Securing Loopholes in Compliance in the z/OS Environment

Sally Oliver
Action Software GmbH

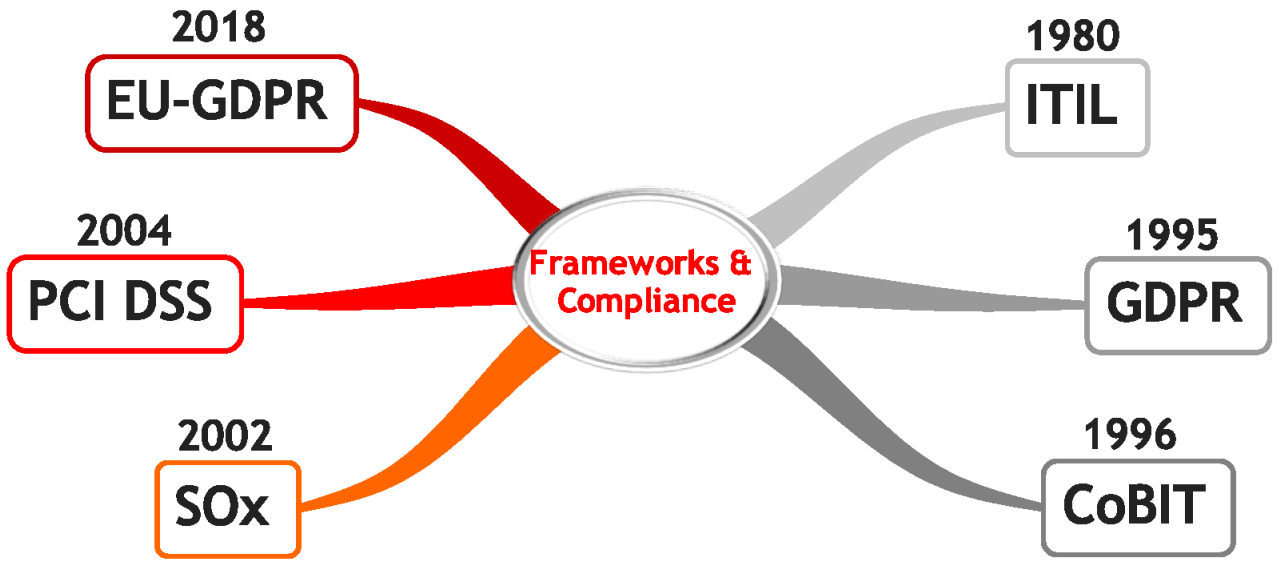
November 2018
Session FE

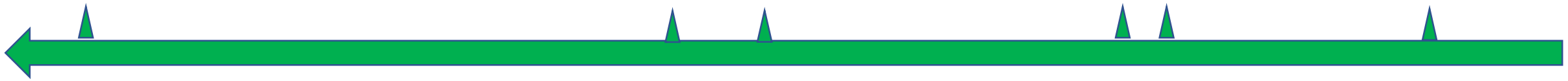



- Background to compliance
- Maximum penalties
- Recent known system malfunctions
- Key risk areas
- Control mapping to Industry Standards, Frameworks and Deficiencies
- Selected control categories
- Summary

Background to Compliance

From Industry Standards to Compliance





2018 Facebook 2.2b Twitter 319m

2015 Apple watch

2010 2 billion Web users ipad

2007 Kindle iphone

2006 Twitter launched

2004 Facebook launched

2000 USB drives Camera phones Y2K Bug

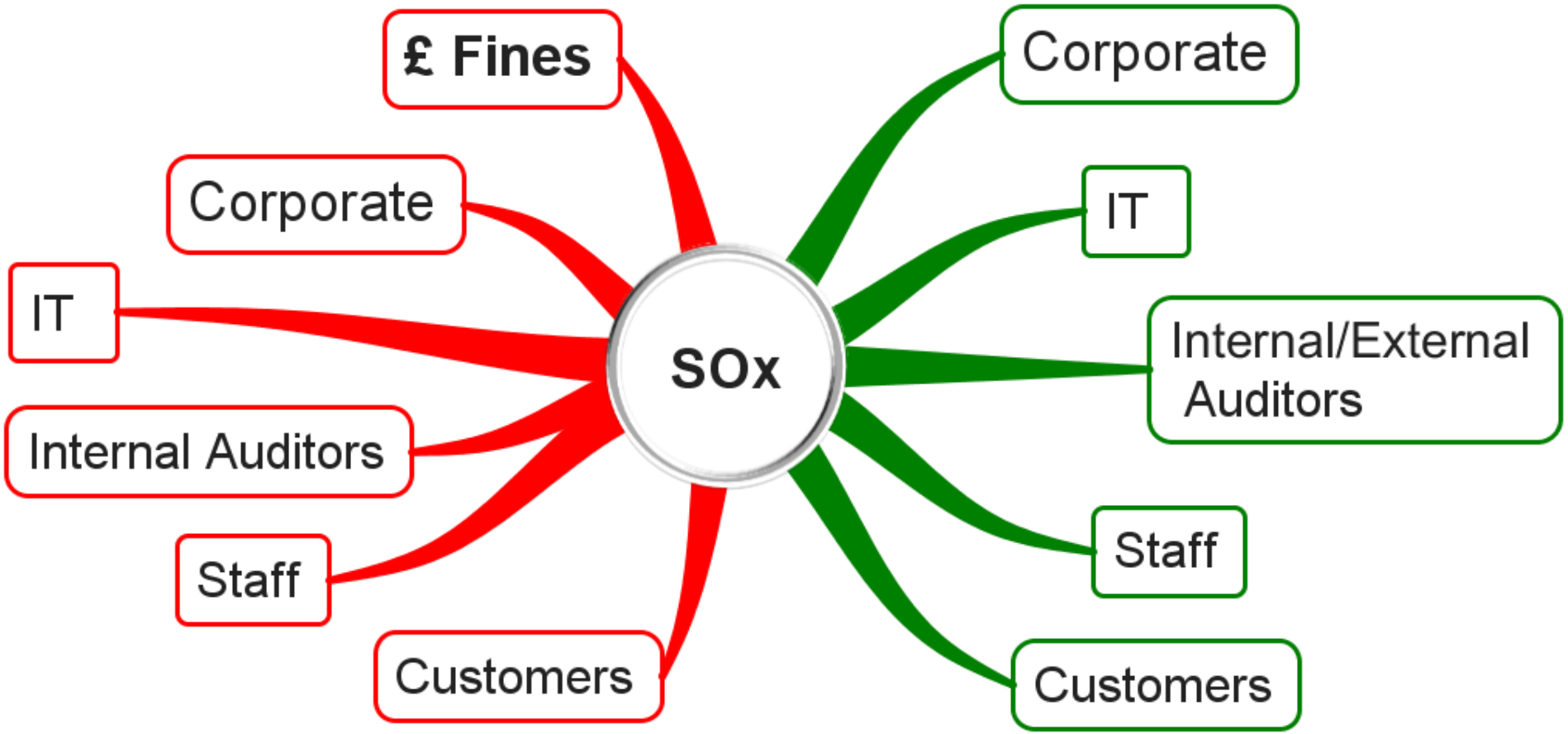
1999 WIFI in homes and cafes

1996 **36m** Web users

1990 Tim Berners Lee CERN WWW

1980 ATMs

1976 Apple micro computers



Sarbanes Oxley Compliance & Penalties

Compliance

SOx

- Sox Manager
- Board, Internal Auditors, IT, Finance
- External auditor independence required to limit conflict of interest
- Senior Executives take individual responsibility for financial reports
- Transparency in all accounting
- Complete audit trails
- Annual Sox compliance audit
- Change management
- Access, security and back-up procedures

Compliance

EU-GDPR

- Data Protection Officer
- All Staff aware/trained
- Member level
- Member right of access
- Member right to erasure
- Restriction of access
- Force segregation of duties for IT processes
- Reporting any breach within 72 hours

Maximum Penalties

Maximum Penalties

Sox

- Up to $5 Million
- Individual fine of $5m and/or imprisoned for up to 20 years,

EU-GDPR

- Up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher

Recent known System Malfunctions

Do as we say don't do as we do!

"EU falls short of its OWN data laws after accidentally publishing 700 records that include the names, addresses and mobile numbers of conference attendees."

Harry Pettit Mail ONLINE 31/5/2018

https://www.dailymail.co.uk/sciencetech/article-5790879/Embarrassing-leak-shows-EU-fallen-short-data-laws-publishing-700-records.html

Royal Bank of Scotland Outage 2012

Actual cost after 3.5m customers were unable to make payments for up to 3 weeks

- £56m fine – FCA £42m/PRA £14m
- £70m compensation
- £500m spent in next 2 years bolstering defences
- Investing £750m over 3 years on IT systems
- Staff bonuses cut
- Reputation damaged
- Still suffering problems
- Business disruption
- Lost revenue
- End-user productivity
- IT productivity
- Detection
- Recovery
- Equipment costs
- Third party costs

The Telegraph 20/11/2014
James Titcomb

Facebook

- Cambridge Analytica sold psychological profiles of the American voters to the political campaigns
- A former Trump aide was a board member of Cambridge Analytica
- Contact with a Kremlin-linked oil giant discussing the ways the data was used to target American voters
- The largest Facebook leak to date
- Final estimate of up to 87 millions mainly American users data harvested
- Data harvested using a personality quiz

TSB

- Migrating from a legacy system to a brand new platform designed for digital banking
- Planned shutdown of internet and mobile banking services for 1 week-end in April resulted in months of disruption
- Almost 2 million customers lost access to their accounts
- Banco Sabadell made a loss in the 3rd quarter of £123m as a result of TSB fiasco

VISA

- Customers in the UK and Europe were unable to use their cards after a system failure prevented access

  Visa said it was a hardware failure

  Chip and pin transactions were affected but ATM withdrawals were not

RBS

- 600,000 payments failed to enter RBS overnight including wages and benefit payments

British Airways

- Unable to get aircraft airborne as a result of a 3rd party travel tech supplier – Amadeus - suffering an outage

Welsh NHS

- Widespread computer failure blocked access to patient files

"Nothing travels faster than light, with the possible exception of bad news."

Douglas Adams

The Power of Social Media

Reality star Kylie Jenner tweeted to her 24 million Twitter followers.

"sooo does anyone else not open Snapchat anymore? Or is it just me… ugh this is so sad"

Snapchat lost $1.3 billion (£930m) in market value

February 2018

Main Key Risk Areas

Unauthorised Access

Problem Detection

Back-up Availability

Incomplete Audit Trail

Data Integrity

Outsourcing

Aging Mainframe Personnel

Illegal Software use

Undocumented Changes

Restoring the System

Control Mapping to Industry Standards, Frameworks and Deficiencies

12 Page Document

- 3 main sections: Control Mapping to Industry Standards
  Frameworks
  z/OS Deficiencies
- Management and Technical overview
- Headings: Control Category
  Industry Standard or Framework
  Industry Standard Control Requirements
  Risk of Taking NO Action

"For every minute spent organising, an hour is earned."

Benjamin Franklin

Selected control categories

Summary

- Perform a risk analysis on your system to see where it really meets the z/OS audit and compliance requirements
- Frameworks need computer driven processes to enforce them
- The more automation you can build into your systems the more you are providing an environment where core functions – particularly business critical and regulatory processes – can run more reliably.
- Improve controllability, stability and transparency to meet compliance.

Non-compliance is far more expensive and damaging than the cost of compliance

We want your feedback!

- Please submit your feedback online at ….
  - http://conferences.gse.org.uk/2018/feedback/FE

- Paper feedback forms are also available from the Chair person

- This session is FE