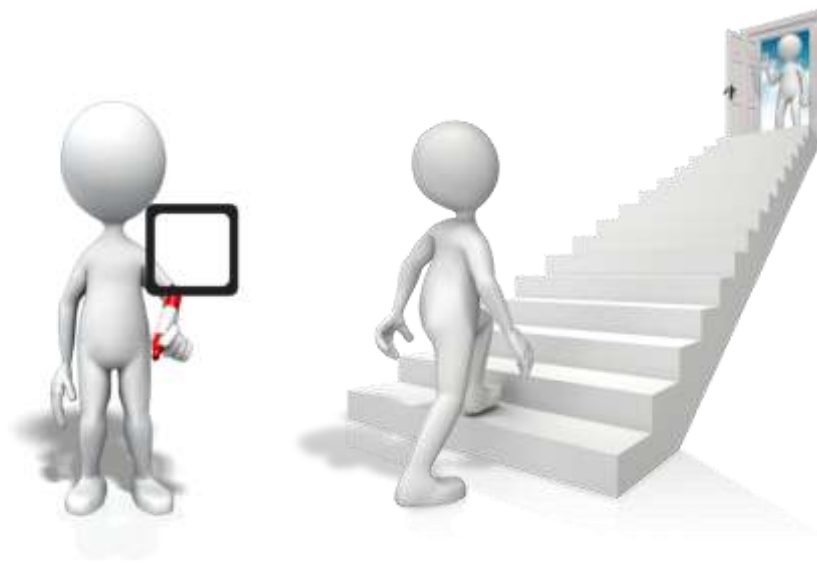




PROTECHT.
LEADERSHIP IN RISK SOLUTIONS

Optimising the Compliance Function in 2014 and beyond

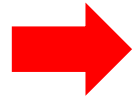


David Tattam
Director
Protecht

Agenda

1. Defining External and Internal Compliance
2. Compliance frameworks
3. Practical solutions
4. Hurdles to success in compliance and how to overcome them

Agenda



1. Defining External and Internal Compliance
2. Compliance frameworks
3. Practical solutions
4. Hurdles to success in compliance and how to overcome them

Compliance

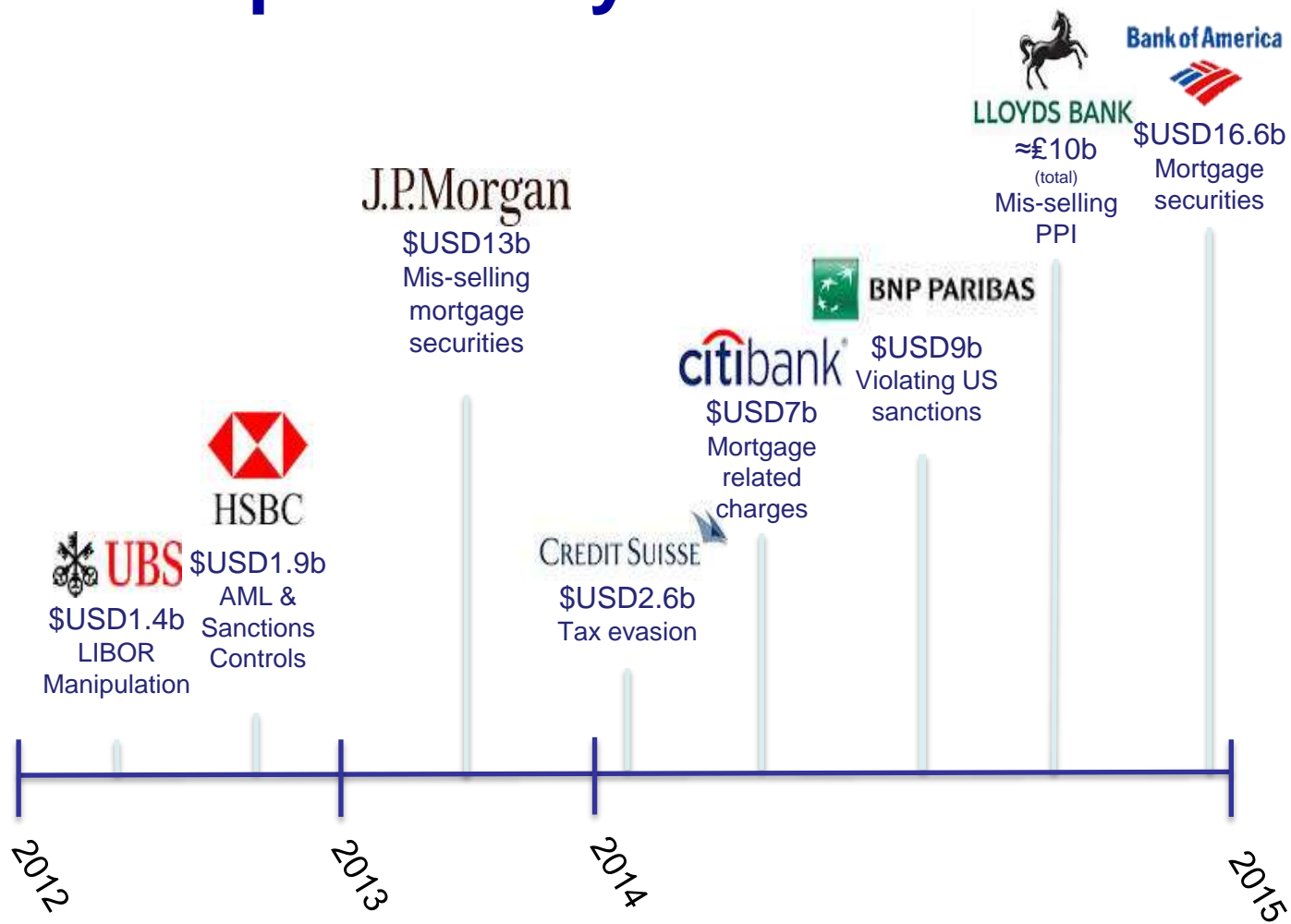
“Conforming to a rule”

Rules may be legal or voluntary obligations and may come from:

- **External:** Laws, Regulations, Codes, Standards
- **External:** Customers, suppliers, lenders
- **Internal:** Policies, Procedures, Controls, Codes

It is more than just meeting the requirements of laws and regulations!

Importance of Compliance: Non compliance by banks



Recent News

March 13, 2014

The EU has updated its 19-year-old data protection laws, with stronger safeguards for citizens' personal data. The new European data protection laws mean that companies found in breach of users' personal data rights will risk fines of up to €100m

Sept 3, 2014

The **European Commission fines smart card chip makers €138 million** (\$181 million) for coordinating their market behavior, thus violating European Union (EU) anti-competition rules that prohibit cartels. In other words, they were punished for price fixing smart card chips.

Samsung, Philips and Infineon colluded through bilateral contacts that occurred from September 2003 to September 2005.

For cooperating with the Commission, i.e. revealing the cartel's existence, Renesas (a Mitsubishi-Hitachi joint venture at the time) received full immunity under the EU's 2006 Leniency Notice.

Philips and Infineon will appeal.

Ensuring compliance

How can we ensure that we comply?

1. Attestations
2. Risk management of the risks that could lead to non-compliance
“Compliance Risk Management”
3. A combination of these techniques decided on a risk based approach = **Compliance Plan**

We need to build a risk based compliance process that is effective and efficient.

Agenda

1. Defining External and Internal Compliance

 2. Compliance frameworks

3. Practical solutions

4. Hurdles to success in compliance and how to overcome them

ONR 192050: Compliance Management Systems

1. 2013 Austrian Standard
2. Minimum standards for development, introduction and maintenance of a CMS
3. Requires certification
4. Only covers statutory compliance and not voluntary
5. Definitions:
 - Compliance: observance of regulations
 - Regulations: all statutory obligations ...
 - Compliance risk: risk of compliance failure
6. Includes compliance risk assessment and measures

ISO 19600: Compliance Management Systems - Guidelines

1. 2012 – Australia proposed ISO standard on compliance programs based on local AS 8306 standard.
2. Adopted as a final draft in Vienna July 2014
3. Risk based approach to compliance – aligned to the ISO 31000 Risk Management guidelines.
4. To be used for a company wide compliance management programme
5. Definitions
 - **Compliance:** Meeting all the organisation's compliance obligations
 - **Compliance Obligation:** requirement that an organisation has to, or chooses to, comply with
 - **Compliance risk:** effect of uncertainty on compliance objectives
 - **Noncompliance:** non-fulfilment of a compliance obligation

Compliance Risk Management Framework ISO 19600

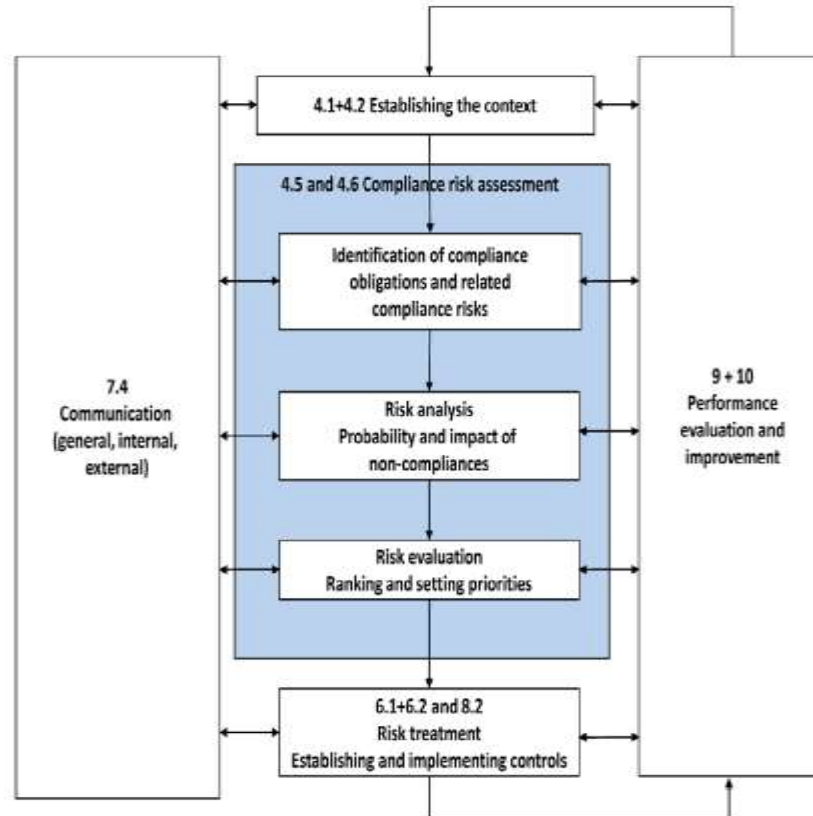


Figure 2 – Risk-based approach in ISO 19600 to compliance management according to ISO 31000 (numbers refer to clause number in ISO/DIS 19600)

ISO 19600 – “Compliance” and ISO 31000 – “Risk” alignment

ISO 31000	ISO 19600
1. Communicate and Consult	1. Communication
2. Establish the Context	2. Establish the Context
3. Risk Identification	3. Obligations and compliance risk identification
4. Risk Analysis	4. Risk Analysis
5. Risk Evaluation	5. Risk Evaluation
6. Risk Treatment	6. Risk Treatment
7. Monitoring and Review	7. Performance evaluation and treatment

Agenda

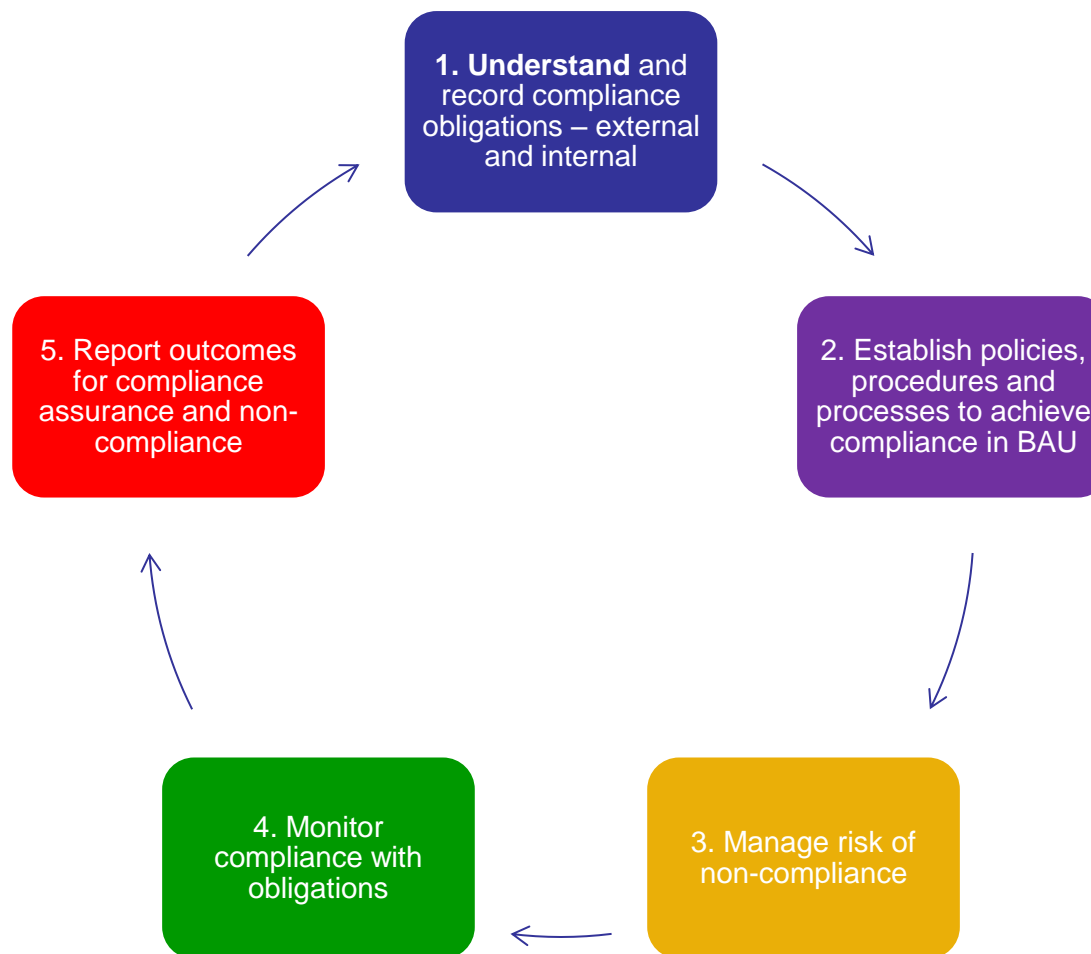
1. Defining External and Internal Compliance

2. Compliance frameworks

 3. Practical solutions

4. Hurdles to success in compliance and how to overcome them

Overall Compliance Framework



1. Understand

The Obligations Register

- An understanding of the company's legal and regulatory obligations. There should be a register that is available company wide and contains information such as:
 - Act or Regulation Name
 - Relevant sections for your organisation
 - Which managers are impacted by the legislation
 - What the legislation means in a practical sense to your company.
 - How the obligation is managed – what controls are in place.
 - Penalties associated with non-compliance
 - A link to policies/procedures that support compliance.
- Users should be able to view their obligations easily by either business unit, function, or owner?
- Process of keeping register up to date. Maybe achieved by internal legal department and / or use of external content provider using “alerts”.

2. Establish

Policies, Procedures and Processes that reflect current legislation and compliance thereto

- Policies that demonstrate how the company complies with current obligations. Policies should be updated to reflect any changes in the legislation. Control over ownership of the policies, review date, and modifications should be evident.
- Procedures and processes must be amended to ensure compliance on day 1.

Checklists

- Checklists can be used by staff to ensure compliance with complex legislation as they undertake their day to day activities. This will be built in as part of the process

Training

- Relevant courses made available to staff to ensure they understand their obligations and a record of training completed should be maintained.

3. Manage Risk of Non-Compliance

Determine methodology of risk management. Should be the same as for ERM

The risk of non-compliance can be managed in one or more ways including:

- Compliance risk and controls self assessment
- Key risk and key control indicators
- Compliance breach management
- Controls assurance for controls over non-compliance
- The outcomes of attestations
- Independent compliance reviews

4. Monitor

Monitor the ongoing level of compliance to provide assurance of otherwise as to the level of compliance to obligations

Monitoring can be undertaken using one or more of the available compliance controls and risk management processes including:

- Key risk and key control indicators
- Controls assurance for controls over non-compliance
- Attestations
- Independent compliance reviews

Attestations

Part of ongoing monitoring of compliance. A robust attestation program for key managers, supported with evidence that compliance policies are being followed, and any breaches properly reported. Typically done through questionnaires completed through a GRC system, or excel/word.

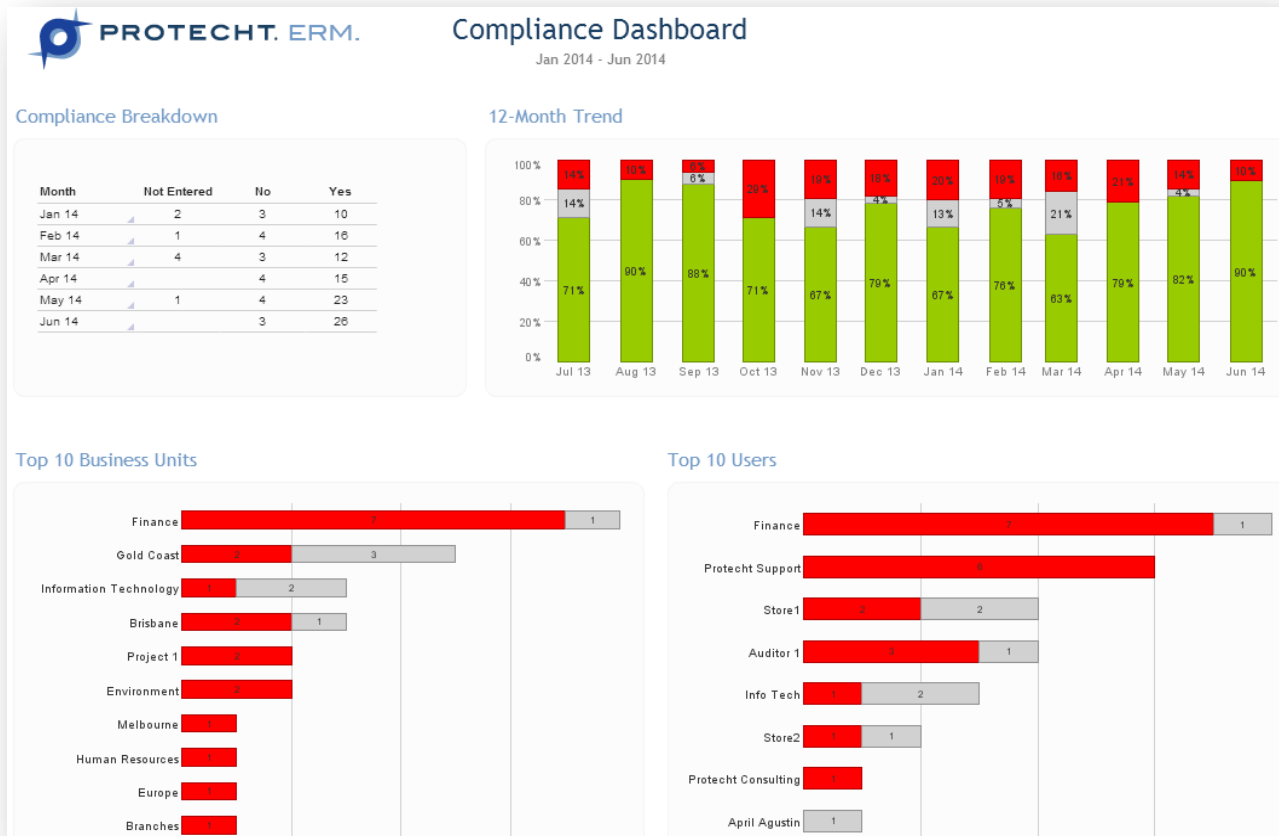
Key components

1. Identify the business unit and / or the person who has responsibility for each “rule”
2. Create clear and easily understood questions relating to each rule, that can be asked of the person responsible, to obtain an “attestation” of compliance
3. Send out compliance attestation requests periodically
4. Obtain attestations answers and where possible, related evidence of compliance
5. Follow up non-compliance and resolve
6. Ongoing reporting

5. Report

Report the findings of the controls and risk management processes around compliance

This will include reports showing the results of Attestations, Risk Assessments, KRIs, Controls Assurance, Compliance Breaches, Compliance Reviews



Compliance Risk Management

Key components

1. Recognise that “non-compliance” as a risk impact (the results of a risk occurring)
2. Identify the key risks that exist that could lead to non-compliance
3. Identify the key controls that exist over the key risks
4. Carry out an assessment of the key risks and controls to provide a “health check” of the compliance process
5. Controls assurance to ensure the key controls are working
6. Implement key risk indicators
7. Implement compliance breach incident management
8. Identify any issues and ensure actions to rectify and put in place and implemented

Compliance Risk Assessment - ONR 192050

Minimum steps:

- Identification of compliance-related processes with a view to the regulations;
- Identification of compliance risks and assessment by their probability of occurrence and consequences;
- Prioritization and, based thereon, implementation of measures.
- Binding instructions must be developed from the risk assessment aimed at preventing or, if applicable, detecting breaches of regulations
- Training must be carried out and recorded based on the risk assessment
- Monitor observance of instructions periodically plus checks of compliance related processes
- Report breaches

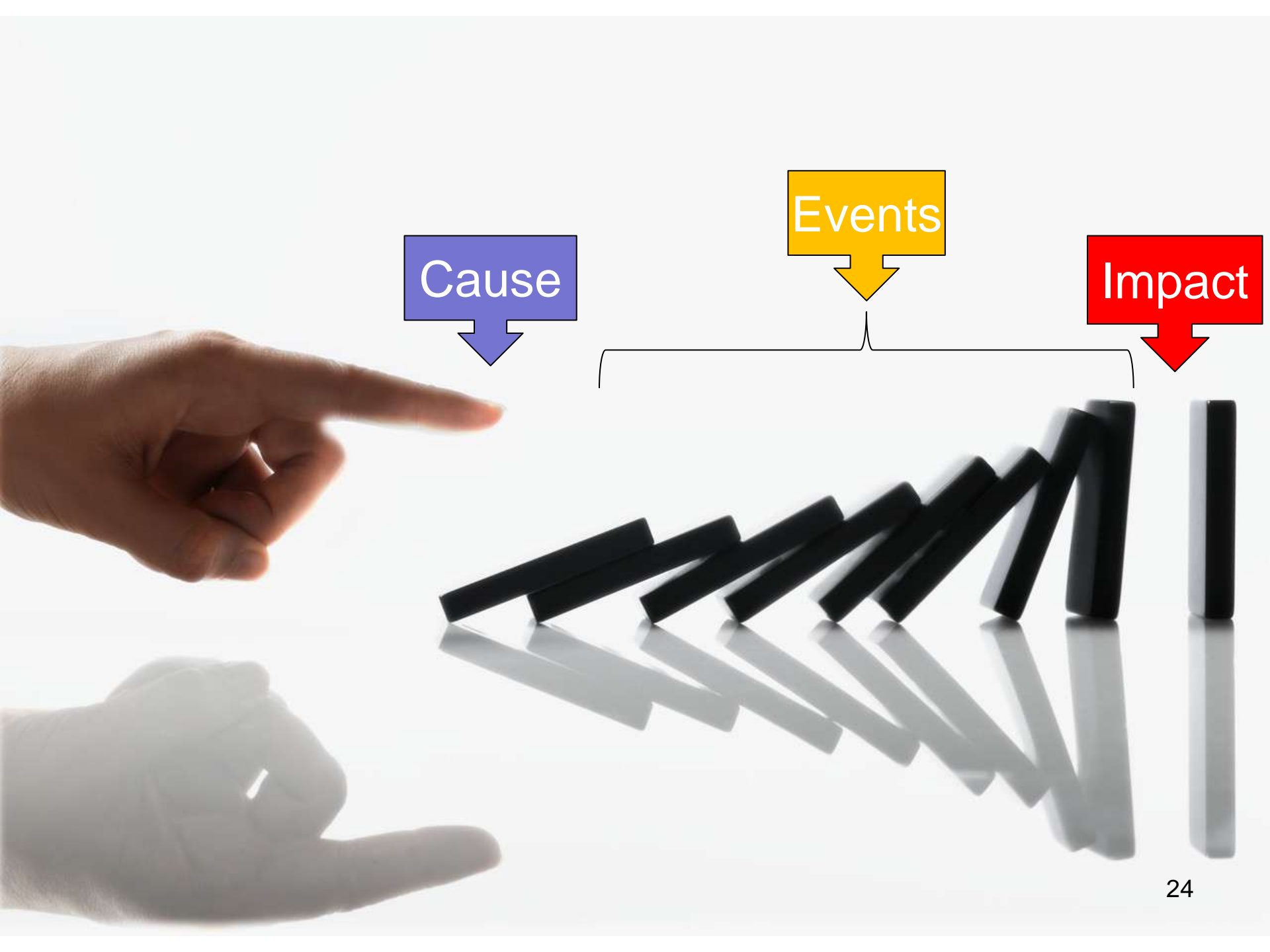
Data Loss

Group remuneration information was unintentionally lost to the media. With a critical piece of work due the next day, Kurt took his laptop home to continue working. On the train ride home and exhausted from work, Kurt put his laptop to the side and fell asleep. When awaking to find his station, Kurt left the train and headed home, leaving the laptop on the train.

The laptop was found by a journalist which resulted in the media releasing some sensational headlines. These headlines continued for over a week, significantly damaging the organisation's reputation and brand. Protests also occurred outside of Head Office causing disruption to the business and employee distress.

It was later revealed that the lost data included customer and employee personal details. Kurt was also a temporary staff member (due to lack of staff in market) who had previously worked of the organisation and was previously removed due to poor performance. In addition, Kurt should no longer have had access to the staff remuneration files or client files as he had moved departments but his access rights had not been removed. Also, given his recent change in department, he had put his password on a post-it-note on the inside of his laptop for safe keeping which was used to access the data.

The organisation suffered regulatory fines due to breach of DSG 2000: Federal Act concerning the Protection of Personal Data S14: Data Security Measures.



Cause

Events

Impact

Data Loss

Group remuneration and client information was unintentionally lost to the media. With a **critical piece of work due the next day**, Kurt **took his laptop home** to continue working. On the train ride home and **exhausted from work from excessive workload**, Kurt put his laptop to the side and **fell asleep**. When awaking to find his station, Kurt left the train and headed home, **leaving the laptop on the train**.

The **laptop was found by a journalist** which resulted in the media releasing some **sensational headlines**. These headlines continued for over a week, significantly **damaging the organisation's reputation and brand**. **Protests** also occurred outside of Head Office causing **disruption to the business** and **employee distress**.

It was later revealed that the lost data included customer and employee personal details. Kurt was also a **temporary staff member** (**due to lack of staff in market**) who had previously worked of the organisation and was previously removed due to **poor performance**. In addition, Kurt should no longer have had access to the staff remuneration files or client files as he had moved departments but his **access rights had not been removed due to human error**. Also, given his recent change in department, he had put his **password on a post-it-note** on the inside of his laptop for safe keeping which was used to access the data.

The organisation suffered **regulatory fines** due to **breach of DSG 2000**: Federal Act concerning the Protection of Personal Data S14: Data Security Measures.

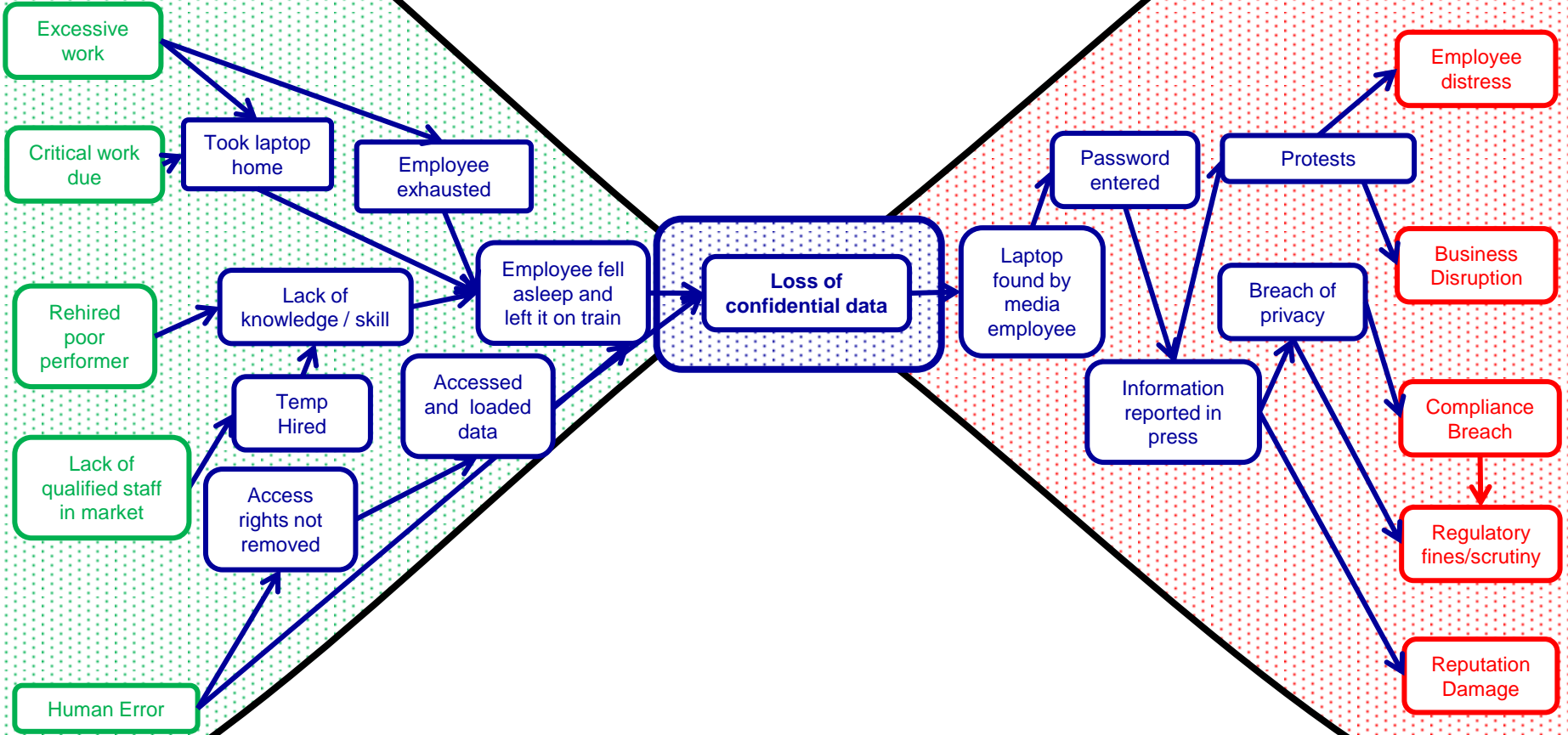
Cause **Event** **Impact**

The Risk Story

Causes

Events

Impacts



Data Loss

Group remuneration and client information was unintentionally lost to the media. With a **critical piece of work due the next day**, Kurt **took his laptop home** to continue working. On the train ride home and **exhausted from work from excessive workload**, Kurt put his laptop to the side and **fell asleep**. When awaking to find his station, Kurt left the train and headed home, **leaving the laptop on the train**.

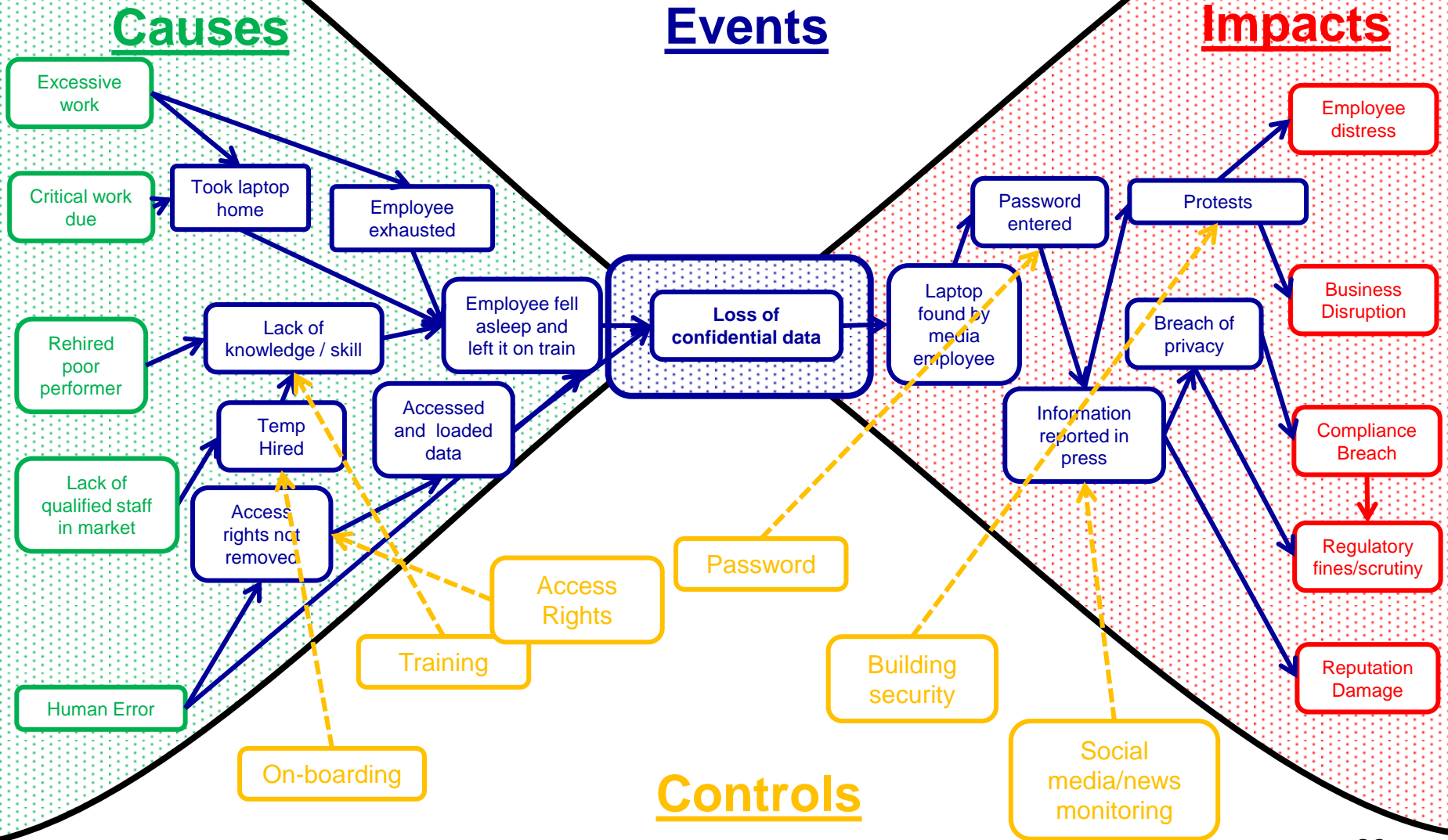
The **laptop was found by a journalist** which resulted in the media releasing some **sensational headlines**. These headlines continued for over a week, significantly **damaging the organisation's reputation and brand**. **Protests** also occurred outside of Head Office causing **disruption to the business** and **employee distress**.

It was later revealed that the lost data included customer and employee personal details. Kurt was also a **temporary staff member** (**due to lack of staff in market**) who had previously worked of the organisation and was previously removed due to **poor performance**. In addition, Kurt should no longer have had access to the staff remuneration files or client files as he had moved departments but his **access rights had not been removed due to human error**. Also, given his recent change in department, he had put his **password on a post-it-note** on the inside of his laptop for safe keeping which was used to access the data.

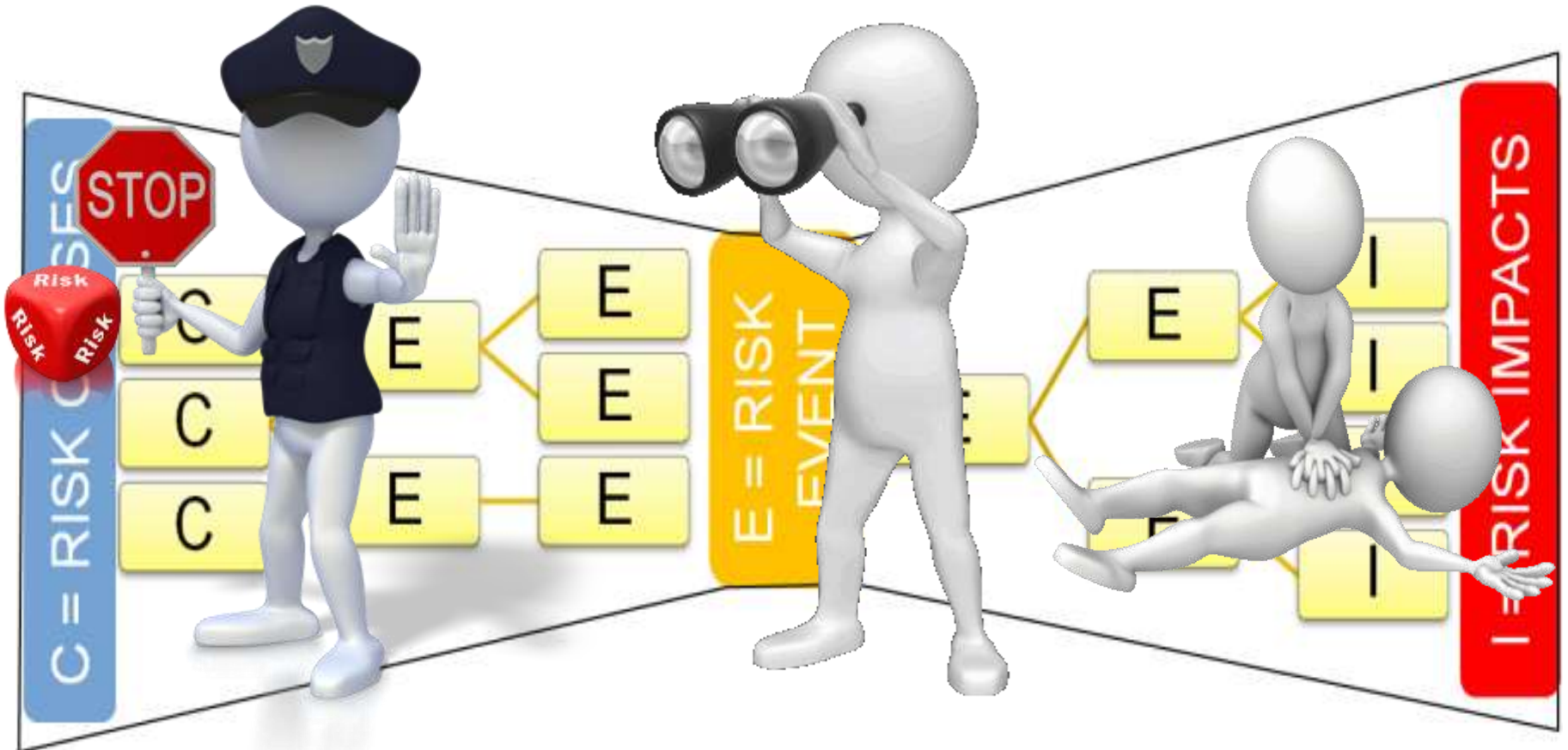
The organisation suffered **regulatory fines** due to **breach of DSG 2000**: Federal Act concerning the Protection of Personal Data S14: Data Security Measures.

Cause **Event** **Impact** **Controls**

The Risk Story



Control Types




Preventive

Detective

Reactive

Agenda

1. Defining External and Internal Compliance
2. Compliance frameworks
3. Practical solutions
-  4. Hurdles to success in compliance and how to overcome them

Towards the optimal compliance process

- Too cumbersome and too much effort and cost to manage
 - Integrate with an overall ERM process to gain efficiencies such as avoiding duplication
 - Adopt a risk based approach to compliance. Determine the compliance management process based on an initial risk assessment
 - Use a specialist Risk and Compliance system that automates the process, workflows the process and enables live dashboard reporting.
- Lack of buy-in from Board, Management and Staff
 - Educate to demonstrate that compliance is an enabler not a hindrance
 - Demonstrate a risk based approach rather than a cumbersome “tick and flick” process
 - Minimise effort (as above)
 - Make compliance understandable – turn legal language into easily understood obligations
- Difficulty in maintaining obligations libraries
 - Have one single library, systemised as part of the risk and compliance system
 - Develop a process, perhaps using external parties, to continually monitor for changes and updates which is linked to updated compliance questions
 - Assign responsibility for the register and its maintenance

Towards to optimal compliance process

- Too complex
 - Use dedicated risk and compliance system that:
 - Maintains all compliance management components (obligations register, risk assessment, attestations etc)
 - Links all components together (links compliance questions to legislation etc)
 - Workflows information so that alerts and actions are automatic
 - Train staff in the overall framework and the “why?”

Ultimate State



Compliance Dashboard

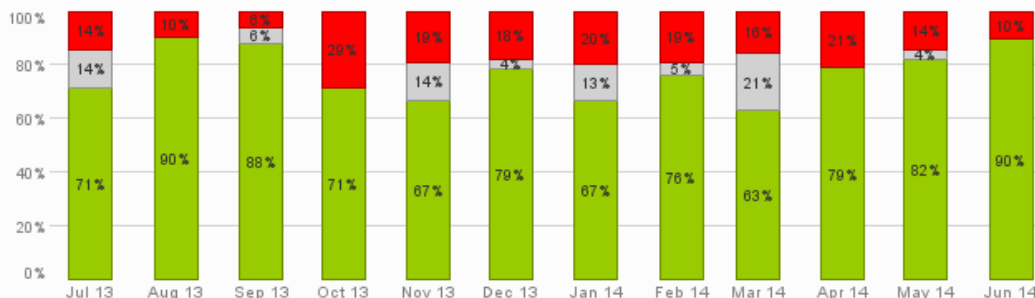
Compliance Dashboard

Jan 2014 - Jun 2014

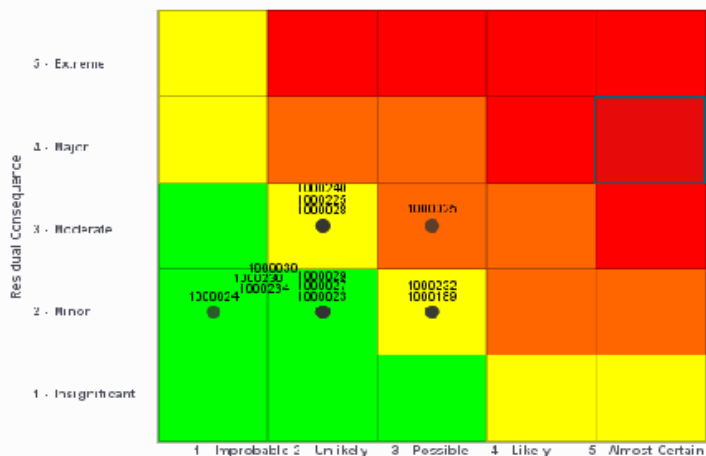
Compliance Breakdown

Month	Not Entered	No	Yes
Jan 14	2	3	10
Feb 14	1	4	16
Mar 14	4	3	12
Apr 14		4	15
May 14	1	4	23
Jun 14		3	26

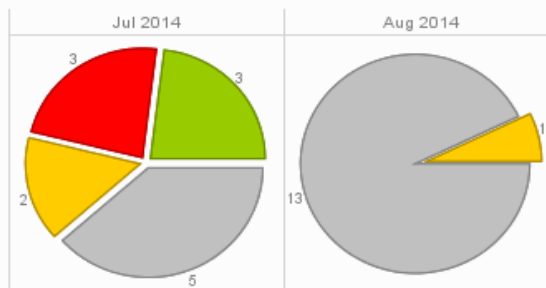
12-Month Trend



Residual Risk Assessment



Ratings Breakdown



Actions

59 Total Actions	45 Open Overdue Actions
46 Open Actions	17 Open Slipped Actions
13 Closed Actions	0 Due in Next 60 Days

Compliance Attestation Dashboard

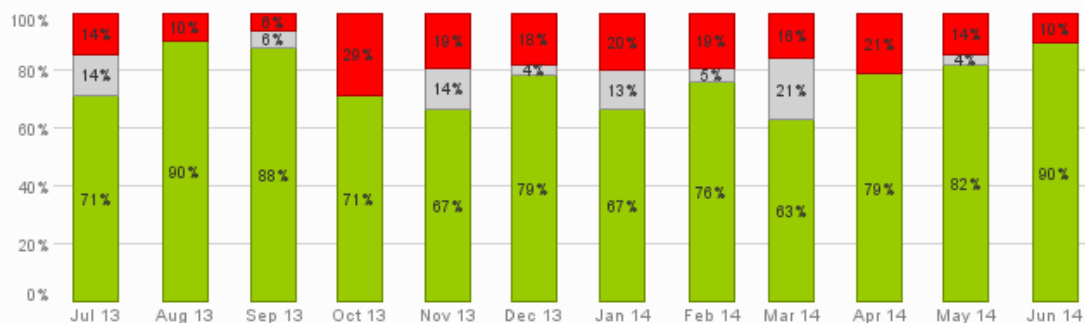
Compliance Dashboard

Jan 2014 - Jun 2014

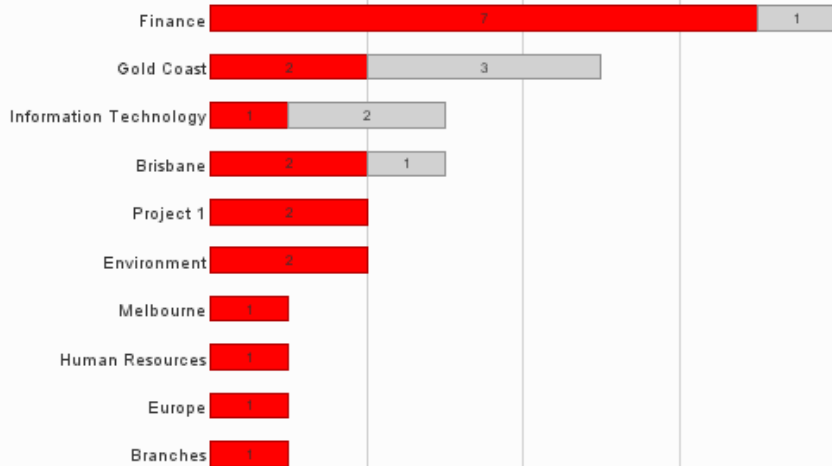
Compliance Breakdown

Month	Not Entered	No	Yes
Jan 14	2	3	10
Feb 14	1	4	18
Mar 14	4	3	12
Apr 14		4	15
May 14	1	4	23
Jun 14		3	26

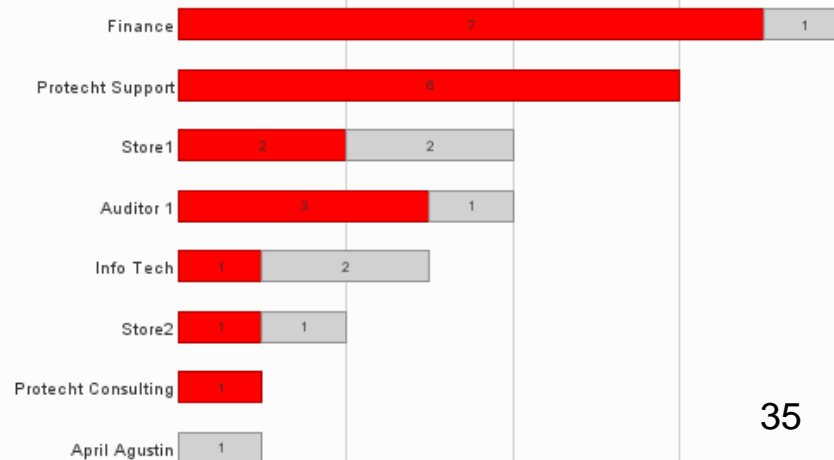
12-Month Trend



Top 10 Business Units



Top 10 Users



Compliance Attestation Dashboard contd

Compliance Details Dashboard

Feb 2014 - May 2014

Compliance Details

Business Unit	Control Name	Response	Confirmed	End of Period	Responsible	Status
Gold Coast	Can you confirm that ATM cash is counted and reconciled to the GL monthly by someone who is independent of ordering and stocking responsibilities?	Not Entered	No	28 Feb 2014	Store1	Open
Information Technology	Can you confirm that administrator passwords for all servers have been changed in the last 90 days?	Yes	No	28 Feb 2014	Info Tech	Open
Information Technology	Can you confirm that all laptops issued have PGP encryption installed on them?	No	No	28 Feb 2014	Info Tech	Open
Finance	Can you confirm that all new suppliers have had their ABN checked and payment details confirmed, prior to loading into the payments system?	No	No	28 Feb 2014	Finance	Open
Finance	Can you confirm that budget variances above 5% have been investigated and commented on?	Yes	No	28 Feb 2014	Finance	Open
Wollongong	Can you confirm that there were no changes to processes or systems that would require an update of the BCM plan?	Yes	No	28 Feb 2014	HR user	Open
Project 1	Can you confirm that there were no changes to processes or systems that would require an update of the BCM plan?	Yes	No	28 Feb 2014	Auditor 1	Open
Environment	Confirm control1 has been completed during the period	No	No	28 Feb 2014	Protecht Support	Open
Project 1	Do you have a formal policy that sets out the approach to BCM, and is this policy summarised in your risk management system?	Yes	No	28 Feb 2014	Auditor 1	Open
Human Resources	Has the OHS officer undergone a refresher training course within the past one year?	Yes	No	28 Feb 2014	HR user	Open
Europe	Has the OHS officer undergone a refresher training course within the past one year?	Yes	No	28 Feb 2014	Protecht Support	Open
Brisbane	Has the OHS officer undergone a refresher training course within the past one year?	Yes	No	28 Feb 2014	Auditor 1	Open
Supplier 1	Has the OHS officer undergone a refresher training course within the past one year?	Yes	No	28 Feb 2014	April Agustin	Open
Brisbane	Has the fire extinguishers for the mills been checked in the last 6 months?	Yes	No	28 Feb 2014	Auditor 1	Open
Information Technology	Has the website domain name been re-registered one month in advance of expiry date?	Yes	No	28 Feb 2014	Info Tech	Open
Finance	Have all insurance policies been reviewed and their adequacy to the Board reported at least once in the past 12 months?	Yes	No	28 Feb 2014	Finance	Open
Human Resources	Have all safety incidents within the past 3 months have been reported and recorded in the OHS register?	Yes	No	28 Feb 2014	HR user	Open
Brisbane	Have all safety incidents within the past 3 months have been reported and recorded in the OHS register?	Yes	No	28 Feb 2014	Auditor 1	Open
Finance	Have the bank reconciliations for the WBC account been completed by the 5th business day of the month? In the comments box record the number of items past 10 days outstanding.	No	No	28 Feb 2014	Finance	Open
Information Technology	Have you installed and maintained a firewall configuration to protect all employee computers?	Yes	No	28 Feb 2014	Info Tech	Open
Brisbane	Please confirm quarterly OHS meeting has been conducted? Attach minutes	Yes	No	28 Feb 2014	Auditor 1	Open
Gold Coast	Can you confirm that ATM cash is counted and reconciled to the GL monthly by someone who is	Yes	No	31 Mar 2014	Store1	Open





PROTECHT.
LEADERSHIP IN RISK SOLUTIONS

Thank You

David Tattam

Director

david.tattam@protecht.com.au

PROTECHT. RISK SOFTWARE.

PROTECHT. RISK ADVISORY.

PROTECHT. RISK TRAINING.

WWW.PROTECHT.COM.AU