
E-PHIS
CONSULTING
...being empowered
E-PHIS CONSULTING
TECH WEBINAR SERIES:
2023 August Edition
ACHIEVING
GOVERNANCE
RISK & COMPLIANCE:
Based on ISO 27001: 2022 Standard.

E-PHIS CONSULTING

Achieving Governance, Risk, and Compliance, guided by the ISO 27001:2022 Standard.

29TH AUG. 2023

Learning Objectives

- ❑ **Understand Governance, Risk, and Compliance (GRC), Needs and Benefits.**
- ❑ **Understand ISO/IEC 27001 and it's Benefits.**
- ❑ **Understand how to achieve GRC through ISO 27001 Implementation**
  - **Governance**
    - **The Organization, Entity & Stakeholders**
  - **Risk Management**
    - **Risk Assessment**
    - **Statement of Applicability (SOA)**
  - **Compliance**
    - **Audit**
    - **Continuous Improvement**

E-PHIS CONSULTING
...being empowered

E-PHIS CONSULTING TECH WEBINAR SERIES:
2023 August Edition

Joseph Benedict
Information and Cybersecurity Expert

Meet Joseph Benedict

Joseph Benedict is a seasoned Cybersecurity and Information Technology (IT) expert with over 13 years of experience in IT Audit and Compliance. He has a proven track record in establishing and implementing Information Technology and Security projects across multiple domains.

He holds a Master of Science in Information Security and Digital Forensic from the University of East London and a Master of Education in Educational Evaluation and Research from Olabisi Onabanjo University. He also has a Bachelor's degree in Information Communication and Technology from the Institut Superieur de Communication et de Gestion.

His skills include Enterprise Architecture, Cyber and Information Security, Information Security Audit, Data and Endpoint Protection, IT Risk Management, Assessment and Treatment, Cybersecurity Intelligence, NIST-CSF, Vulnerability and Threat Management, Enterprise Network Architecture, ISMS – ISO 27001 Audit and Implementation, Training and Mentorship, Data Center and Infrastructure Design and Management, Change Management, Project Management, Business Continuity & Disaster Recovery, and Incident Response Management.

A member of several professional associations, including the Association of Enterprise Architecture, Information Systems Audit and Control Association (ISACA), Institute of Strategic Manager Nigeria (ISMN), and Project Management Institute (PMI). He has also volunteered his expertise in Cybersecurity Exam Development and as a mentor with ISACA.

Joseph's impressive track record, commitment to excellence, and dedication to making a positive impact make him an outstanding candidate for the 100 Best Youth from the Continent award.

Virtual
via Microsoft Teams

ACHIEVING GOVERNANCE RISK & COMPLIANCE:

Based on ISO 27001: 2022 Standard.

29TH
AUG. 2023
12NOON
(LAGOS, NIGERIA TIME)

Register Via
https://bit.ly/3rU8ZJV

Learning Objectives

- ❑ **Understand Governance, Risk, and Compliance (GRC), Needs and Benefits.**
- ❑ **Understand ISO/IEC 27001 and it's Benefits.**
- ❑ **Understand how to achieve GRC through ISO 27001 Implementation**
  - **Governance**
    - **The Organization, Entity & Stakeholders**
  - **Risk Management**
    - **Risk Assessment**
    - **Statement of Applicability (SOA)**
  - **Compliance**
    - **Audit**
    - **Continuous Improvement**

E-PHIS CONSULTING

What is Governance, Risk, and Compliance?

Governance, Risk, and Compliance (GRC) is a structured way to align IT with business goals while managing risks and meeting all industry and government regulations. It includes tools and processes to unify an organization's governance and risk management with its technological innovation and adoption.

Companies use GRC to provide assurance that organizational goals are reliably achieved, uncertainty remove and meet compliance requirements are meet.

E-PHIS CONSULTING

What is Governance, Risk, and Compliance?

PROVIDE ASSURANCE

GOVERNANCE

PRINCIPLE PERFORMANCE is to **RELIABLY ACHIEVE OBJECTIVES ADDRESS UNCERTAINTY** and **ACT WITH INTEGRITY.**

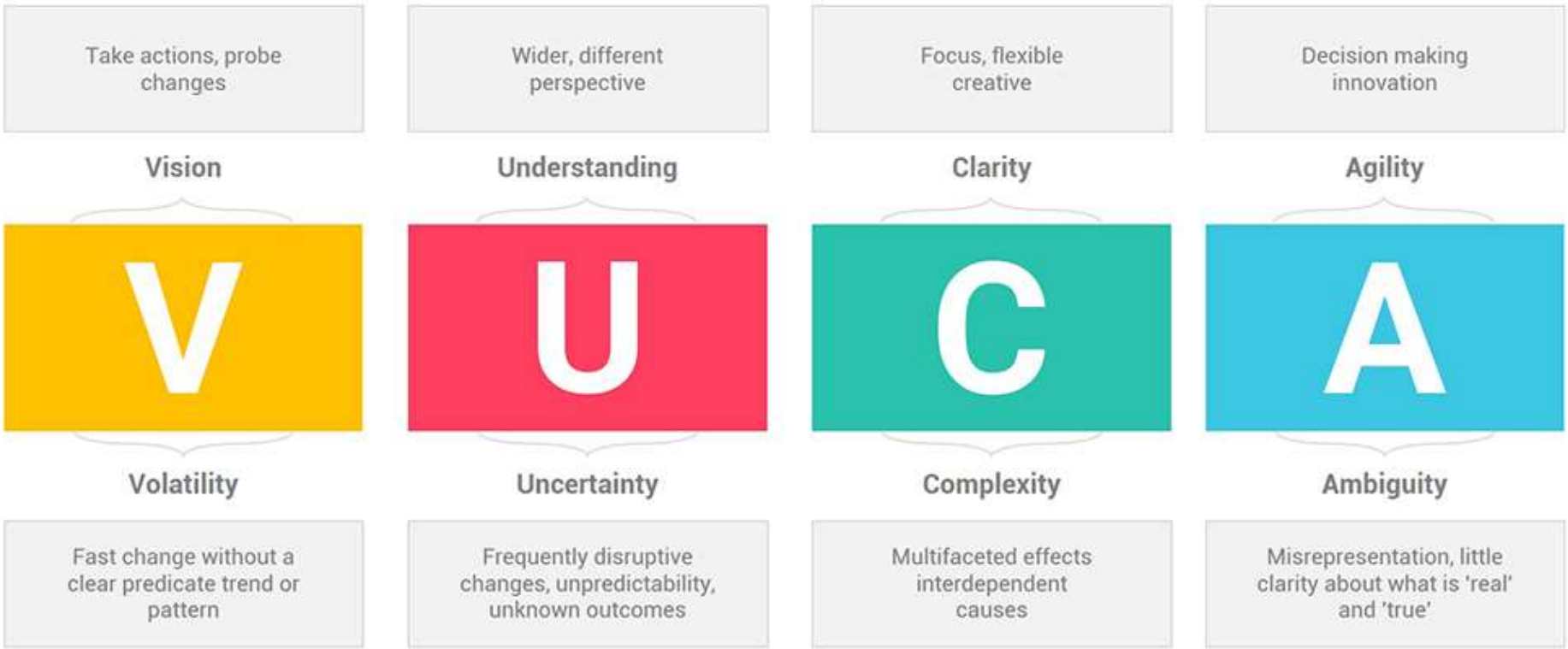
RISK

COMPLIANCE

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Why do we NEED GRC...



Benefits of Governance, Risk, and Compliance

Stability: resolution to immediate and long-term risk exposure while allowing for an agile and scalable control environment.

Optimization: Non-value adding activities are eliminated and value-adding activities are streamlined to reduce time and any undesirable variations.

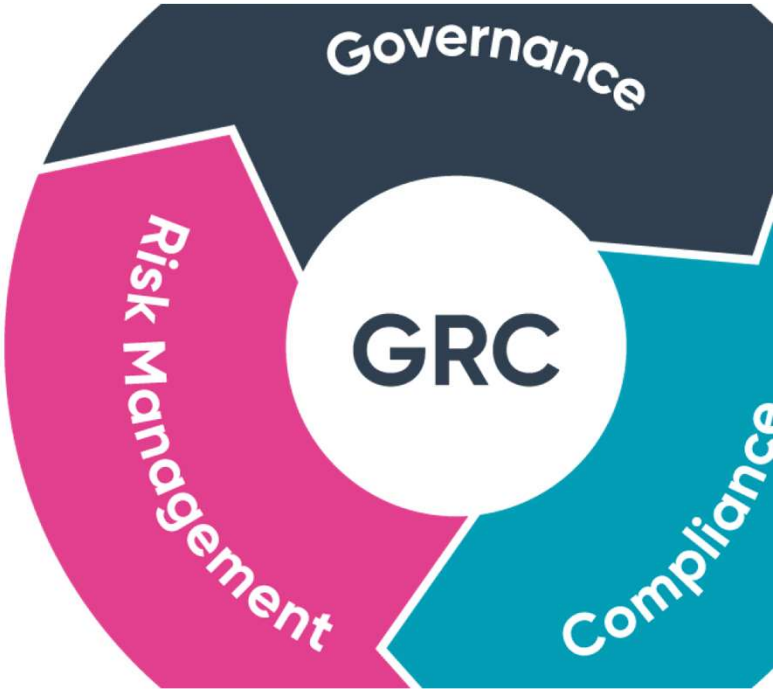
Transparency: ability to view a more complete picture of the organization and processes, allowing owners to have access and control over necessary content to understand the business unit profile and applicable risks and challenges.

Benefits of Governance, Risk, and Compliance

Reduced Costs: Lower costs contribute to the overall ROI gains represented by effective GRC activities. There is also reduced costs in maintaining duplicated controls, tests, issues, actions, and reporting across multiple disciplines.

Consistency: Improved alignment of objectives with mission, vision, and value of the organization, resulting in better decision-making agility and confidence.

…. Pls ADD yours….



What is ISO/IEC 27001?

E-PHIS CONSULTING

ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS). It defines requirements an ISMS must meet.

The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.

Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard.

Benefits of ISO/IEC 27001

Implementing the information security framework specified in the ISO/IEC 27001 standard helps you:

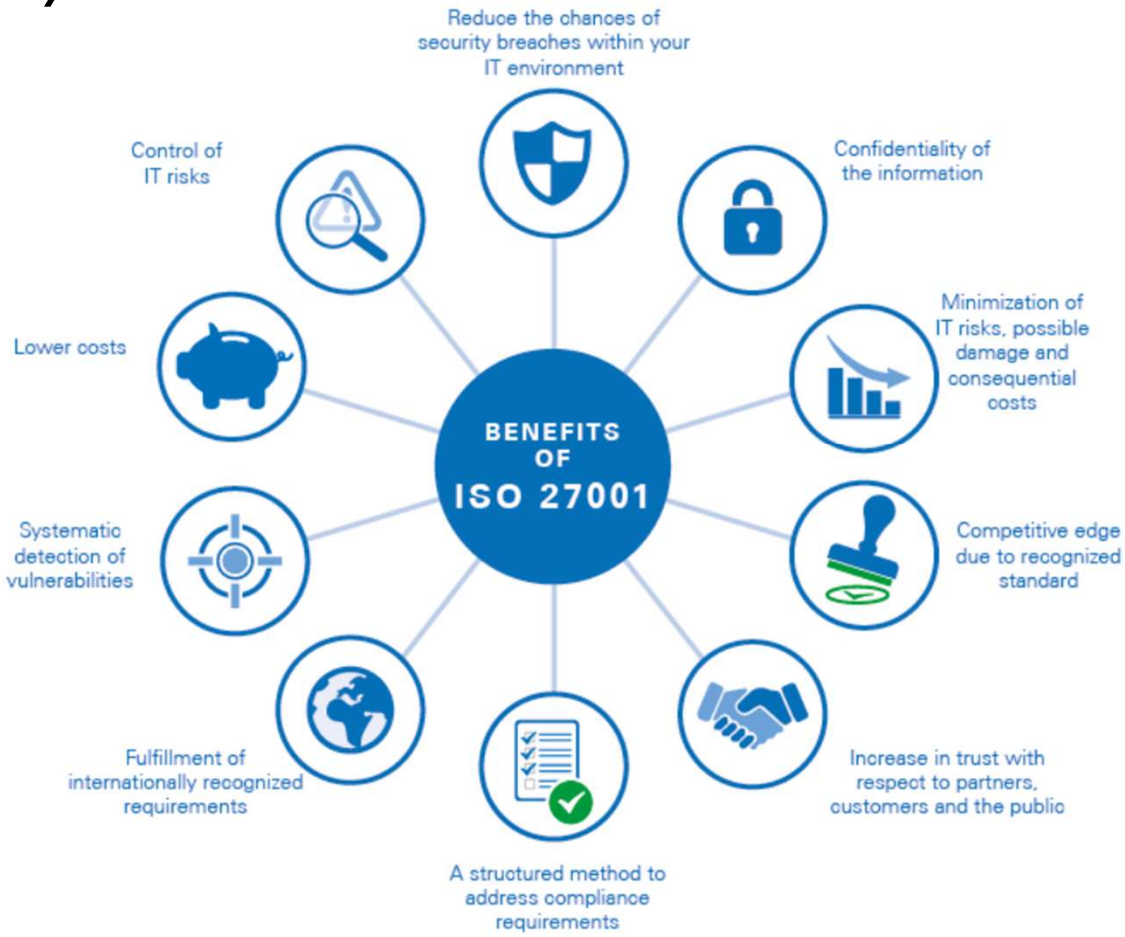
- ✓ Reduce your vulnerability to the growing threat of cyber-attacks Respond to evolving security risks.
- ✓ Ensure that assets such as financial statements, intellectual property, employee data and information entrusted by third parties remain undamaged, confidential, and available as needed.
- ✓ Provide a centrally managed framework that secures all information in one place

Benefits of ISO/IEC 27001

E-PHIS CONSULTING

Implementing the information security framework specified in the ISO/IEC 27001 standard helps you:

- ✓ Prepare people, processes and technology throughout your organization to face technology-based risks and other threats.
- ✓ Secure information in all forms, including paper-based, cloud-based and digital data.
- ✓ Save money by increasing efficiency and reducing expenses for ineffective defense technology.



ISO 27001 consists of **TWO** parts –The main part of the standard and the Annex A

The main part of the standard is comprised of 11clauses, however the clauses 0-3 are clauses that describe the standard itself so they are not important for the implementation, while the clauses from 4-10 set the requirements for information security, the requirement which your company must fulfill if you want to be compliant with the standard.

E-PHIS CONSULTING

ISO27001 CLAUSE

Introduction
1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

ANNEX A SECTIONS:

Annex A (normative) Information security controls reference

A.5. Organizational controls - 37
A.6. People Controls - 8
A.7. Physical Controls - 14
A.8. Technology Controls - 34

E-PHIS CONSULTING

ASSURANCE = Governance, Risk, and Compliance

Governance

4. Context of the organization
5. Leadership
7. Support

Risk

6. Planning
8. Operation

Compliance

9. Performance evaluation
10. Improvement

Annex A (normative) Information security controls reference

5. Organizational controls - 37
6. People Controls - 8
7. Physical Controls - 14
8. Technology Controls - 34

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Governance:
RELIABLY ACHIEVE OBJECTIVES

4 Context of the organization

4.1 Understanding the organization and its context
4.2 Understanding the needs and expectations of interested parties
4.3 Determining the scope of the information security management system
4.4 Information security management system

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Governance:
RELIABLY ACHIEVE OBJECTIVES

5 Leadership

5.1 Leadership and commitment
5.2 Policy
5.3 Organizational roles, responsibilities and authorities

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Governance:
RELIABLY ACHIEVE OBJECTIVES

7 Support

7.1 Resources
7.2 Competence
7.3 Awareness
7.4 Communication
7.5 Documented information
7.5.1 General
7.5.2 Creating and updating
7.5.3 Control of documented information

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Risk:
ADDRESS UNCERTAINTY

6 Planning

6.1 Actions to address risks and opportunities
6.1.1 General
6.1.2 Information security risk assessment
6.1.3 Information security risk treatment

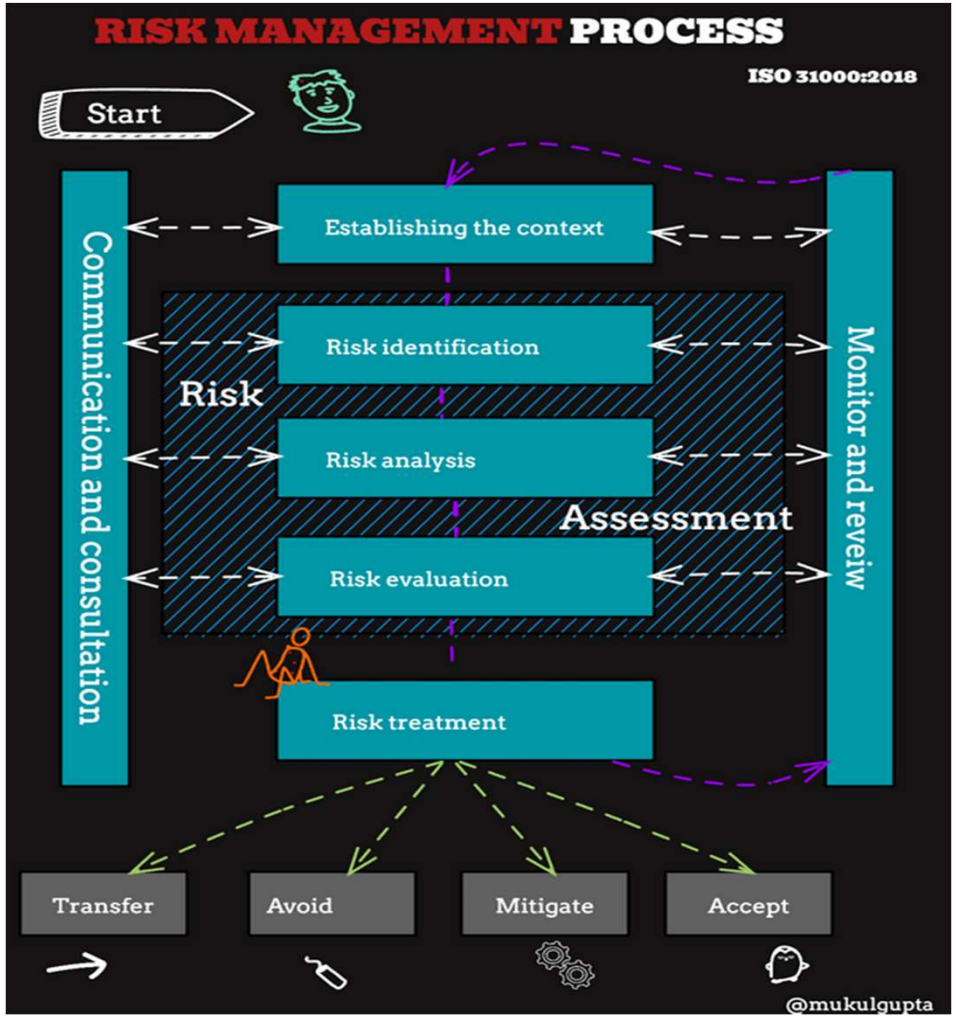
6.2 Information security objectives and planning to achieve them

6.3 Planning of changes

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Risk:
ADDRESS UNCERTAINTY



INFORMATION SECURITY RISK ASSESSMENT – RISK IDENTIFICATION [CLAUSE 6.1.2]

Asset	Risk Owner	Threat	Vulnerability	Impact (1-5)	Likelihood (1-5)	Risk (=I+L)
Server	Administrator	Electricity outage	No UPS			
		Fire	No fire extinguisher			
Contract	Managing director	Access by unauthorized persons	The contract is left on a table			
		Fire	No fire protection			
System administrator	Department head	Accident	No one else knows the passwords			

INFORMATION SECURITY RISK ASSESSMENT – RISK ANALYSIS AND EVALUATION [CLAUSE 6.1.2]

Asset	Risk Owner	Threat	Vulnerability	Impact (1-5)	Likelihood (1-5)	Risk (=I+L)
Server	Administrator	Electricity outage	No UPS	4	2	6
		Fire	No fire extinguisher	5	3	8
Contract	Managing director	Access by unauthorized persons	The contract is left on a table	4	4	8
		Fire	No fire protection	4	3	7
System administrator	Department head	Accident	No one else knows the passwords	5	3	8

STATEMENT OF APPLICABILITY [CLAUSE 6.1.3]

ISO 27001:2013 Controls			Applicability (YES/NO)	Justification for selection/non-selection	Implementation method	Status
Clause	**No.**	**Control Objective/Control**				
Asset Management	8.2	Information classification				
	8.2.1	Classification of information	Yes	Risks #45, 89 and 125; Agreement with company XYZ.	Documented in the Classification Policy	Implemen
	8.2.2	…				
	8.2.3	….				
Physical and Environmental Security	11.1	Secure Areas				
	11.1.5	Working in secure areas	No	Not applicable control because of the nature of our business. The company doesn't have or use secure areas. There is not even a server room, because cloud servers are used.	N/A	N/A
	11.1.6	….				

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Risk:
ADDRESS UNCERTAINTY

8 Operation

8.1 Operational planning and control
8.2 Information security risk assessment
8.3 Information security risk treatment

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Compliance:
ACT WITH INTEGRITY.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.2 Internal audit
9.2.1 General
9.2.2 Internal audit programme

9.3 Management review
9.3.1 General
9.3.2 Management review inputs
9.3.3 Management review results

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Compliance:
ACT WITH INTEGRITY.

10 Improvement

10.1 Continual improvement
10.2 Nonconformity and corrective action

QUESTIONS AND ANSWERS


E-PHIS
CONSULTING
...being empowered
E-PHIS CONSULTING
TECH WEBINAR SERIES:
2023 August Edition
ACHIEVING
GOVERNANCE
RISK & COMPLIANCE:
Based on ISO 27001: 2022 Standard.

E-PHIS CONSULTING

Achieving Governance, Risk, and Compliance, guided by the ISO 27001:2022 Standard.

29TH AUG. 2023

Learning Objectives

- ❑ **Understand Governance, Risk, and Compliance (GRC), Needs and Benefits.**
- ❑ **Understand ISO/IEC 27001 and it's Benefits.**
- ❑ **Understand how to achieve GRC through ISO 27001 Implementation**
  - **Governance**
    - **The Organization, Entity & Stakeholders**
  - **Risk Management**
    - **Risk Assessment**
    - **Statement of Applicability (SOA)**
  - **Compliance**
    - **Audit**
    - **Continuous Improvement**

E-PHIS CONSULTING
...being empowered

E-PHIS CONSULTING TECH WEBINAR SERIES:
2023 August Edition

Joseph Benedict
Information and Cybersecurity Expert

Meet Joseph Benedict

Joseph Benedict is a seasoned Cybersecurity and Information Technology (IT) expert with over 13 years of experience in IT Audit and Compliance. He has a proven track record in establishing and implementing Information Technology and Security projects across multiple domains.

He holds a Master of Science in Information Security and Digital Forensic from the University of East London and a Master of Education in Educational Evaluation and Research from Olabisi Onabanjo University. He also has a Bachelor's degree in Information Communication and Technology from the Institut Superieur de Communication et de Gestion.

His skills include Enterprise Architecture, Cyber and Information Security, Information Security Audit, Data and Endpoint Protection, IT Risk Management, Assessment and Treatment, Cybersecurity Intelligence, NIST-CSF, Vulnerability and Threat Management, Enterprise Network Architecture, ISMS – ISO 27001 Audit and Implementation, Training and Mentorship, Data Center and Infrastructure Design and Management, Change Management, Project Management, Business Continuity & Disaster Recovery, and Incident Response Management.

A member of several professional associations, including the Association of Enterprise Architecture, Information Systems Audit and Control Association (ISACA), Institute of Strategic Manager Nigeria (ISMN), and Project Management Institute (PMI). He has also volunteered his expertise in Cybersecurity Exam Development and as a mentor with ISACA.

Joseph's impressive track record, commitment to excellence, and dedication to making a positive impact make him an outstanding candidate for the 100 Best Youth from the Continent award.

Virtual
via Microsoft Teams

ACHIEVING GOVERNANCE RISK & COMPLIANCE:

Based on ISO 27001: 2022 Standard.

29TH
AUG. 2023
12NOON
(LAGOS, NIGERIA TIME)

Register Via
https://bit.ly/3rU8ZJV

Learning Objectives

- ❑ **Understand Governance, Risk, and Compliance (GRC), Needs and Benefits.**
- ❑ **Understand ISO/IEC 27001 and it's Benefits.**
- ❑ **Understand how to achieve GRC through ISO 27001 Implementation**
  - **Governance**
    - **The Organization, Entity & Stakeholders**
  - **Risk Management**
    - **Risk Assessment**
    - **Statement of Applicability (SOA)**
  - **Compliance**
    - **Audit**
    - **Continuous Improvement**

E-PHIS CONSULTING

What is Governance, Risk, and Compliance?

Governance, Risk, and Compliance (GRC) is a structured way to align IT with business goals while managing risks and meeting all industry and government regulations. It includes tools and processes to unify an organization's governance and risk management with its technological innovation and adoption.

Companies use GRC to provide assurance that organizational goals are reliably achieved, uncertainty remove and meet compliance requirements are meet.

E-PHIS CONSULTING

What is Governance, Risk, and Compliance?

PROVIDE ASSURANCE

GOVERNANCE

PRINCIPLE PERFORMANCE is to **RELIABLY ACHIEVE OBJECTIVES ADDRESS UNCERTAINTY** and **ACT WITH INTEGRITY.**

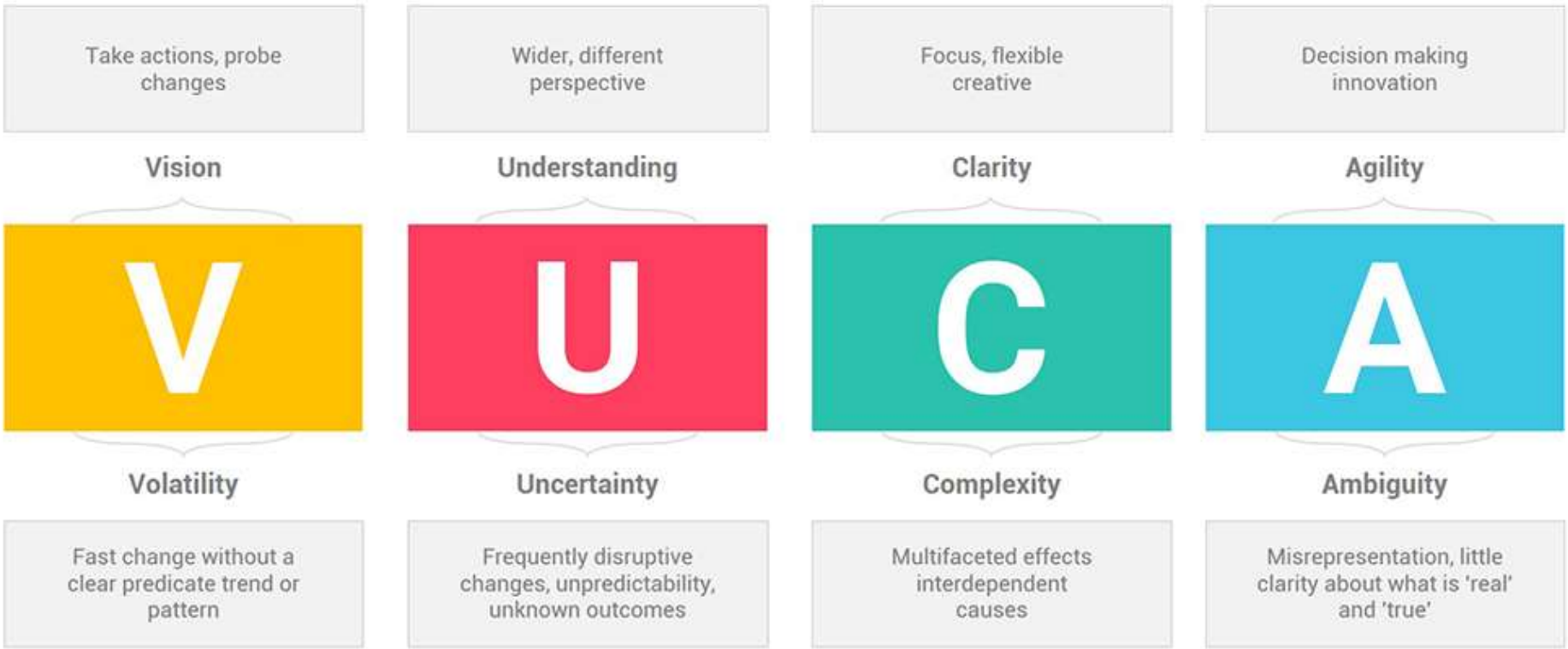
RISK

COMPLIANCE

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Why do we NEED GRC...



Benefits of Governance, Risk, and Compliance

Stability: resolution to immediate and long-term risk exposure while allowing for an agile and scalable control environment.

Optimization: Non-value adding activities are eliminated and value-adding activities are streamlined to reduce time and any undesirable variations.

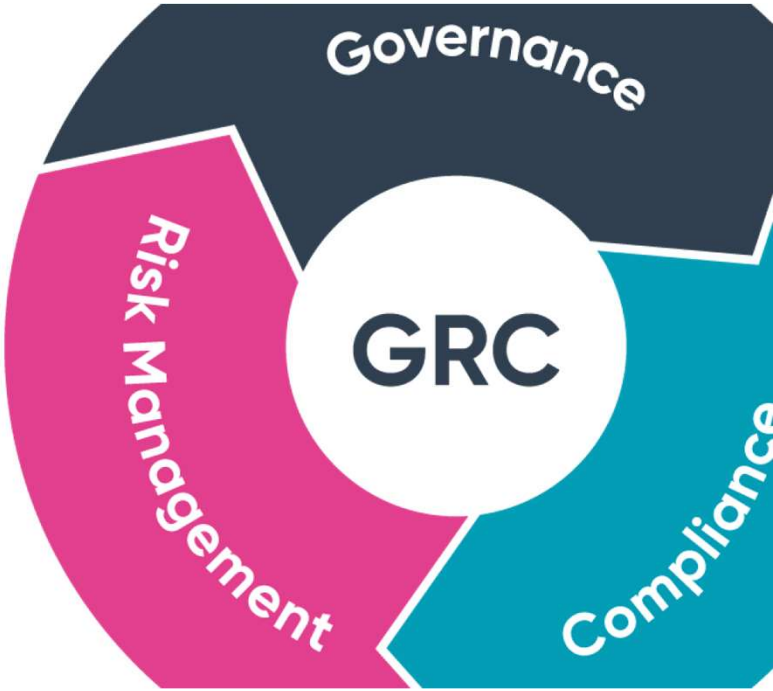
Transparency: ability to view a more complete picture of the organization and processes, allowing owners to have access and control over necessary content to understand the business unit profile and applicable risks and challenges.

Benefits of Governance, Risk, and Compliance

Reduced Costs: Lower costs contribute to the overall ROI gains represented by effective GRC activities. There is also reduced costs in maintaining duplicated controls, tests, issues, actions, and reporting across multiple disciplines.

Consistency: Improved alignment of objectives with mission, vision, and value of the organization, resulting in better decision-making agility and confidence.

…. Pls ADD yours….



What is ISO/IEC 27001?

E-PHIS CONSULTING

ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS). It defines requirements an ISMS must meet.

The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.

Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard.

Benefits of ISO/IEC 27001

Implementing the information security framework specified in the ISO/IEC 27001 standard helps you:

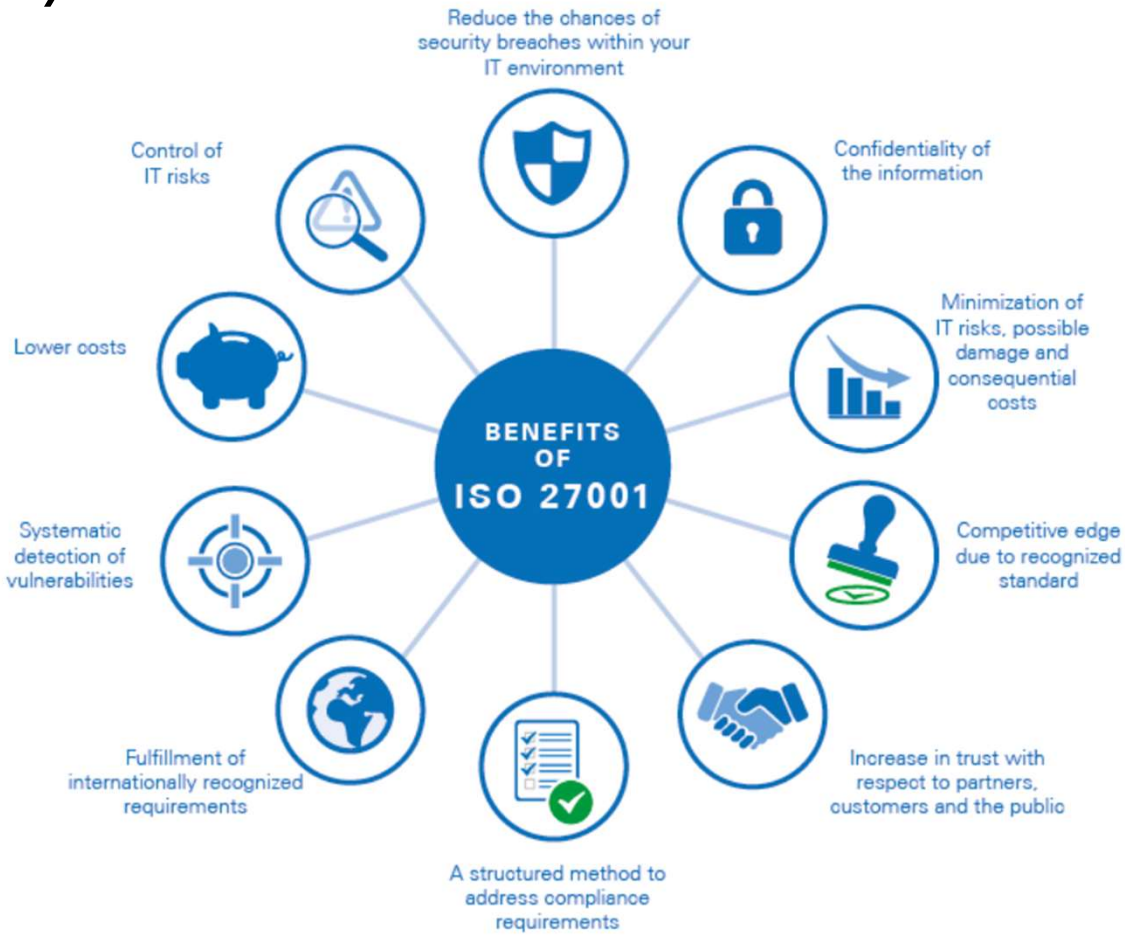
- ✓ Reduce your vulnerability to the growing threat of cyber-attacks Respond to evolving security risks.
- ✓ Ensure that assets such as financial statements, intellectual property, employee data and information entrusted by third parties remain undamaged, confidential, and available as needed.
- ✓ Provide a centrally managed framework that secures all information in one place

Benefits of ISO/IEC 27001

E-PHIS CONSULTING

Implementing the information security framework specified in the ISO/IEC 27001 standard helps you:

- ✓ Prepare people, processes and technology throughout your organization to face technology-based risks and other threats.
- ✓ Secure information in all forms, including paper-based, cloud-based and digital data.
- ✓ Save money by increasing efficiency and reducing expenses for ineffective defense technology.



ISO 27001 consists of **TWO** parts –The main part of the standard and the Annex A

The main part of the standard is comprised of 11clauses, however the clauses 0-3 are clauses that describe the standard itself so they are not important for the implementation, while the clauses from 4-10 set the requirements for information security, the requirement which your company must fulfill if you want to be compliant with the standard.

E-PHIS CONSULTING

ISO27001 CLAUSE

Introduction
1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

ANNEX A SECTIONS:

Annex A (normative) Information security controls reference

A.5. Organizational controls - 37
A.6. People Controls - 8
A.7. Physical Controls - 14
A.8. Technology Controls - 34

E-PHIS CONSULTING

ASSURANCE = Governance, Risk, and Compliance

Governance

4. Context of the organization
5. Leadership
7. Support

Risk

6. Planning
8. Operation

Compliance

9. Performance evaluation
10. Improvement

Annex A (normative) Information security controls reference

5. Organizational controls - 37
6. People Controls - 8
7. Physical Controls - 14
8. Technology Controls - 34

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Governance:
RELIABLY ACHIEVE OBJECTIVES

4 Context of the organization

4.1 Understanding the organization and its context
4.2 Understanding the needs and expectations of interested parties
4.3 Determining the scope of the information security management system
4.4 Information security management system

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Governance:
RELIABLY ACHIEVE OBJECTIVES

5 Leadership

5.1 Leadership and commitment
5.2 Policy
5.3 Organizational roles, responsibilities and authorities

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Governance:
RELIABLY ACHIEVE OBJECTIVES

7 Support

7.1 Resources
7.2 Competence
7.3 Awareness
7.4 Communication
7.5 Documented information
7.5.1 General
7.5.2 Creating and updating
7.5.3 Control of documented information

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Risk:
ADDRESS UNCERTAINTY

6 Planning

6.1 Actions to address risks and opportunities
6.1.1 General
6.1.2 Information security risk assessment
6.1.3 Information security risk treatment

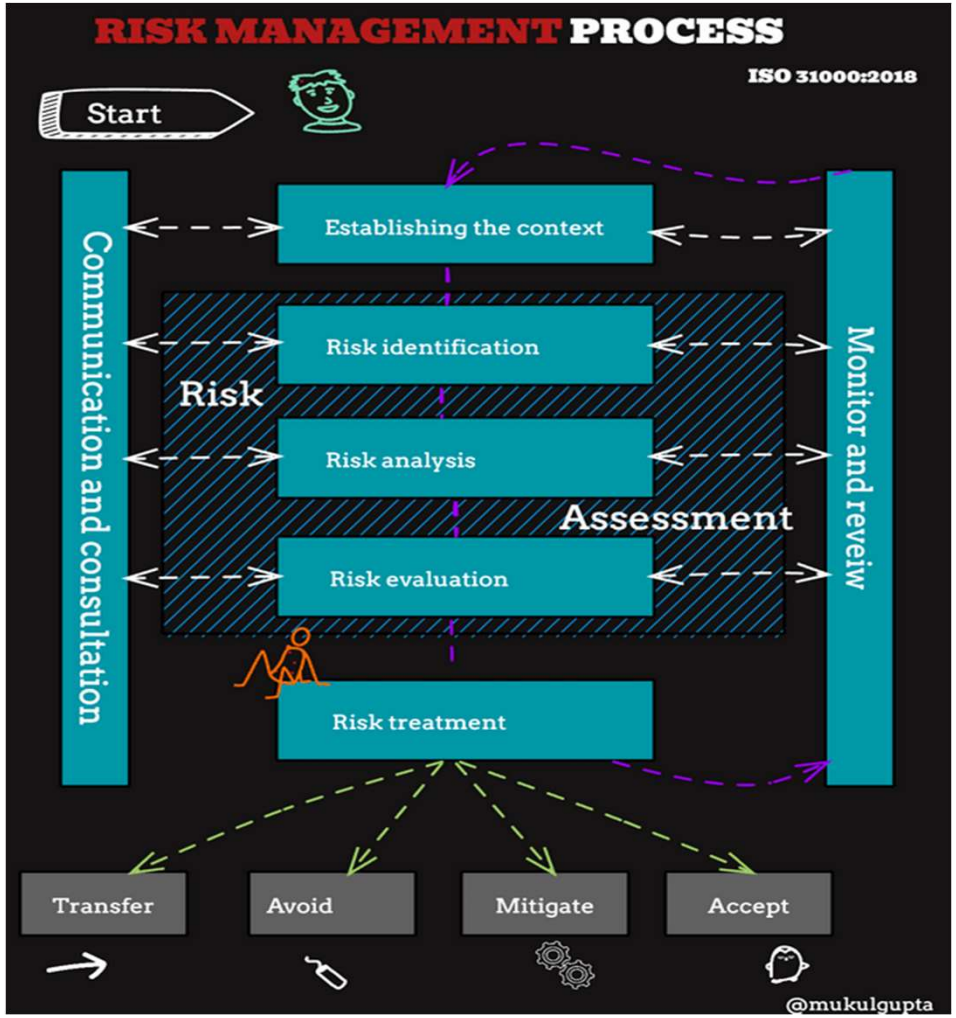
6.2 Information security objectives and planning to achieve them

6.3 Planning of changes

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Risk:
ADDRESS UNCERTAINTY



INFORMATION SECURITY RISK ASSESSMENT – RISK IDENTIFICATION [CLAUSE 6.1.2]

Asset	Risk Owner	Threat	Vulnerability	Impact (1-5)	Likelihood (1-5)	Risk (=I+L)
Server	Administrator	Electricity outage	No UPS			
		Fire	No fire extinguisher			
Contract	Managing director	Access by unauthorized persons	The contract is left on a table			
		Fire	No fire protection			
System administrator	Department head	Accident	No one else knows the passwords			

INFORMATION SECURITY RISK ASSESSMENT – RISK ANALYSIS AND EVALUATION [CLAUSE 6.1.2]

Asset	Risk Owner	Threat	Vulnerability	Impact (1-5)	Likelihood (1-5)	Risk (=I+L)
Server	Administrator	Electricity outage	No UPS	4	2	6
		Fire	No fire extinguisher	5	3	8
Contract	Managing director	Access by unauthorized persons	The contract is left on a table	4	4	8
		Fire	No fire protection	4	3	7
System administrator	Department head	Accident	No one else knows the passwords	5	3	8

STATEMENT OF APPLICABILITY [CLAUSE 6.1.3]

ISO 27001:2013 Controls			Applicability (YES/NO)	Justification for selection/non-selection	Implementation method	Status
Clause	**No.**	**Control Objective/Control**				
Asset Management	8.2	Information classification				
	8.2.1	Classification of information	Yes	Risks #45, 89 and 125; Agreement with company XYZ.	Documented in the Classification Policy	Implemen
	8.2.2	…				
	8.2.3	….				
Physical and Environmental Security	11.1	Secure Areas				
	11.1.5	Working in secure areas	No	Not applicable control because of the nature of our business. The company doesn't have or use secure areas. There is not even a server room, because cloud servers are used.	N/A	N/A
	11.1.6	….				

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Risk:
ADDRESS UNCERTAINTY

8 Operation

8.1 Operational planning and control
8.2 Information security risk assessment
8.3 Information security risk treatment

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Compliance:
ACT WITH INTEGRITY.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.2 Internal audit
9.2.1 General
9.2.2 Internal audit programme

9.3 Management review
9.3.1 General
9.3.2 Management review inputs
9.3.3 Management review results

ASSURANCE = Governance, Risk, and Compliance

E-PHIS CONSULTING

Compliance:
ACT WITH INTEGRITY.

10 Improvement

10.1 Continual improvement
10.2 Nonconformity and corrective action

QUESTIONS AND ANSWERS