



DOCUMENT AUTOMATION SOFTWARE

GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE

HOW TO STRENGTHEN YOUR ORGANIZATION'S DEFENSES

Prepared by: ActiveDocs Enterprise Compliance Research Group
ActiveDocs Product Management Group

Audience: Senior Managers in Large Enterprises, Enterprise Governing Body Members, Process Optimization Specialists, Internal Audit Managers

Abstract: Organizations can strengthen their three lines of defense, following the ECIIA benchmark for regulatory guidance, with ActiveDocs, and reduce the effort associated with handling Governance, Risk Management, and Compliance.

OVERLAND PARK

Southcreek Office Park
7301 West 129th Street
Suite 160
Overland Park, KS 66213, USA
Ph +1 913 888 1999

LONDON

199 Bishopsgate
London
EC2M 3TY
United Kingdom
Ph +44 20 3290 1788

AUCKLAND

Level 6, 27 Gillies Avenue
Newmarket, Auckland 1023
Post: PO Box 289
Auckland 1140, New Zealand
Ph +64 9 520 5650

BRISBANE

192 Ann Street
Brisbane, QLD 4000
Post: PO Box 604
Paradise Point QLD 4216, Australia
Ph +61 7 3040 6616



Copyright

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of ActiveDocs Limited.

Copyright© ActiveDocs™ Limited. All rights reserved.

Microsoft is a registered trademark and Microsoft SQL Server, Microsoft Access, Microsoft Outlook, and Microsoft Windows are trademarks of Microsoft Corporation in the United States and/or other countries.

Other product and company names herein may be the trademarks of their respective owners.

Disclaimer: While ActiveDocs has taken care to ensure the accuracy and quality of this document, all content including fitness for a particular purpose are provided without any warranty whatsoever, either expressed or implied. In no event shall ActiveDocs, or its employees, be liable for any direct, indirect, incidental or consequential, special or exemplary damages resulting from the use of this document or from the use of any products described in this guide. Any persons or businesses mentioned within this document are strictly fictitious. Any resemblances to existing or deceased persons, or existing or defunct businesses, are entirely coincidental. This document will be updated regularly and changes will be included in later versions. If you experience any discrepancies in the content of this document, please e-mail info@activedocs.com.



Contents

1	Summary	1
2	Global Compliance Requirement Landscape.....	2
3	What is Governance, Risk Management, and Compliance (GRC)?	8
3.1	Definition of GRC	8
3.2	Role of GRC within Large Enterprises	8
4	Organizational three lines of defense	10
4.1	1 st Line of Defense.....	10
4.2	2 nd Line of Defense	10
4.3	3 rd Line of Defense	10
4.4	External Audit and Regulators	10
5	Governance, Risk Management, and Compliance with ActiveDocs	12
6	How ActiveDocs customers solved their GRC issues	16
6.1	Royal Dutch Shell – GRC in global HR.....	16
6.2	Ricoh – GRC in Sales	17
6.3	Bayer – GRC in pharmaceutical industry	18
6.4	ABB – GRC in Contract Management	19
7	Conclusions	20



1 Summary

The development of the trio of Governance, Risk Management, and Compliance is increasing the demand on the resources of organizations world-wide. It is becoming more difficult to keep up with the growing requirements of legislation and industry-specific regulations. In response, organizations need a system of defenses against the consequences of non-compliance in order to reduce their risk exposure. The European Confederation of Institutes of Internal Auditing (ECIIA) has issued benchmark guidance for regulatory compliance mechanisms recommending a 'three lines of defense' model to improve organizations' governance and reduce overall risk exposure. ActiveDocs is an enterprise-grade tool that strengthens all three lines of defense, and has been used by large global organizations such as Shell, Bayer, ABB, and many others.



2 Global Compliance Requirement Landscape

Increasingly tighter compliance requirements have been imposed on all aspects of running of a business. This has been of particular importance within the realm of both internal and external communication, and reporting within the business. Every piece of outgoing external communication can be subjected to scrutiny under multiple applicable laws and industry-specific regulations. Even internal communication has become increasingly regulated, following the slow-moving wave of accounting audit regulations that started with the Sarbanes-Oxley Act, and has extended into other auditable areas of business.

Examples of both internal and external communication that can be subjected to legal and regulatory scrutiny are shown below.

Employment contracts	Shareholder reporting
Insurance policies	Internal policies and procedures
Business contracts	Police/security check documentation
Contractor agreements	Contracts
Promotional emails	Proposals
Business emails	Business correspondence
Customer communication	Insurance policies
Helpdesk communication	Financial statements
Purchase agreements	Customer communication
RFP responses	Quotes
Accounting reports	Online statements
Board reports	Loyalty/reward program communication

Many of the listed types of communication and documents are required to comply with multiple laws and regulations.



Employment Contracts

USA

Federal Legislation and Regulations

Fair Labor Standards Act
National Labor Relations Act
Occupational Safety and Health Act
Employee Retirement Income Security Act
Family and Medical Leave Act
Labor Management Reporting and Disclosure Act

State specific employment legislation

Industry specific regulations

UK (England, Wales)

Employment Rights Act
National Minimum Wage Act
National Minimum Wage Regulations
Working Time Regulations
Working Time Directive
Maternity and Parental Leave, etc Regulations
Paternity Leave Regulations
Paternity and Adoption Leave Regulations
Parental Leave Directive
Transfer of Undertakings (Protection of Employment) Regulations (If a company is taken over)
Health and Safety at Work Act
Trade Union and Labour Relations (Consolidation) Act
Pensions Act
Finance Act
Income Tax (Earnings and Pensions) Act
Equality Act

At least **6** country-level laws, state-specific regulations, industry-specific regulations

At least **16** country-level laws, industry-specific regulations

Penalties for non-compliance†

Up to **\$500,000** and **5 years in prison**

Unlimited fine and up to **2 years in prison**

Employment Contract (continued)

New Zealand

Employment Relations Act 2000
Health and Safety in Employment Act 1992
Parental Leave and Employment Protection Act 1987
Parental Leave and Employment Protection Regulations 2002

Industry Specific
Health and Safety in Employment (Adventure Activities) Regulations 2011
Health and Safety in Employment (Asbestos) Regulations 1998
Health and Safety in Employment (Mining Administration) Regulations 1996
Health and Safety in Employment (Mining—Underground) Regulations 1999
Framework for the Accredited Employers Programme

At least **4** country-level laws and regulations, industry-specific regulations

Australia

Fair Work Act 2009
Fair Work Amendment Act 2013
Fair Work Regulations 2009
Fair Work Australia Rules 2010
Small Business Fair Dismissal Code
Fair Work (State Declarations—employers not to be national system employers) Endorsement 2009
Workplace Relations Act 1996
Workplace Relations Regulations 2006

At least **8** country-level laws and regulations, state regulations, industry-specific regulations

Penalties for non-compliance†

Up to **\$500,000** and **2 years in prison**

Up to **\$51,000** per offence incident



Insurance Policies

USA

Federal Legislation and Regulations

Homeowners Insurance Protection Act of 2013
 Competitive Health Insurance Act
 Federal Life Insurance Transparency Act
 Terrorism Risk Insurance Act of 2002 Reauthorization Act of 2013
 Insurance Consumer Protection and Solvency Act of 2013
 Access to Insurance for All Americans Act
 Small Farm Insurance Act of 2013
 Dental Insurance Fairness Act of 2013
 Social Security Disability Insurance for the Terminally Ill Act of 2013
 Insurance Capital and Accounting Standards Act of 2013
 Securities Act

McCarran-Ferguson Act 1945 – Historical de-centralization of regulation of insurance in USA which resulted in State specific Insurance regulation bodies – Insurance Commissioners/Directors of Insurance/Commissioners of Insurance/Superintendents of Insurance

UK (England, Wales)

Financial Services and Markets Act
 Contracts (Applicable Law) Act
 Insurance Conduct of Business Sourcebook
 Financial Services Authority Regulations
 Third Parties (Rights against Insurers) Act

At least **11** country-level laws, state-specific regulations, industry-specific regulations

At least **5** country-level laws, industry-specific regulations

Penalties for non-compliance†

Unlimited fine and up to **10 years in prison**

Unlimited fine and up to **10 years in prison**

Insurance Policy (continued)

New Zealand

Insurance Law Reform Act 1985
 Fair Trading Act 1986
 Accident Insurance (Insurer Returns) Regulations 1999
 Accident Insurance (Interest on Crown Advances) Regulations 1999
 FRS-35: Financial Reporting of Insurance Activities
 FRS-34: Life Insurance Business
 Insurance Intermediaries Act 1994
 Insurance (Prudential Supervision) Act 2010
 Insurance (Prudential Supervision) Regulations 2010
 NZ IFRS 4: Insurance Contracts
 Securities Act

At least **10** country-level laws and regulations, industry-specific regulations

Australia

Insurance Act 1973
 Corporations Act 2001
 Insurance Contracts Act 1984
 Insurance (Agents & Brokers) Act 1984
 Financial Services Reform Act 2001
 General Insurance Code of Practice (self-regulatory code)
 Regulations issued by:
 Australian Prudential Regulation Authority
 Australian Securities and Investment Commission

At least **5** country-level laws, industry-specific regulations

Penalties for non-compliance†

Unlimited fine

Unlimited fine and up to **10 years in prison**



B2B Contracts – Contractor Agreements etc.

USA

Federal Legislation and Regulations

Uniform Commercial Code

State specific contract regulations

State-specific regulations and conformance to the Uniform Commercial Code

UK (England, Wales)

Sale of Goods Act
Supply of Goods and Services Act
Contracts (Applicable Law) Act
Enterprise Act 2002

At least 3 country-level laws, industry-specific regulations

Penalties for non-compliance[†]

Unlimited fine

Unlimited fine and up to 2 years in prison

New Zealand

Fair Trading Act 1986
Sale of Goods Act 1908
Contracts (Privity) Act 1982
Illegal Contracts Act 1970
Construction Contracts Act 2002
Construction Contracts Regulations 2003
Public Bodies Contracts Act 1959

At least 5 country-level laws

Australia

Trade Practices Act 1974
Contracts Review Act
Competition and Consumer Act 2010
Corporations Act 2001

State specific legislation with a number of common law precedents

State-specific legislation with a number of common law precedents and compliant with federal law

Penalties for non-compliance[†]

Unlimited fine

Unlimited fine and up to 10 years in prison



B2C Contracts – Purchase agreements, quotes, sales documents

USA

Federal Legislation and Regulations

Wall Street Reform and Consumer Protection Act
Fair Debt Collection Practices Act
Fair Credit Reporting Act
Truth in Lending Act
Fair Credit Billing Act

State specific consumer protection regulations

At least **5** country-level laws, state-specific consumer protection regulations, industry-specific regulations

UK (England, Wales)

Unfair Contract Terms Act
Consumer Credit Act
Under the Trade Descriptions Act
Consumer Protection Act
Contracts (Applicable Law) Act
Unfair Terms in Consumer Contracts Regulations 1999,
Consumer Protection (Distance Selling) Regulations 2000
Electronic Commerce Regulations 2002
General Product Safety Regulations 2005

At least **8** country-level laws, industry-specific regulations

Penalties for non-compliance[†]

Unlimited fine

Unlimited fine and up to 2 years in prison

New Zealand

Consumer Guarantees Act
Sale of Goods Act 1908
Fair Trading Act
Credit Contracts and Consumer Finance Regulations 2004
Illegal Contracts Act 1970
Minors' Contracts Act 1969
Motor Vehicle Sales Act
Credit Contracts and Consumer Finance Act
Layby Sales Act
Financial Service Providers (Registration and Dispute Resolution) Act

At least **9** country-level laws, industry-specific regulations

Australia

Australian Consumer Law (ACL)
Underpinned by the Intergovernmental Agreement (IGA) for ACL
Competition and Consumer Act 2010

Country-wide consumer protection law

Penalties for non-compliance[†]

Unlimited fine

Unlimited fine and up to 2 years in prison

[†] Note that the indicated penalties are the maximum, and will vary with the severity of the offence, usually up to the amount that is sufficient to compensate for the harm caused by non-compliance. An organization may be liable to pay fines under multiple legislations.

Every single piece of communication is typically affected by at least 5 different laws, regulations, ordinances, common law, and industry-specific standards. Communication templates, or “gold standards”, are initially created by individuals and teams who are aware of the legal obligations that are associated with their release. When these “gold standards” become used organization-wide, and changes to them are necessary, users do not tend to get their modifications approved by the experts. The ad-hoc nature of amendments to the “gold standard” templates may result in legal non-compliance or obligations that the organization may not wish to make or cannot fulfil. Non-compliance, in most cases, is not caused by malicious intentions, but mere lack of awareness of the specific requirements that are imposed on the content that has been modified.



Organizations decide to implement Governance, Risk Management, and Compliance solutions not only to strengthen their defenses against the exposure to litigation, and penalties associated with non-compliance, but also to establish more robust business processes that can be more easily managed and controlled internally.



3 What is Governance, Risk Management, and Compliance (GRC)?

3.1 Definition of GRC

The definitions of these terms vary. However, the widely accepted definition has been provided by Gartner:

3.1.1 Governance

The process by which policy is set and decision making is executed.

3.1.2 Risk Management

The process for preventing an unacceptable level of uncertainty in business objectives with a balance of avoidance through reconsideration of objectives, mitigation through the application of controls, transfer through insurance and acceptance through governance mechanisms. It is also the process to ensure that important business processes and behaviors remain within the tolerances associated with policies and decisions set through the governance process.

3.1.3 Compliance

The process of adherence to policies and decisions. Policies can be derived from internal directives, procedures and requirements, or external laws, regulations, standards and agreements.

3.2 Role of GRC within Large Enterprises

With the growing requirements that organizations face in the fields of governance, risk management, and compliance, GRC software may sometimes be considered, or hoped to be, the plug-and-play solution that will satisfy all GRC needs of the organization. It is crucial, however, that the organization is fully aware of the environment it operates in, can identify the compliance requirements that are relevant to its operations, is able to determine which processes are responsible for good governance, which processes make it possible to manage and control the risk that every environment and all business activities carry, and how to achieve compliance with all relevant laws, regulations, and industry standards. Only then can a qualified decision be made as to: (a) whether GRC software can address the issues the organization encounters or internal process optimization is needed prior to implementing a software solution, and (b) how requirements can be gathered so that a GRC software solution that meets the requirements can be selected.

The primary goal of every deployment of GRC software should be to strengthen the organization's defenses against unwanted outcomes of business processes. As an example of the process, let us consider the issuance of an insurance policy with multiple endorsements. The desired outcome of this process is a policy document that accurately reflects the level of risk associated with the specific case, includes the latest terms and conditions, is issued to the parameters specified by the customer, and complies with all relevant laws and regulations. There are, however, multiple possible unwanted outcomes with different degrees of impact on the issuing organization. The policy may be issued with minor mistakes or omissions that are



discovered, and consequently must be corrected. The parameters of the policy may not reflect the risk associated with the endorsements that were issued, thus exposing the organization to greater degrees of financial risk. The endorsements that were issued may have not been approved by the relevant regulatory body, thus exposing the insurer to penalties and litigation. GRC software must strengthen the organization's defenses against these undesirable outcomes, and must make it possible to monitor the overall risk exposure by assuring auditability of all relevant processes.

Every organization is different and has specific GRC needs, and may wish to control and audit disparate processes with a single software solution. It is important that the selected GRC solution can satisfy the requirements set out by the compliance and auditing teams in their entirety. If no single GRC software is found to be able to meet those requirements, then the "best-of-breed" solutions targeted at their respective areas of expertise should be utilized. It is worth noting that some GRC solutions focus on passive monitoring and evaluation of the risks that are known to exist in the business; some are point solutions that reduce exposure in one area of the business; and some combine all aspects of GRC i.e. risk reduction, correct procedure enforcement, risk exposure evaluation, and provision of audit data. GRC software is nearly always required to integrate with existing solutions and data sources, and must be able to do so utilizing industry open standards of connectivity.



4 Organizational three lines of defense

The European Confederation of Institutes of Internal Auditing issued the benchmark regulatory guidance for organizational defense. The scheme is based on the three lines of defense that encompass all management activities. This includes the line of business processes, control mechanisms, and internal audit.

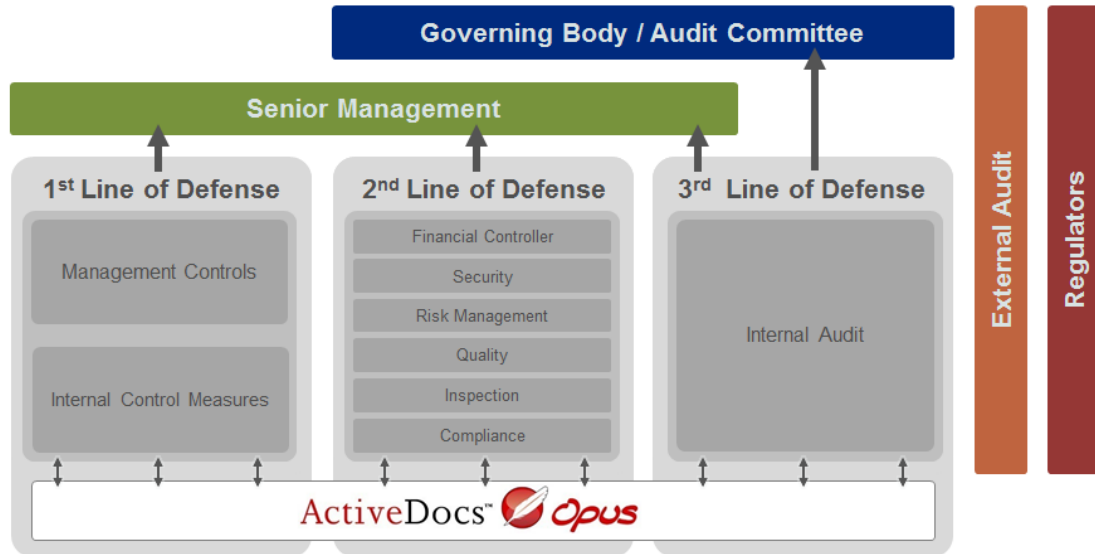


FIGURE 1: BENCHMARK MODEL FOR REGULATORY GUIDANCE (SOURCE: ECIIA, JUNE 2013)

4.1 1st Line of Defense

The 1st Line of Defense involves the mechanisms that touch on line-of-business processes. The business processes must be robust and controllable. The operational management takes ownership of the processes, is accountable for assessment, and proactively takes actions to mitigate risks associated with the activities for which they are responsible.

4.2 2nd Line of Defense

The 2nd Line of Defense in the organization assists the risk owners, and reports the relevant risk information both up and down the organization. Appropriate segregation of duties and access control is crucial. This line of defense monitors the implementation of risk management practices by operational management.

4.3 3rd Line of Defense

The 3rd Line of Defense provides assurance to the senior management and the governing body. It provides a representation of the state of the risk management framework implemented throughout the organization.

4.4 External Audit and Regulators

The external auditor contributes as an outside body, providing assurance regarding compliance with current legislation and regulations that are applicable to operations of the organization.



The detailed explanation of the Three Lines of Defense model can be downloaded from ECIIA website:

<http://eciia.eu/wp-content/uploads/2013/09/OCV-3.2-3LD-Model.pdf>



5 Governance, Risk Management, and Compliance with ActiveDocs

ActiveDocs can contribute to all three lines of defense across a range of processes in the organization. Its unique feature set makes it possible to address all three essential needs of GRC: (1) reduce the level of risk that is inherently associated with business activities, (2) enforce that the correct procedures are followed, and (3) evaluate overall risk exposure and provide auditing data.

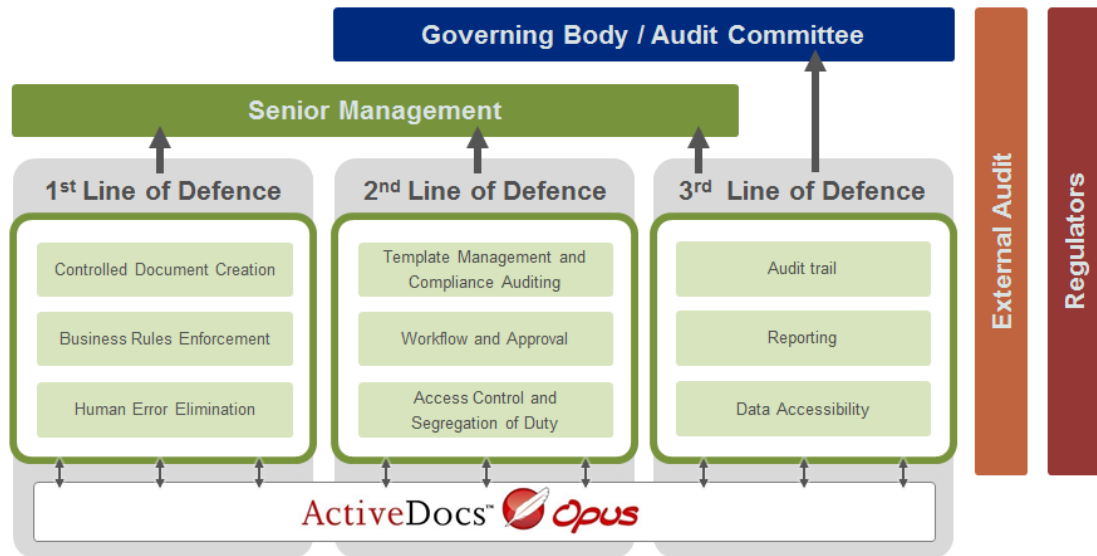


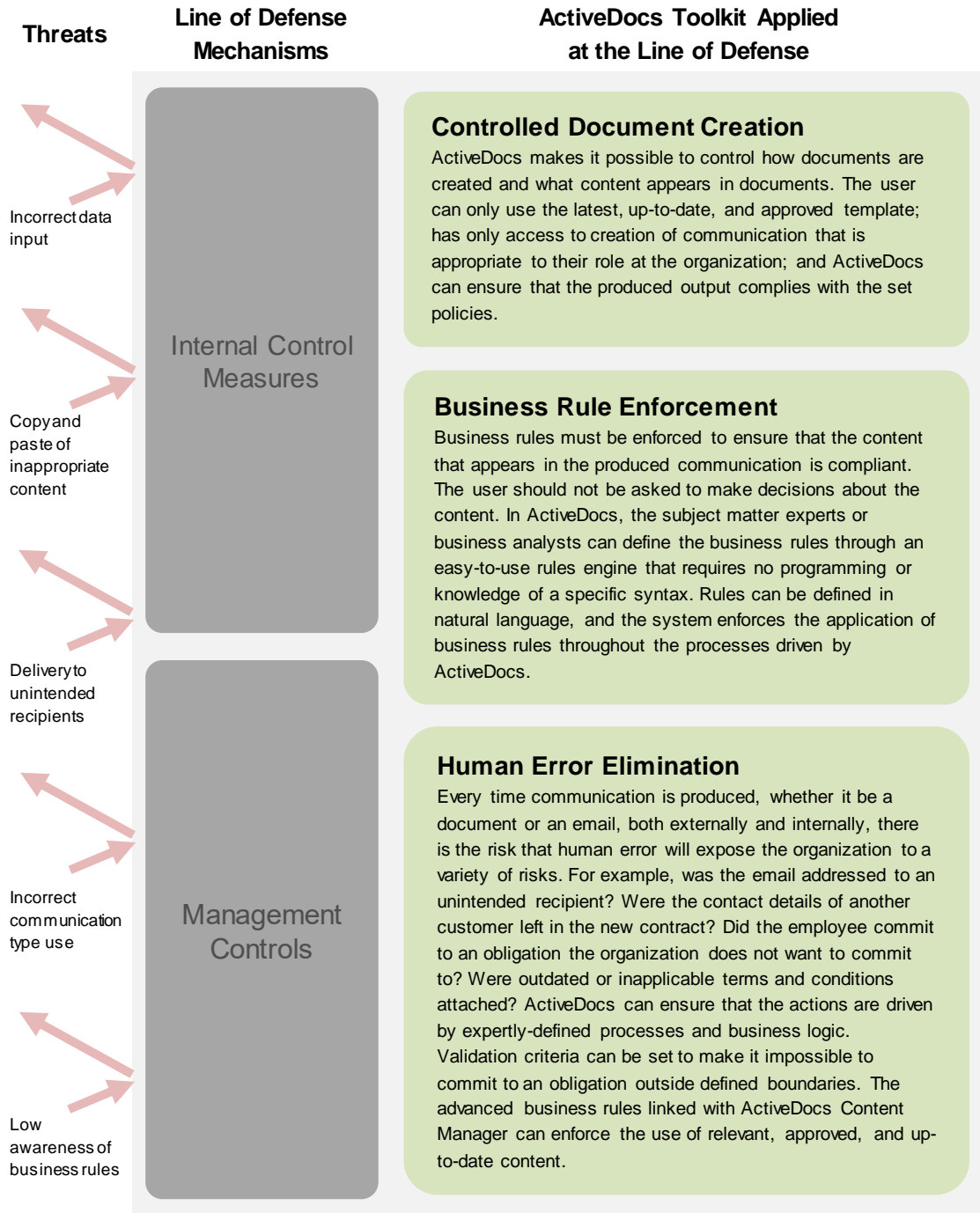
FIGURE 2: ACTIVEDOCS FUNCTIONALITY MAPPING ONTO ECIIA BENCHMARK MODEL FOR REGULATORY GUIDANCE

ActiveDocs' functional areas are mapped onto the three lines of defense of the ECIIA model. This can assure that the organization's defenses have been strengthened by the means of making the business processes more robust. Management is fully in control and can assure that the correct procedures are in place. The audit team is empowered by the ability to monitor the business in real-time, and have easy access to audit data.

The following diagrams illustrate how ActiveDocs can be used to strengthen each line of defense. The ability to address all three lines of defense is crucial to every successful enterprise-wide deployment of any GRC solution. ActiveDocs' unparalleled capabilities across all lines of defense make it an essential tool in organizations' overall GRC strategy.

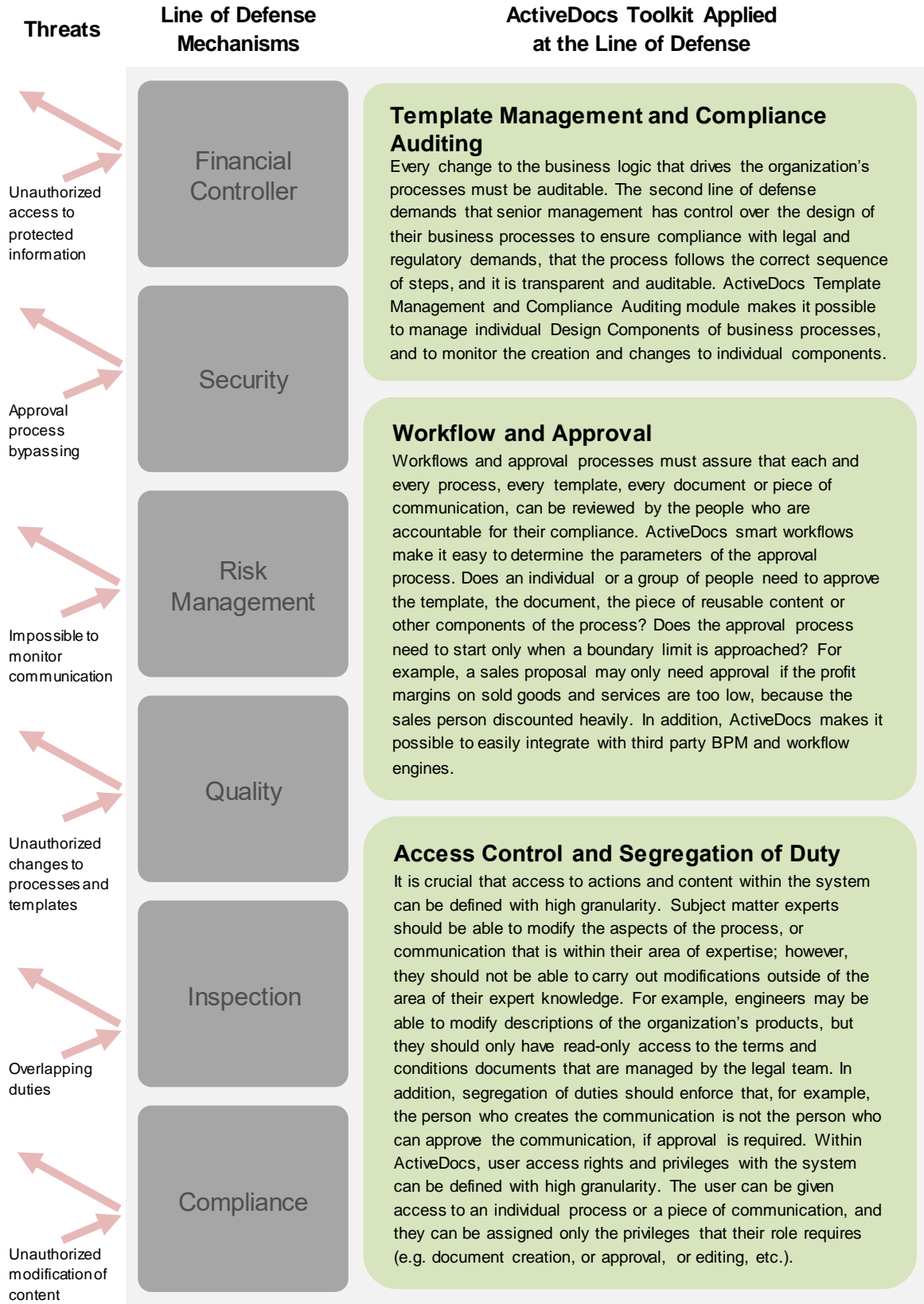


1st Line of Defense



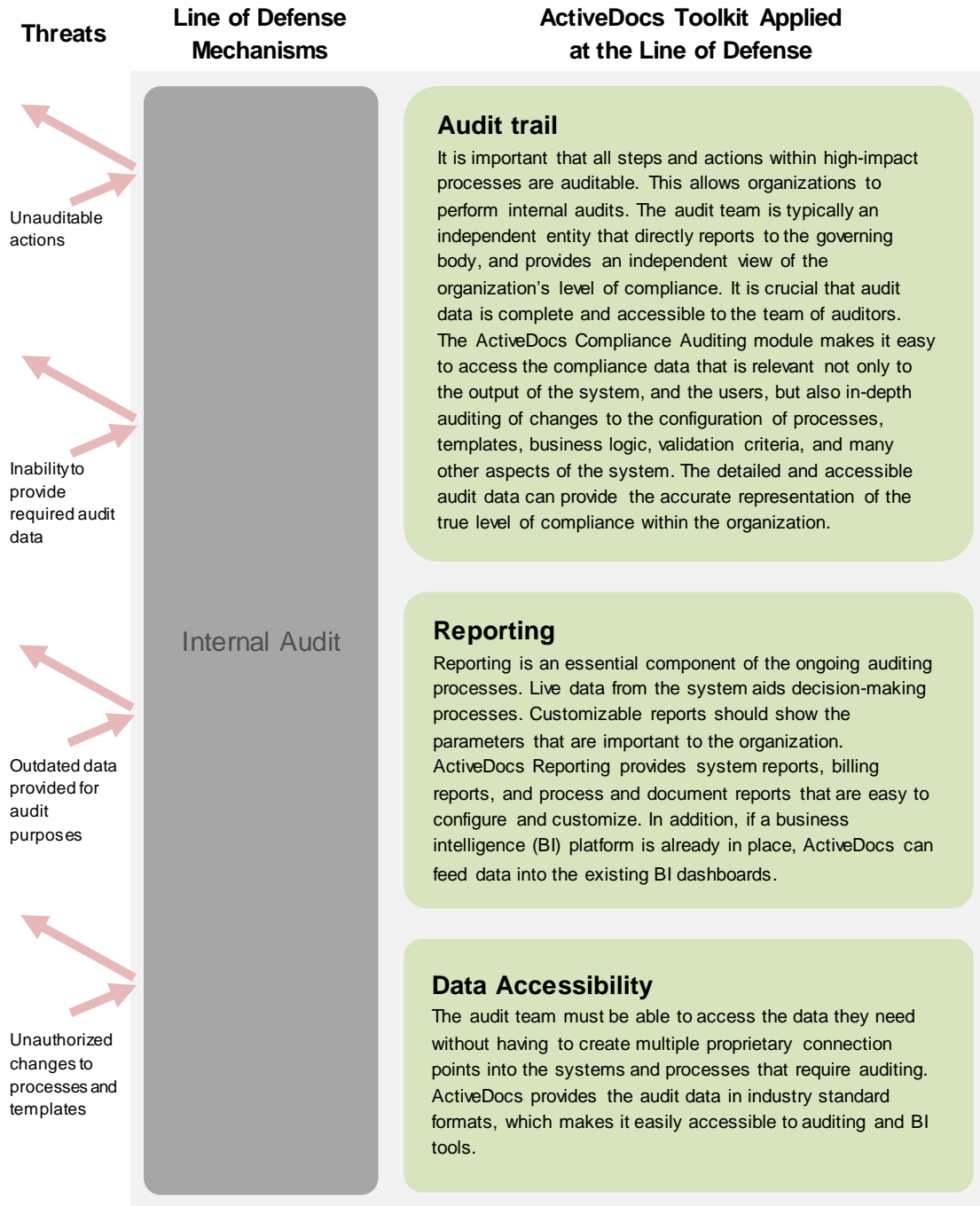


2nd Line of Defense





3rd Line of Defense






6 How ActiveDocs customers solved their GRC issues

Several specific examples of how some ActiveDocs customers solved their GRC issues are presented in tables below. Case studies are available, and can provide more detailed descriptions of the solutions.

6.1 Royal Dutch Shell – GRC in global HR

 Shell	1 st Line of Defense	2 nd Line of Defense	3 rd Line of Defense
Line of defense issue	Manual creation of HR documents, business rules implemented as written instructions.	Proliferation of hundreds of templates, users able to use outdated templates. Every document manually reviewed after creation, time consuming, not all errors can be caught.	Difficult to audit templates and instructions due to proliferation of multiple versions of templates with no central repository.
ActiveDocs solution	Single button document creation where the content is determined by business rules, and the data is supplied automatically from the central ERP SAP system.	Templates undergo rigorous approval processes. Central template and content repository. Individual document parameters checked at the time of document creation. Workflows driving post-creation approval processes where required.	Easy access to audit data from a single central location.

For detailed description of ActiveDocs solution at Shell, please refer to:
Royal Dutch Shell Case Study (https://www.activedocs.com/case_studies/shell.html)




6.2 Ricoh – GRC in Sales

RICOH	1st Line of Defense	2nd Line of Defense	3rd Line of Defense
Line of defense issue	Sales proposals containing inaccurate pricing information and product descriptions.	Difficult to review and change proposal templates. No controlled workflow processes.	No centralized access to proposal data, no auditable link between sales data and the information in proposals.
ActiveDocs solution	Automated creation of sales proposals utilizes live pricing and product description data.	Smart workflows determine which proposals need to be approved and by whom.	Central access to data on issued sales proposals with the ability to establish an auditable link with the actual sales.

For detailed description of ActiveDocs solution at RICOH, please refer to: *RICOH Case Study* (https://www.activedocs.com/case_studies/ricoh.html)




Bayer – GRC in pharmaceutical industry

	1 st Line of Defense	2 nd Line of Defense	3 rd Line of Defense
Line of defense issue	Manual creation of sensitive multi-legislation contracts was a manual process.	Legal teams have had to be involved throughout the process of contract creation to assure compliance with multiple legislation and regulation environments.	Audit of contract parameters based on manually populated metadata and may have required inspection of individual documents to obtain additional information.
ActiveDocs solution	Creation of documents driven by business rules automatically includes correct wording for the given case and legal environments.	Smart approval workflow processes where ActiveDocs integrates with Bayer’s SharePoint platform and Nintex workflows.	Metadata populated automatically, ensuring accuracy. ActiveDocs reporting makes it possible to access document parameters easily in industry-standard formats and via ActiveDocs Reports.

For detailed description of ActiveDocs solution at Bayer, please refer to: *Bayer Pharmaceuticals Case Study* (https://www.activedocs.com/case_studies/bayer.html)



6.3 ABB – GRC in Contract Management

	1 st Line of Defense	2 nd Line of Defense	3 rd Line of Defense
Line of defense issue	Contract content manually copied and pasted from a variety of disparate data sources could cause inaccuracies in the produced contractual documents.	Low transparency of the contract creation process, inaccurate or missing metadata, difficult to review produced contracts, manual filing into contract management software Selectica.	Difficult to perform contract audit, no easy access to data about contract content or the origin of data in the documents.
ActiveDocs solution	ActiveDocs assembles contracts automatically, based on standardized business rules, and utilizes the latest, approved, content.	Easy to control contract creation where templates, reusable content, and business rules can be approved prior to being used for contract creation. The contract approval process can be simplified, and the contracts are automatically filed into Selectica, which is used for contract management.	Easy access to data that was used to generate the contract documents.

For detailed description of ActiveDocs solution at ABB, please refer to: *ABB Case Study* (https://www.activedocs.com/case_studies/abb.html)



7 Conclusions

Governance, Risk Management, and Compliance demands have been increasing, and the demands on compliance and audit teams within organizations world-wide have been growing. The Three Lines of Defense framework can be adopted to strengthen an organization's ability to cope with legislation and regulatory pressures.

ActiveDocs is a tool that can provide unparalleled levels of support to all three lines of defense. It can be used to make any organization's line-of-business processes more robust, to put control mechanisms in place that enforce the correct procedures, and to enable and simplify internal audit practices.