4.3 Tracking and auditing					
4.4 Legislative and regulatory reports					
4.5 Legislative and regulatory filings					
Summary					
Overall Assessment					

Jeitosa's Global Vendor Assessment model allows you to identify areas most critical to your organization and evaluate potential vendors according to the availability, usability, configurability and cost of specific global capabilities.

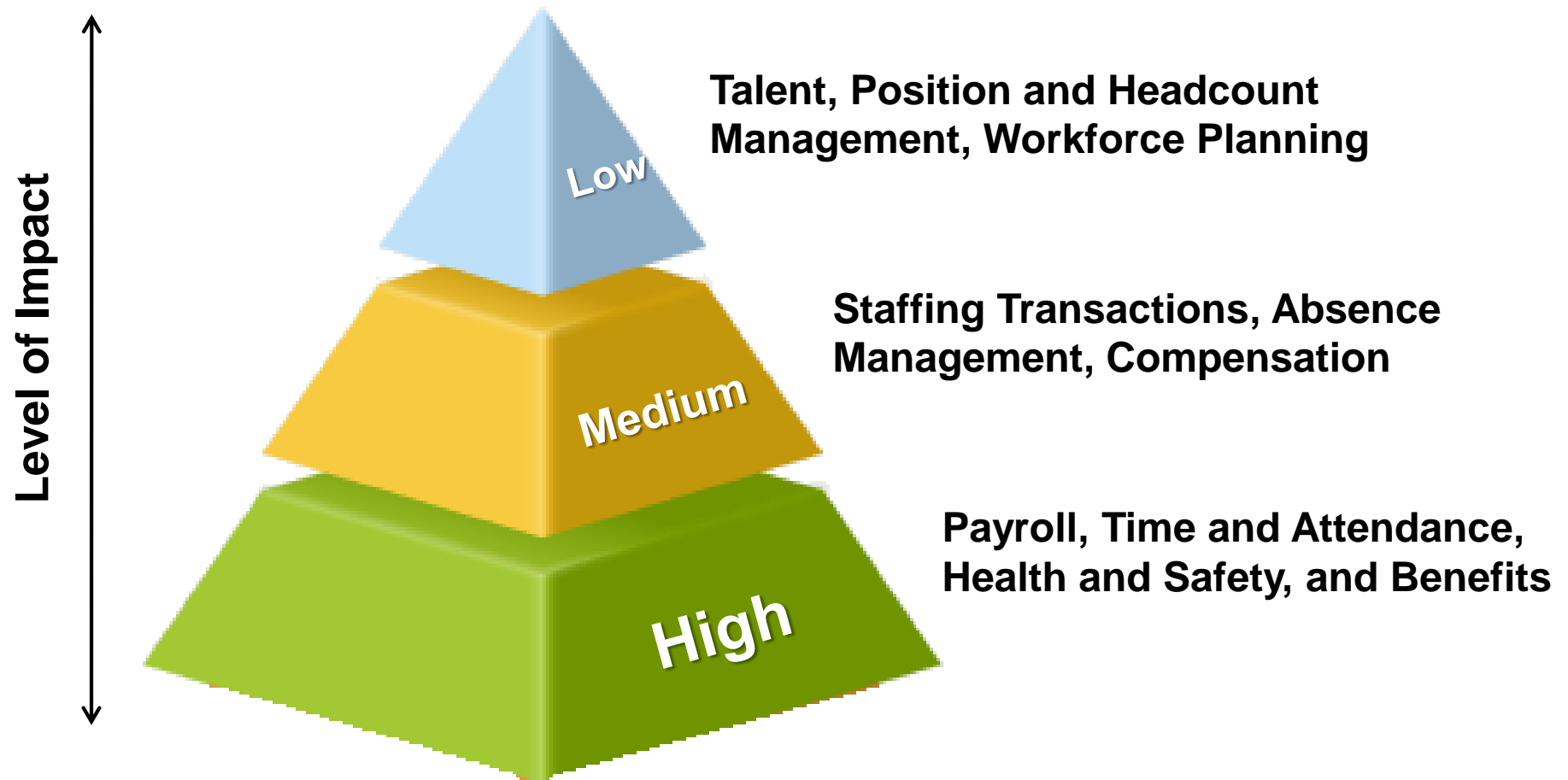
Source: Jeitosa



Global Compliance Framework



Global Compliance Model



Source: Jeitosa



High Impact Areas

- Areas that bring the greatest risk of exposure to the organization and, therefore, need the most focused attention and expert localized support.
- Requires a either local technology solution with third-party solution provider to meet highly specialized, country-specific requirements or a global solution with highly developed localizations or “add-ons.”
- High impact areas:
 - Payroll
 - Time and Attendance
 - Health and Safety
 - Benefits

Source: Jeitosa



High Impact Areas – Payroll

- Highly driven by country/state labor and tax laws
- Few providers offer global payroll and the implementation is always a challenging effort
- Local payroll solutions/services with interfaces between core HR system and the local payroll providers
 - **Advantage:** necessary expertise is available in the local country to accurately pay employees and handle taxes
 - **Disadvantage:** inefficiencies and lack of negotiating power associated with managing many diverse relationships with different suppliers, as well as the maintenance costs of managing multiple interfaces for every local country payroll
- Some country examples include:
 - **Brazil:** complex tax calculations, vacation payments and frequent labor law changes
 - **Germany:** unions have considerable power over the process with very tightly controlled data protection requirements
 - **France:** complex calculations for overtime and absence

Source: Jeitosa



High Impact Areas – Time and Attendance

- Time and Attendance is directly tied to the payroll system and is also highly impacted by local regulations
- Data collection rules are often similar; the big differences lie in the data processing logic
 - Time scales and weekly hours may vary by country (or state, or city, or industry type or collective agreements)
 - Complex rules for calculating breaks, overtime and time off
- Some country examples include:
 - **Germany**: Flexible Retirement for Employees Act in Germany, which encourages companies to establish a part-time employment program for employees age 55 or older. If the weekly hours for an older employee are reduced by 50 percent, the employee receives his or her part-time income plus a 20 percent pay supplement (based on the part-time income).
 - **Brazil**: Employees working on night shifts are entitled to receive a pay supplement based on the number of hours worked between 10pm and 5am.

Source: Jeitosa



High Impact Areas – Benefits

- Define benefits that required by law and are commonly offered in the industry, as well as by the organization's local competitors.
- Some components and plans are considered as compensation in some countries, and benefits in other countries:
 - Company cars and meals can be considered as compensation allowances in some countries and as benefits in some others, and are taxed differently.
- Some countries have open enrollment based on choice; for others a benefits package is assigned based on eligibility rules and legally mandated benefits.
- Some country examples include:
 - **Australia's Superannuation:** Money is set aside over the worker's lifetime to provide for retirement.
 - **Mexico's INFONAVIT:** Employers contribute five percent of the worker's earnings to the Worker's Housing Fund.
 - **Brazil's Child Care Allowance:** In Brazil, workers with pre-school age children (up to 5 years old) are entitled to a child care allowance.

Source: Jeitosa



Medium Impact Areas

- These areas present a lower level of risk exposure to the organization; however, they are still complex and time-consuming in their requirements.
- Some systems can handle this through configurable business processes, automated workflows and localized reporting.
- Medium impact areas:
 - Staffing transactions such as hires, promotions, demotions, transfers and terminations
 - Absence Management
 - Compensation

Source: Jeitosa



Medium Impact Areas – Staffing

- Most impacted by country-specific legislation are **hires** and **terms**:
 - Labor contracts:
 - **Denmark**: the contract must be presented to the employee on the first day of work at the latest and must describe clearly the salary conditions, workplace, working hours, annual leave and notice period.
 - **Italy**: contract can be presented to the worker within 30 days of employment.
 - **Japan**: a labor contract is not required; instead, companies with 10 or more employees must create a set of work rules, which are applied to every worker.
 - Notifications and Administrative Procedures:
 - **Spain**: new hires must be notified to Social Security before the employee starts.
 - **China**: Hukou system requires a family booklet to be issued with information about the worker, family members, birth date, marital status, address, etc.
 - **Belgium**: employers are required to use the language of the region in which they are located for all worker related documentation.
 - **Saudi Arabia**: employers must send an annual report to the local labor office with employee data, such as names, ID numbers, positions, nationality, age and compensation, and expected workforce increase/decrease for the following year.

Source: Jeitosa



Medium Impact Areas – Absence

- Most impacted items: holiday calendars, time off and vacation accrual, carryover rules, and absence types.
- Many time-off types are common across countries, such as maternity, sickness and jury duty.
- Others are less common but still used in some countries, such as paternity and childcare leave.
- Some country examples include:
 - **South Korea**: Employees are entitled to three days of paternity leave upon the birth of a child and it must be taken within 30 days of the child's birth.
 - **Pakistan**: Muslim female employees are entitled a mourning period in the event of the husband's death.
 - **South Africa**: Employees must take annual leave no later than six months after the annual leave cycle.
 - **Israel**: The Jewish calendar year consists of 12 or 13 months of 29 or 30 days and varies in length of 353, 354, 355, 383, 384, or 385 days based on the lunar cycle.

Source: Jeitosa



Medium Impact Areas – Compensation

- Bonuses and merit increases are similar across countries, and percentages, eligibilities, and targets can be configured in modern global HR systems.
- Some countries have specific allowances and wage types. For example, in some countries, the law allows employers to pay workers in goods (e.g., food) rather than money.
- Some countries consider benefits as compensation elements. For example, meal and transportation allowances can be considered compensation while meal and transportation tickets can be a required benefits in some others.
- Collective agreements impact compensation for certain unions and industries.
- Some country specific examples:
 - **China**: compensation is typically divided into four elements: base pay, incentives, allowances and benefits. There is also an “inflationary supplement,” which is a percentage added to the base salary.
 - **Russia**: the law requires employers to pay the salary in two or more installments per month.
 - **Finland**: financial payments are not required by law; instead, workers can be compensated by “gaining of experience”

Source: Jeitosa



Low Impact Areas

- These areas present minimum risk to the organization and have little legislative or regulatory controls that impact HR processes.
- Differences in terminology and definitions in customary business practices
- Low impact areas:
 - Talent management: recruitment, performance reviews, training, career and succession planning.
 - Positions, headcount management, and workforce planning

Source: Jeitosa



Low Impact Areas – Talent Management

Talent Management:

- Any solid HR system should be able to accommodate global requirements for talent management.
- There are rarely any compliance-related particularities around performance management, learning management, and career and succession planning.
- In some countries, like France, companies are required to provide a minimum number of training hours per employee per year, and this information can easily be tracked through data extracts and reports with the relevant information.

Workforce Planning, Positions and Headcount Management:

- Some countries have the need to report changes to the workforce to their governments, but once the information is in the system, it's just a matter of extracting and formatting the data to be sent.
- Mainly budget-driven and not impacted by legislative or regulatory compliance.
- Country-specific rules for severance pay can impact workforce reductions

Source: Jeitosa



Global Compliance Risk Assessment (1 of 2)

Conduct a global compliance risk study by business process and country to assess your areas of risk

Detailed Compliance Risk Assessment by Function and by Country

	Requirement Name	Germany	Australia
1	General		
1-4	Multiple/Native Languages	Common	Optional
1-5	Multiple/Local Currencies	Legislative	Legislative
2	Personal		
2-1	Personal Identification	Legislative	Legislative
2-2	Personal Attributes	Legislative	Legislative
2-3	Address	Legislative	Legislative
2-4	Address Validation	Innovative	Innovative
2-7	Military Service	Common	Optional
2-8	Ethnicity	Legislative	Legislative
2-9	Disability Information	Legislative	Optional
2-10	Related Persons	Optional	Good
2-12	Data retention	Legislative	Legislative
3	Employment		
3-1	Employment Categories	Legislative	Legislative
3-2	Temporary Staff	Legislative	Legislative
3-3	Third Party Temporary	Legislative	Legislative
3-4	Trainees and Apprentices	Legislative	Legislative
3-5	Workforce Reintegration	Optional	Optional
3-6	Labor Agreements	Legislative	Legislative
3-8	Employee Movement	Common	Common
3-9	Termination	Legislative	Legislative

	Requirement Name	Germany	Australia
4	Organization		
4-2	Organizational Details	Legislative	Legislative
4-3	Workplace Location(s)	Legislative	Legislative
4-4	Jobs	Legislative	Common
4-5	Job Family	Good	Good
4-6	Job Descriptions	Good	Good
4-7	Job Evaluation	Good	Good
4-8	Titles	Common	Common
4-9	Positions	Good	Good
4-10	Position Descriptions	Good	Good
4-11	Project Assignments	Innovative	Innovative
5	Compensation		
5-1	Salary Packaging	Common	Common
5-2	Base Ranges	Common	Common
5-3	Base Salary	Optional	Legislative
5-4	Allowances	Legislative	Legislative
5-5	Bonuses	Legislative	Legislative
5-6	Variable Compensation	Legislative	Legislative
5-7	Stock Management	Good	Good
5-8	Equity Management	Good	Good
5-9	Severance Payments	Legislative	Legislative

	Requirement Name	Germany	Australia
6	Performance		
6-1	Performance Appraisal	Good	Good
6-2	Career Growth Planning	Good	Good
6-3	Probation	Optional	Common
6-4	Discipline	Legislative	Legislative
7	Staffing		
7-1	Staffing Management	Good	Good
7-2	Recruiting Management	Good	Good
7-3	Applicant Management	Good	Good
7-4	Pre-employment verification	Common	Common
7-5	Employment Offer	Legislative	Legislative
7-6	Work History	Optional	Optional
7-7	Education	Good	Good
7-8	Affirmative Action	Optional	Optional
7-9	Succession Planning	Good	Good
7-10	Expatriate Management	Good	Good
7-11	Work Permits	Legislative	Legislative
8	Time		
8-1	Standard Hours	Legislative	Legislative
8-2	Working Schedule	Legislative	Legislative
8-3	Overtime	Legislative	Legislative
8-4	Vacation	Legislative	Legislative

	Requirement Name	Germany	Australia
8-5	Leave	Legislative	Legislative
8-6	Carry Over	Legislative	Legislative
9	Learning		
9-1	Skills & Competency	Common	Common
9-2	Licenses & Certification	Good	Good
9-3	Competency Testing	Innovative	Innovative
9-4	Course Administration	Common	Common
9-5	Course Delivery	Common	Common
9-6	Training Information	Common	Common
9-7	Mentor Program	Innovative	Innovative
9-8	Training Compliance	Optional	Optional
10	Health & Safety		
10-1	Health	Legislative	Legislative
10-2	Safety	Legislative	Legislative
10-3	Accident Investigation	Legislative	Legislative
10-4	Employee Assistance (EAP)	Good	Good
10-5	Rehabilitation	Legislative	Legislative

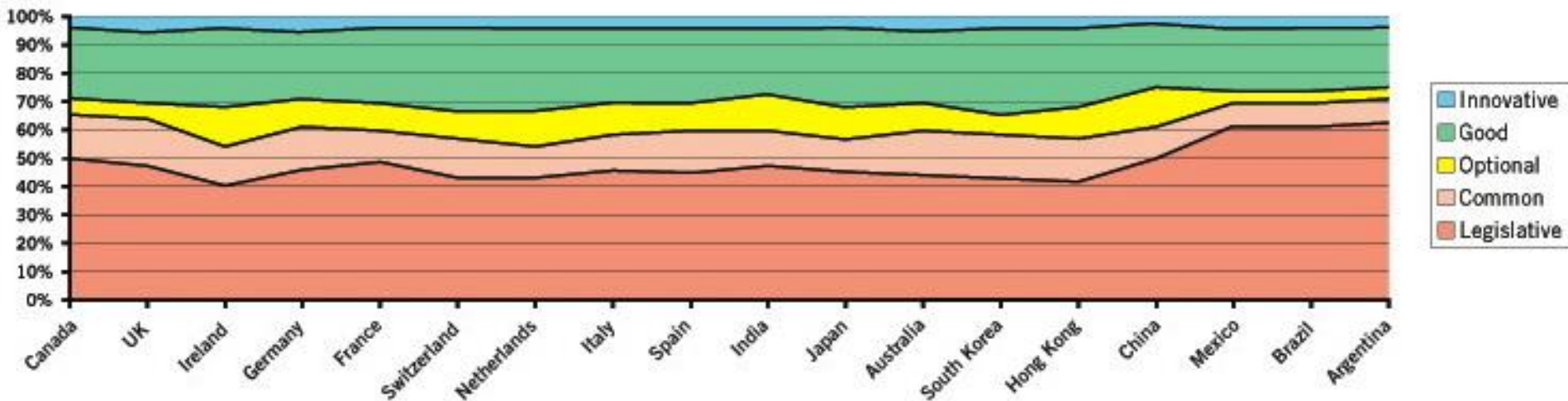
Source: Jeitosa



Global Compliance Risk Assessment (2 of 2)

Conduct a global compliance risk study by business process and country to assess your areas of risk

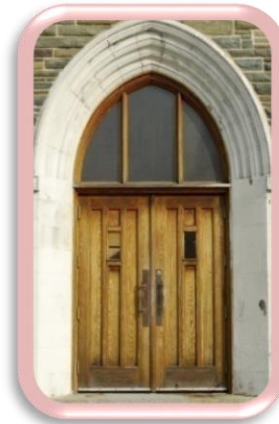
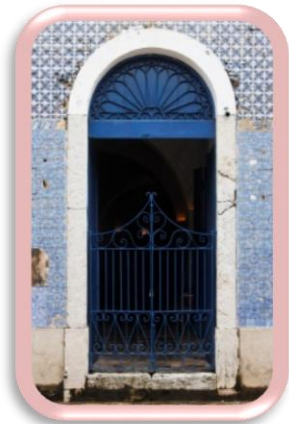
Summary Compliance Risk Assessment by Country



Source: Jeitosa



Security and Cloud Computing

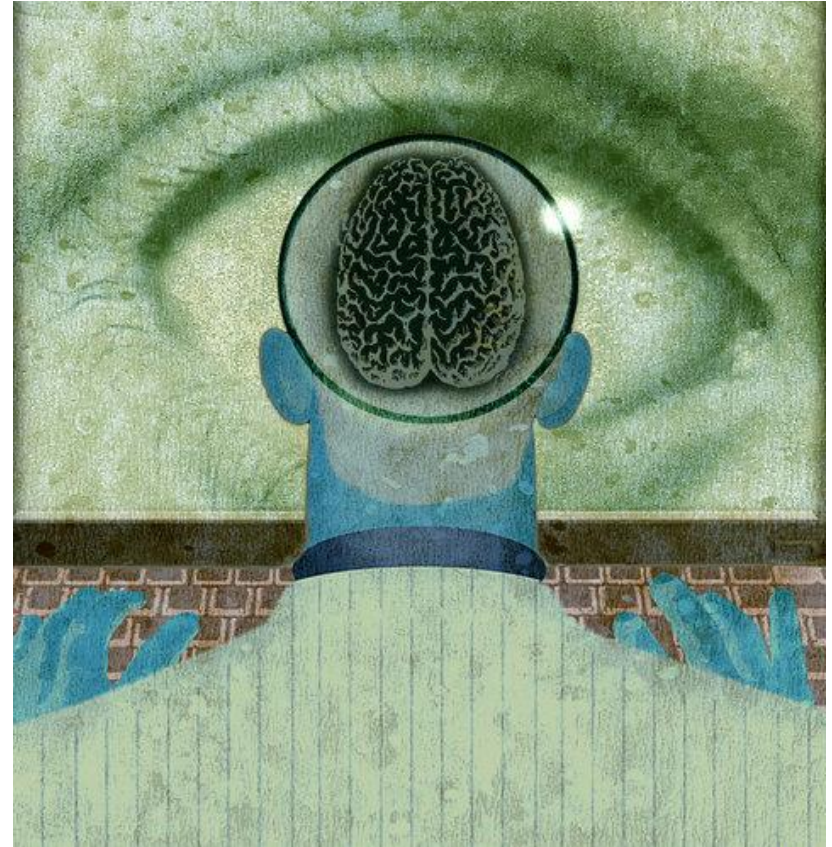


Security and Cloud Computing

Situation Assessment

“Big Data Is Opening Doors, but Maybe Too Many”

- We have become a data-driven society; Big Data is here to stay
- The questions “Who has data about you?” and “Where is the data about you located?” are impossible to answer today
- Your responsibility is to ensure that ***proper access controls*** are in place

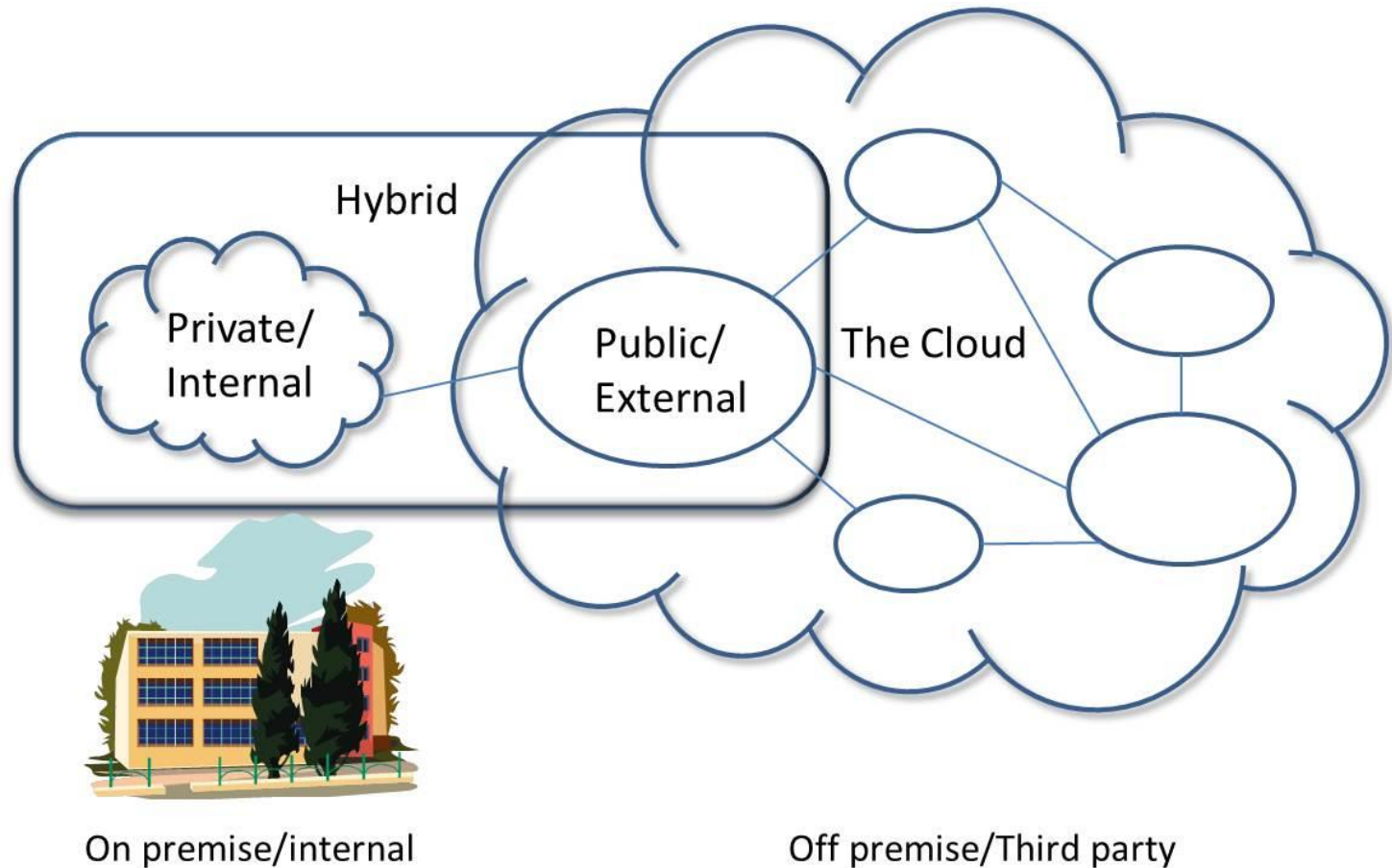


Anthony Freda

Source: New York Times, March 23, 2013



Types of Clouds: Public – Private – Hybrid



Cloud Computing Types

Source: Terry Bird, Chief Information Security Officer, DFG



Types of Clouds: Public – Private – Hybrid

Characteristic	Public cloud storage	Private cloud storage	Hybrid cloud storage
Scalability	Very high	Limited	Very high
Security	Good, but depends on the security measures of the service provider	Most secure, as all storage is on-premise	Very secure; integration options add an additional layer of security
Performance	Low to medium	Very good	Good, as active content is cached on-premise
Reliability	Medium; depends on Internet connectivity and service provider availability	High, as all equipment is on premise	Medium to high, as cached content is kept on-premise, but also depends on connectivity and service provider availability
Cost	Very good; pay-as-you-go model and no need for on-premise storage infrastructure	Good, but requires on-premise resources, such as data center space, electricity and cooling	Improved, since it allows moving some storage resources to a pay-as-you-go model



What is Cloud Computing?

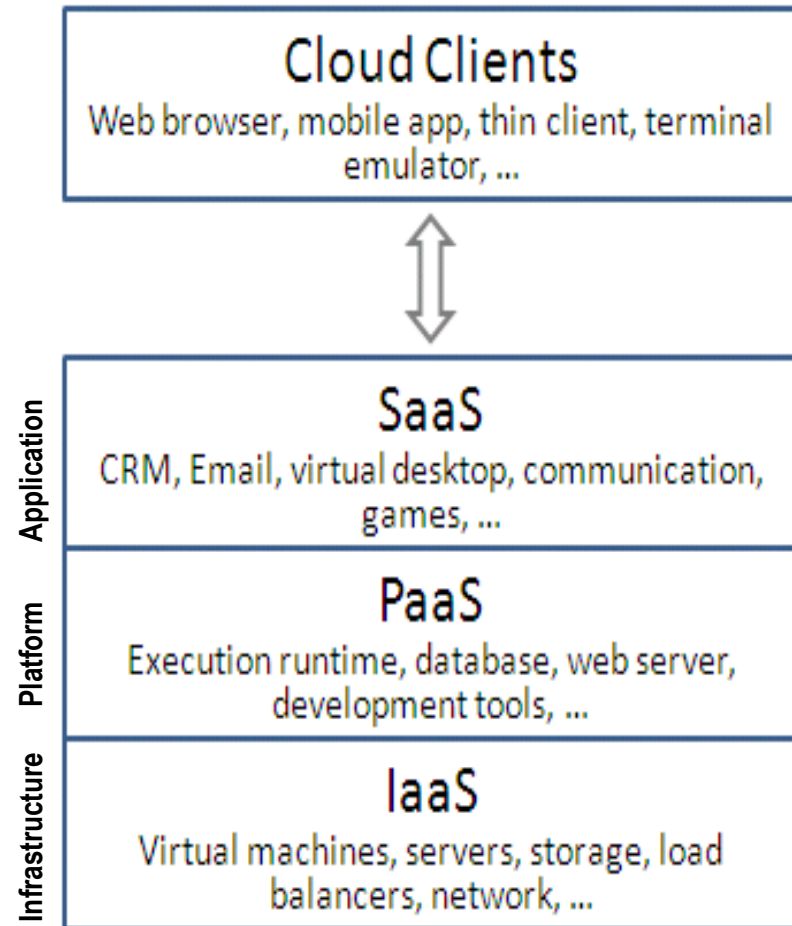
Infrastructure as a Service (IaaS) -

Fundamental computing resources to deploy software, including OS and applications (for example, Rackspace Cloud, Amazon EC2, SAVVIS)

Platform as a Service (PaaS) -

Applications based on programming languages and tools supported by the cloud provider (for example, Force.com, Google App Engine, OpenShift)

Software as a Service (SaaS) - Cloud provider applications running on a cloud infrastructure (for example, Salesforce.com, SuccessFactors, CloudPay, Workday)



Source: Terry Bird, Chief Information Security Officer, DFG



Key Considerations with Moving to the Cloud

- Develop a Risk Management Plan. Understand what business processes the vendor will perform and which ones you will perform.
- Define clearly areas of responsibility. Even though you are outsourcing some or all of the process to a vendor, you may still own the risks.
- Request the vendor's latest Service Organization Controls (SOC) report(s). There are three types, so it is important to receive all relevant reports.
- Create a list of topics and questions specific to the business processes that your vendor performs and develop a checklist to assess how well they are meet your expectations.



Checklist for Cloud Providers (1 of 5)

1. Data Protection

- How is your data separated from other customers' data and protected while at rest and in motion?
- What authentication and access controls are in place to protect your data?
- Can the vendor ensure that your data is securely removed/erased when requested, on a schedule or at termination of an agreement?

2. Identity Management

- Can the vendor support a security model that uses your usernames and passwords (SSO, SAML, ADFS, etc.)?
- What security parameters are in place to protect your information?

Source: Terry Bird, Chief Information Security Officer, DFG



Checklist for Cloud Providers (2 of 5)

3. Vulnerability Management and Incident Response

- Does the vendor have a vulnerability management program that scans for vulnerabilities on networks, servers, and applications including web applications? If so, what is the vulnerability remediation process?
- In the event of a breach, what is the vendor's notification process?

4. Availability

- What is the vendor's historical and guaranteed uptime?
- What is the vendor's peak load and do they have capacity to handle not only your current, but also your future needs?

Source: Terry Bird, Chief Information Security Officer, DFG



Checklist for Cloud Providers (3 of 5)

5. Privacy

- How does the vendor protect your data and ensure that only authorized users can access the data?
- How does the vendor remain in compliance with privacy requirements/ regulations (HIPAA, Safe Harbor, Data Protection Act, PCI-DSS, etc.)?

6. Application, Database and Network Security

- What security measures does the vendor have in place to protect the production environment?
- Does the vendor develop applications using secure coding configurations such as OWASP?

Source: Terry Bird, Chief Information Security Officer, DFG



Checklist for Cloud Providers (4 of 5)

7. Business Continuity and Disaster Recovery

- Does the vendor have a BCP and DRP? Are the plans available for review? What are the guaranteed SLAs under a DR scenarios?

8. Compliance Requirements/Certifications

- Is the vendor compliant/certified in all of the areas required for the business processes that will be handled (PCI-DSS, HIPAA, Basel II, Safe Harbor, Sarbanes-Oxley, privacy regulations, etc.)
- Does the vendor have current non-qualified SSAE16/ISAE3402, SOC-1, SOC-2 or SOC-3 report(s) available that cover the business processes that will be handled?

Source: Terry Bird, Chief Information Security Officer, DFG



Checklist for Cloud Providers (5 of 5)

9. Other Legal Contractual Considerations/Requirements

- What are the penalties and fines if the vendor does not meet the agreed upon SLAs?
- Non-Disclosure Agreement (NDA) specifying data ownership and agreeing that data will not be disclosed outside of the contract terms.
- Requirement that the vendor submits proof of compliance requirements/certifications at least annually.
- Annual submission of a passing SOC report. If not, then the vendor must perform an audit on all processes performed by vendor.
- Statements on intellectual property, who owns what? If the vendor is developing a custom application, who owns the code, etc.?
- How can you and/or the vendor terminate the contract? What fees/actions are associated with either?

Source: Terry Bird, Chief Information Security Officer, DFG



Details on SOC Reports

- **SOC-1: Reporting on Controls at a Service Organization**

- An independent audit report of internal controls over financial reporting (ICFR), associated with Statement on Standards for Attestation Engagements (SSAE) 16. There are two types of SSAE 16 reports; Type 1 is a report on a service organization's system and the suitability of the design of controls and Type 2 is a report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls
- Note that there is an identical standard for international SO's, International Standard on Assurance Engagements (ISAE) 3402

- **SOC-2: Report on Security, Availability, Integrity, Confidentiality, Privacy (for Cloud/SaaS)**

- This report type is intended to meet the need to understand an SO's internal controls around confidentiality, availability, integrity, security and privacy. It is intended for use by stakeholders such as customers, regulators, business partners, suppliers and directors. Similar to SOC-1, there are two types: type I, report on management's description of an SO's system and the suitability of the design of controls, and type II, report on management's description of an SO's system and the suitability of the design and effectiveness of controls.
- SOC-2 should be of great interest to many SOs, including data centers and cloud computing companies. It also applies to any entity subject to HIPAA or the US Gramm-Leach-Bliley Act (GLBA) and other key compliance requirements.

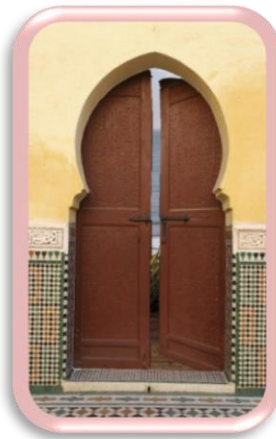
- **SOC-3: Trust Services Report for Service Organization**

- Trust Services was revised by AICPA in 2010 to incorporate the former SysTrust (security, etc., of a system) and Privacy (especially personal data) principle documents that were in place for years. This report type is intended to meet the needs of users who want assurance on the controls at an SO such as confidentiality, availability, processing integrity, security and privacy, but who do not have the need for or the knowledge necessary to make effective use of a SOC-2 report. The reports are for general use and, therefore, can be freely distributed or posted on a web site.

Source: Terry Bird, Chief Information Security Officer, DFG



Conclusion



Conclusion

1. Assess the product globalization strategy and the global capabilities of your vendors
2. Build a global compliance framework to assess your level of risk by country and business process
3. Evaluate the security and access controls around your cloud computing platform



**For more information on this or any
other HR technology topic go to**



<http://core.ihrim.org>

