



# SETTIMANA DELLA SOSTENIBILITÀ

25-28 MARZO 2025



**CONFINDUSTRIA  
VENETO EST**

Area Metropolitana  
Venezia Padova Rovigo Treviso

# Cybersecurity e sostenibilità

Giancarlo Butti  
25 Marzo 2025

# Giancarlo Butti

Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il **MIP Politecnico di Milano**. Referente Regolamento DORA (in precedenza ESG) e Inclusion del Comitato Scientifico del **CLUSIT**.

Si occupa di ICT, sicurezza, organizzazione e normativa dai primi anni 80.

**Auditor, security manager ed esperto di privacy**, affianca all'attività professionale quella di **divulgatore**, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni...

Oltre 170 corsi e seminari presso **ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNIVERSITA DI MILANO, CA FOSCARI, CEFRIEL, ABI**, master presso diversi atenei.

Ha all'attivo oltre **800** articoli e collaborazioni con oltre **40** testate.

Ha pubblicato **28 fra libri e white paper** alcuni dei quali utilizzati come testi universitari.

Ha partecipato alla redazione di **31 opere collettive** nell'ambito di **ABI LAB, Oracle/CLUSIT Community for Security, Rapporto CLUSIT**.

Socio e già proboviro di **AIEA** è socio del **CLUSIT**, di **DFA**, di **ACFE** e del **BCI**.

Partecipa a numerosi gruppi di lavoro.

Ha inoltre acquisito le certificazioni/qualificazioni (**LA BS 7799, LA ISO IEC 27001:2005/2013/2022, LA ISO 20000-1, LA ISO IEC 42001**), **CRISC, CDPSE, ISM, DPO, DPO UNI 11697:2017, DPO UNI CEI EN 17740:2024, CBCI, AMBCI**

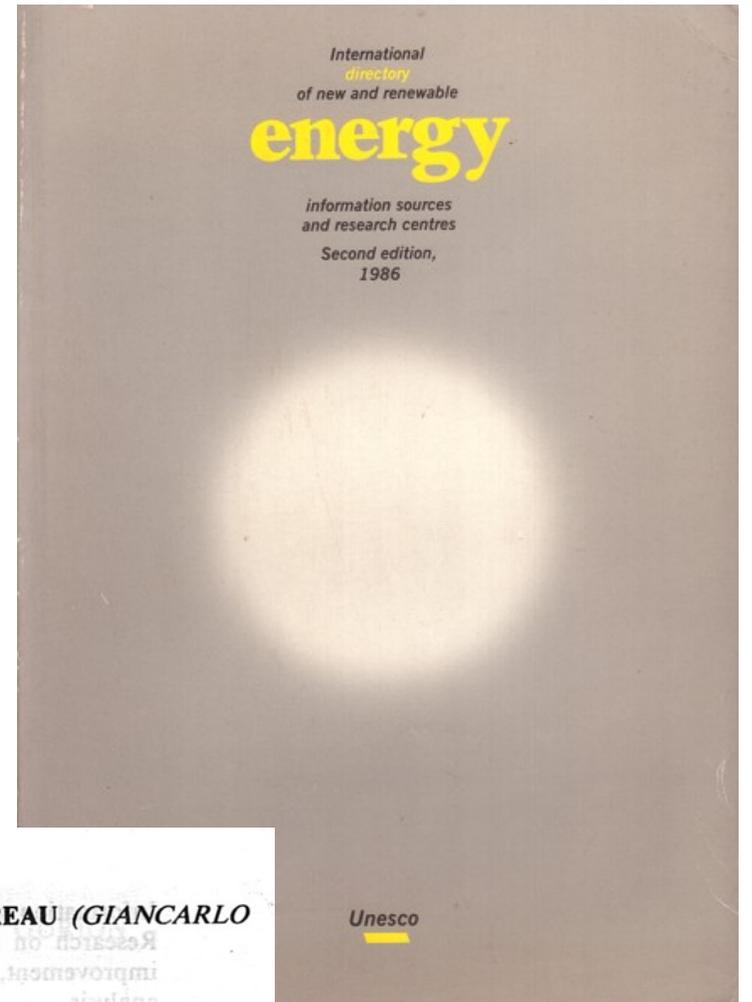
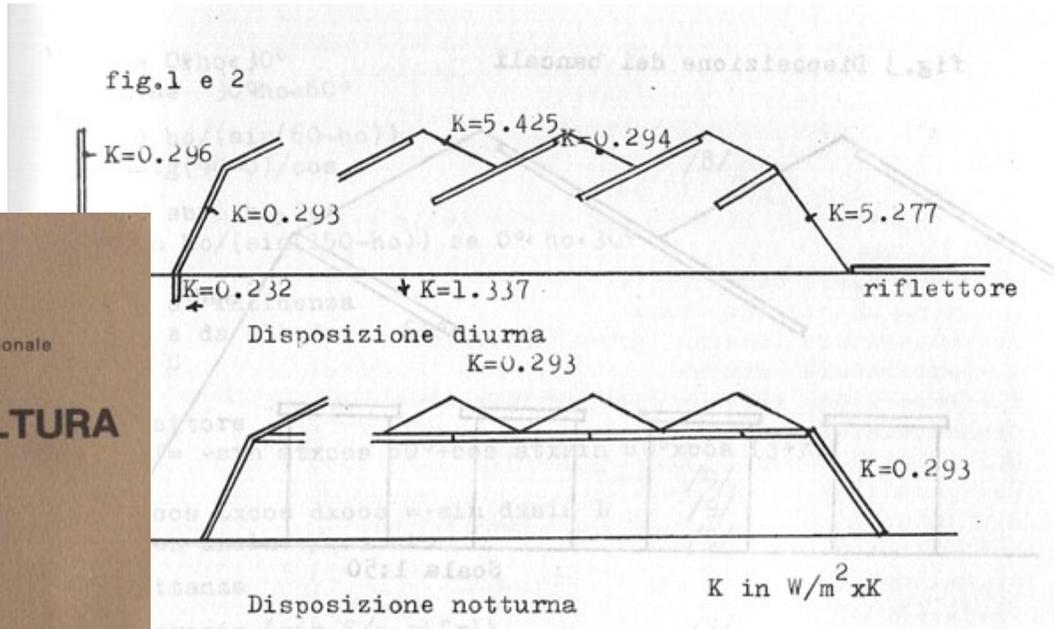
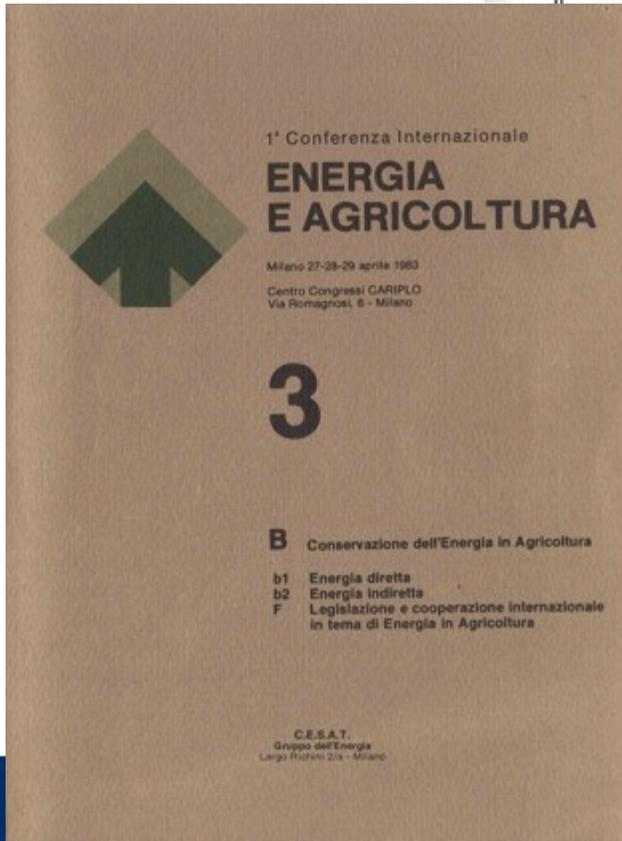


**SETTIMANA  
DELLA  
SOSTENIBILITÀ**  
25-28 MARZO 2025



**CONFINDUSTRIA  
VENETO EST**  
Area Metropolitana  
Venezia Padova Rovigo Treviso

# ESG Environmental, Social, Governance



## ITALY

**1502 GIANCARLO BUTTI PROFESSIONAL BUREAU (GIANCARLO BUTTI STUDIO PROFESSIONALE)**  
Via Mulini, 17  
Valmadrera  
I-22049 Como

# Cybersecurity e sostenibilità

## Recommendations for Solar Energy Cybersecurity

### CYBERSECURITY CONSIDERATIONS

- There is rapid and continued growth in grid-connected, large-scale solar inverter-based resources (IBR) and behind-the-meter distributed energy resources (DER).
- IBR/DER cybersecurity attacks may impact the energy critical infrastructure sector.
- Combined use of smart-grid technologies, mobile applications, and cloud-based control systems introduces several risks, including:
  - New cyber-attack vectors for the U.S. electric grid
  - Expanded attack surfaces
  - Malicious control of the IBR/DER cyber-physical system through the Internet
  - Logical or physical local ports could offer a foothold into networks (e.g., enterprise, operational, behind-the-meter)
  - Compromised Personally Identifiable Information (PII) or financial information resulting from compromised IBR/DER networks

### CYBERSECURITY IMPACTS

IBR/DER vendors, owners, operators, aggregators, grid operators, and government organizations must understand cyber threats targeting IBR/DER can create both localized and widespread impacts:

**Local Impacts**

- Failure of operations
- Damage to equipment
- Loss of IBR/DER service availability
- Theft of PII and financial information
- Compromise of IBR/DER safety systems

**Large-Scale Impacts**

- Harvesting of PII and financial information
- Shutdown of IBR/DER networks
- Exposure of upstream and partner IT networks to compromise
- Misconfiguration of IBR/DER grid-support functions leading to dangerous conditions
- Loss of consumer confidence in IBR/DER ecosystem
- Bulk power system reliability impact

### OBSERVED WEAKNESSES IN IBR/DER EQUIPMENT

#### Field Equipment Hardening

- Unencrypted storage allows attackers to steal credentials for use in accessing IBR/DER or partner systems, networks, and cloud services.
- Debugging or other unused ports are not removed or disabled prior to deployment
- Default or generic system accounts using default or generic passwords, enabling malicious activities and preventing accountability.
- Host-Based Intrusion Detection Systems (HIDS) not enabled, logs and alerts not shared upstream to Security Operations Center (SOC).
- Local logs not enabled or integrated with a Security Information and Event Management (SIEM) system.
- System administrators cannot revoke access to shared or local accounts when personnel leave the organization or no longer require access.

#### Network Protection & Monitoring

- IBR/DER networks do not always support encryption for data-at rest or data-in-transit.
- Network-Based Intrusion Detection Systems (NIDSs) are not installed at key network locations, e.g., IT/OT DMZs, cloud firewall, or DER gateway
- Enterprise systems or IBR/DER networks may not require or enforce proper network segmentation.
- Regular vulnerability scanning and patching of backend/cloud infrastructure is not performed by IBR/DER owners/operators.
- Firmware updates are sent in cleartext or do not include authentication mechanisms

**CONTACT:**  
 Jay Johnson | jjohns2@sandia.gov, Jon Hurtado | jghurta@sandia.gov,  
 Bheshaj Krishnappa | bkrishnappa@seia.org, Larry Collier | larry.collier@nerc.net,  
 Dan Goodlett | dan.goodlett@nerc.net

  
**NERC**  
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

  
**SEIA**  
Solar Energy Industries Association

  
**Sandia National Laboratories**

  
U.S. DEPARTMENT OF ENERGY

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003625.

## SANDIA REPORT

SAND2017-13262  
 Unlimited Release  
 Printed December 2017

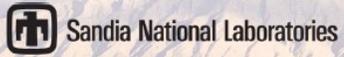
# Roadmap for Photovoltaic Cyber Security

Jay Johnson

Prepared by  
 Sandia National Laboratories  
 Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003625.

Approved for public release; further dissemination unlimited.



# Obiettivi di sostenibilità



## SOSTENIBILITÀ E CYBER SECURITY LA RICERCA

Ricerca sviluppata  
con il contributo  
non condizionante di



**SETTIMANA  
DELLA  
SOSTENIBILITÀ**

25-28 MARZO 2025

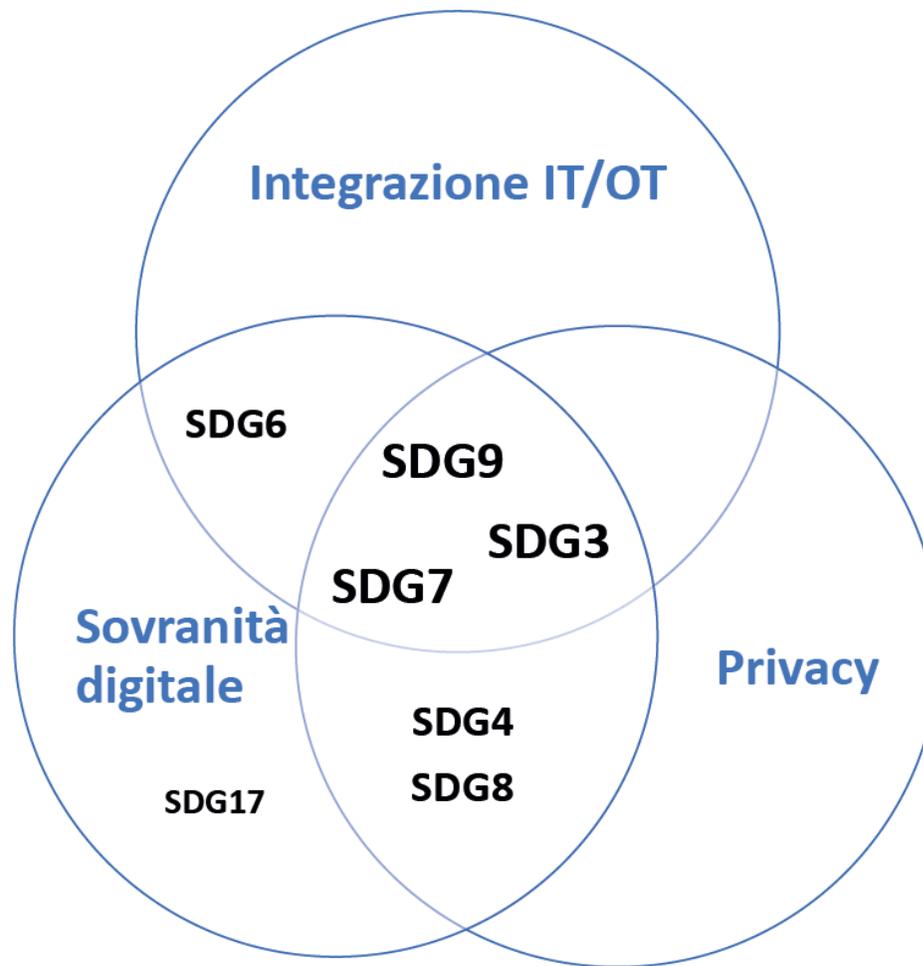


**CONFINDUSTRIA  
VENETO EST**

Area Metropolitana  
Venezia Padova Rovigo Treviso

# Sovrapposizioni

<b>SDG3</b> Salute e benessere	<b>SDG9</b> Imprese, innovazione, infrastrutture
<b>SDG4</b> Istruzione di qualità	<b>SDG10</b> Ridurre le disuguaglianze
<b>SDG6</b> Acqua pulita e servizi igienico-sanitari	<b>SDG13</b> Lotta contro il cambiamento climatico
<b>SDG7</b> Energia pulita e accessibile	<b>SDG17</b> Partnership per gli obiettivi
<b>SDG8</b> Lavoro dignitoso	



**Accessibilità dei sistemi**

**SDG10**

**Controllo dei consumi**

**SDG13**

	INTEGRAZIONE IT/OT	PRIVACY	SOVRANITÀ DIGITALE	CARATTERISTICHE
<b>SDG3</b> Salute e benessere	Gestione dei dispositivi medici presenti nelle strutture sanitarie	Protezione dati pazienti rispetto ad attacchi esterni e interni	Garanzia che i dati dei pazienti non possano essere acquisiti da Stati esteri	
<b>SDG4</b> Istruzione di qualità		<ul style="list-style-type: none"> <li>• Protezione dati studenti rispetto a attacchi esterni</li> <li>• Protezione dati degli studenti rispetto a gestori piattaforme</li> </ul>	Garanzia che i dati degli studenti non possano essere acquisiti da Stati esteri	
<b>SDG6</b> Acqua pulita e servizi igienico-sanitari	Gestione del flusso integrato delle acque		Garanzia che i dati delle infrastrutture idriche non possano essere acquisiti da Stati esteri	
<b>SDG7</b> Energia pulita e accessibile	<ul style="list-style-type: none"> <li>• Gestione delle reti smart grid nei loro diversi componenti (centrale, smart meter domestici...)</li> <li>• Gestione degli impianti di produzione</li> </ul>	Gestione dei sistemi di monitoraggio e controllo dei comportamenti degli utenti	Garanzia che i dati delle infrastrutture energetiche non possano essere acquisiti da Stati esteri	



# Environmental

- Gli attacchi informatici possono compromettere i sistemi di sicurezza e causare danni ambientali, come fuoriuscite di petrolio o sostanze chimiche, che hanno conseguenze gravi per l'ambiente e la salute pubblica.
- La sicurezza informatica è cruciale per proteggere le infrastrutture critiche, come quelle energetiche o idriche, dalle minacce informatiche che potrebbero avere ripercussioni ambientali.
- I processi di hardening dei sistemi informatici, che mirano a ridurre la superficie di attacco attraverso la configurazione sicura di componenti hardware e software, possono essere implementati con un'attenzione particolare all'efficienza energetica. Ciò include la disattivazione di servizi non necessari, l'ottimizzazione delle configurazioni e l'aggiornamento regolare dei sistemi per garantire sia la sicurezza che l'efficienza operativa.

# Environmental

- L'adozione di tecnologie virtualizzate e cloud può contribuire a migliorare sia la sicurezza che la sostenibilità, attraverso la condivisione di risorse e l'ottimizzazione dei carichi di lavoro.
- L'Analisi del Ciclo di Vita (LCA) rappresenta una metodologia rigorosa per valutare l'impatto ambientale di prodotti, servizi e sistemi lungo l'intero ciclo di vita, dalla estrazione delle materie prime fino allo smaltimento finale. Applicata nel contesto della cybersecurity, questa metodologia permette di analizzare l'impronta ecologica delle soluzioni di sicurezza informatica, considerando fattori come il consumo energetico, l'utilizzo di risorse, le emissioni di gas serra e la produzione di rifiuti elettronici. L'integrazione dell'LCA nella progettazione e implementazione delle strategie di cybersecurity consente di identificare opportunità di miglioramento e di ottimizzare il rapporto tra efficacia delle misure di sicurezza e impatto ambientale.

# Social

- La tutela dei dati personali e il rispetto della privacy rappresentano pilastri fondamentali di una condotta aziendale responsabile, in linea con la dimensione “Social” dei parametri ESG. In un contesto sempre più attento alla trasparenza, le imprese devono dimostrare chiaramente il loro impegno in materia di sicurezza informatica, ormai considerata parte integrante della responsabilità sociale. Non sono solo gli enti regolatori a richiedere maggiore chiarezza su questi aspetti, ma anche consumatori e investitori, interessati a valutare come le aziende gestiscono i pericoli digitali e tutelano i dati sensibili
- Per salvaguardare tale fiducia, la sicurezza informatica deve prevenire intrusioni e violazioni dei dati personali, proteggendo così la reputazione aziendale.

# Social

- L'attenzione crescente verso la riservatezza e l'integrità delle informazioni riflette il ruolo sempre più centrale che la cybersecurity ricopre nella valutazione della responsabilità sociale delle organizzazioni. Chi non adotta misure adeguate rischia non solo di incorrere in conseguenze legali ed economiche, ma anche di subire gravi ripercussioni reputazionali, minando la fiducia di clienti, dipendenti e partner.

# Governance

- La protezione dei sistemi digitali è profondamente intrecciata alla gestione aziendale, poiché richiede un solido meccanismo di supervisione per affrontare i rischi informatici e assicurare il rispetto delle normative in vigore.

# Esempio di impatto su un DATA CENTER di alcuni eventi climatici

(Security Summit 2023)

<b>Dispositivi IT</b>	<b>50%</b>
<b>UPS</b>	<b>11%</b>
<b>Illuminazione</b>	<b>3%</b>
<b>Cooling</b>	<b>36%</b>

<https://doi.org/10.1016/j.jobe.2022.104167>

La quota relativa al raffreddamento è quindi molto consistente ed un evento climatico caratterizzato da un caldo intenso aumenta notevolmente i consumi.

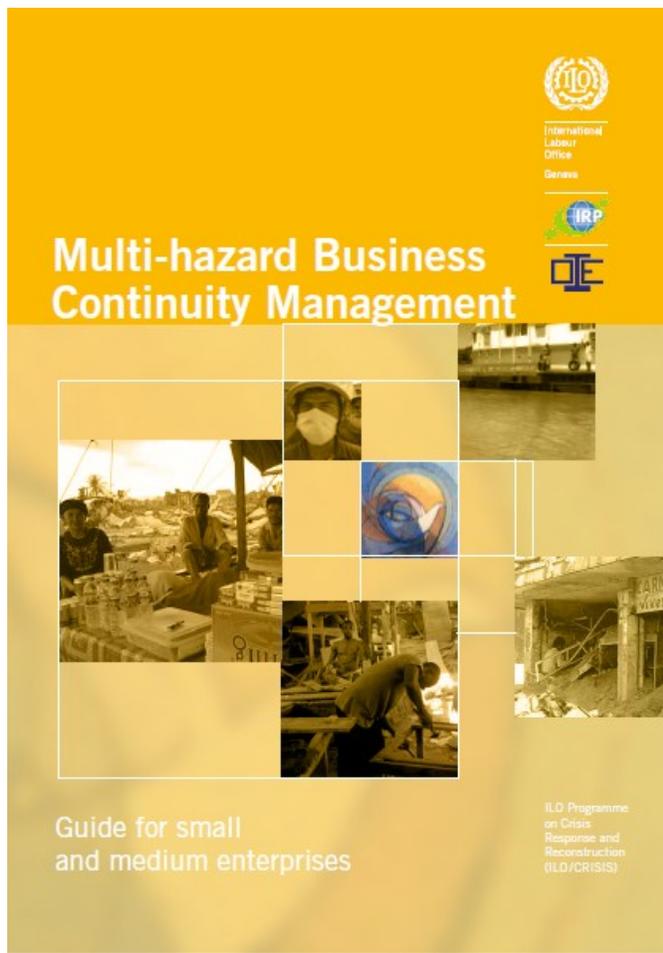
Se tale evento è abbinato ad un lungo periodo di siccità si avranno, lato produzione di energia, le seguenti conseguenze:

- riduzione della produzione energetica da centrali idroelettriche per mancanza di acqua di alimentazione delle turbine
- riduzione della produzione energetica da centrali termiche per mancanza di acqua di raffreddamento.

Quindi ad un aumento della richiesta di energia avviene in corrispondenza di una riduzione della sua produzione.

È quindi necessario ipotizzare delle soluzioni per fronteggiare questi eventi, e queste possono comprendere:

<b>Riduzione dei consumi</b>	<b>Efficientamento energetico del CED con uso di apparati poco energivori</b> <b>Attivazione di un Building Management System</b>
<b>Aumento della propria capacità produttiva autonoma</b>	<b>Autoproduzione da fonti rinnovabili</b> <b>Autoproduzione di energia da fonti tradizionali aumentando la capacità di stoccaggio (se possibile in funzione della collocazione del CED e delle norme di sicurezza anti incendio)</b>



- Chapter 1.....**
- Terminology and Basic Notions.....**
  - 1.1. Overview.....
  - 1.2. Risks and related concepts.....
  - 1.3. Business Continuity Management (BCM) and Planning (BCP).....
  - 1.4. Supply Chains and Business Continuity Management.....
  - 1.5. Disaster Risk: What to do.....
- Chapter 2.....**
- Assessments for Business Continuity Management.....**
  - 2.1. Overview.....
  - 2.2. Step 1: Determine Your Business Priority.....
  - 2.3. Step 2: Identify Assets and Inputs for Your Priority.....
  - 2.4. Step 3: Identify the Time-critical Operations.....
  - 2.5. Step 4: Analyse Internal and External Risks Areas.....
- Chapter 3.....**
- Planning for Business Continuity.....**
  - 3.1. Overview.....
  - 3.2. Step 5. Prepare a Set of Possible Threat Scenarios.....
  - 3.3. Step 6: Design and Validate the Plan.....
- Chapter 4.....**
- Communicating and Training on the Business Continuity Plan.....**
  - 4.1. Overview.....
  - 4.2. Step 7: Design and Roll-out Communication Procedures.....
  - 4.3. Step 8: Design and Deliver Training on BCM.....
- Chapter 5.....**
- Implementing the Business Continuity Plan.....**
  - 5.1. Overview.....
  - 5.2. Step 9: Activate and Deactivate the BCP.....
  - 5.3. Step 10: Gather Lessons Learnt and Adjust the BCP.....

**Grazie per  
l'attenzione!**

[giancarlo.butti@promo.it](mailto:giancarlo.butti@promo.it)



**SETTIMANA  
DELLA  
SOSTENIBILITÀ**

25-28 MARZO 2025



**CONFINDUSTRIA  
VENETO EST**

Area Metropolitana  
Venezia Padova Rovigo Treviso